

Sobre el teorema de los números primos en progresiones aritmética

MATEO ANDRÉS MANOSALVA AMARIS

DIRECTOR:

JOHN JAIME RODRIGUEZ



FACULTAD DE CIENCIAS
DEPARTAMENTO DE MATEMÁTICAS
BOGOTÁ, D.C, COLOMBIA
22 DE OCTUBRE DE 2024

ABSTRACT

The prime number theorem is the assestion that in the limit, the quotient $\frac{\pi(x) \log x}{x}$ goes to 1, which means that $\pi(x) \sim \frac{x}{\log x}$, where $\pi(x)$ is the prime counting function. In arithmetic progressions $a + kq$ with $(a, q) = 1$, we have that $\pi_{a,q}(x)$; the prime counting function restricted to the progression, has the asymptotic behavior $\pi_{a,q}(x) \sim \frac{x}{\phi(q) \log x}$, meaning that primes are uniformly distributed among the residue classes modulo q . In this work, we will present the proof of this result, the underlying ideas, and applications. For this, we will make use of Tauberian theory, which will allow us to present a detailed and concise proof, followed by studying the non-vanishing of $L(\chi, s)$ and some properties of Dirichlet characters and series.

RESUMEN

El teorema de los números primos nos dice que en el límite, el cociente $\frac{\pi(x) \log x}{x}$ tiende a 1, es decir, que $\pi(x) \sim \frac{x}{\log x}$ donde $\pi(x)$ es la función contadora de primos. En progresiones aritméticas $a + kq$ con $(a, q) = 1$, tenemos que $\pi_{a,q}(x)$; la función contadora restringida a la progresión, tiene el comportamiento asintótico $\pi_{a,q}(x) \sim \frac{x}{\phi(q) \log x}$, es decir, los primos se distribuyen uniformemente en las clases de residuos módulo q . En este trabajo se presentará la prueba de este resultado, las ideas subyacentes y aplicaciones. Para esto, haremos uso de la teoría Tauberiana, lo que nos permitirá presentar una prueba detallada y corta, que se seguirá estudiando la no nulidad de $L(\chi, s)$ y algunas propiedades de los caracteres y series de Dirichlet.

Contenido

1 | Preliminares

1.1	Funciones aritmética	8
1.1.1	La función de Möbius	11
1.2	Convolución de Dirichlet	14
1.2.1	Propiedades de algunas funciones aritmética	18
1.3	Sumación Parcial	21
1.3.1	La integral de Riemann-Stieltjes	23
1.3.2	Algunas propiedades de la integral de Riemann-Stieltjes	25
1.4	Algunas estimaciones básicas	26
1.4.1	Una equivalencia importante	27
1.5	Series de Dirichlet	32
1.5.1	Propiedades algebraicas	33
1.5.2	Propiedades analíticas	34
1.5.3	El producto de Euler	41
1.6	La función zeta de Riemann	47

2 | El teorema de Dirichlet

2.1	Caracteres y el teorema de Dirichlet	54
2.1.1	Ortogonalidad de los caracteres	57
2.1.2	Caracteres de Dirichlet	60

Introducción

” *La matemática posee no solo verdad, sino también belleza suprema; una belleza fría y austera, como aquella de la escultura, sin apelación a ninguna parte de nuestra naturaleza débil, sin los adornos magníficos de la pintura o la música, pero sublime y pura, y capaz de una perfección severa como solo las mejores artes pueden presentar*

— **Bertrand Russel**

Alrededor del año 300 a.C. Euclides prueba que hay infinitos números primos, establece que si los primos son finitos, entonces el producto $p_1 \dots p_n + 1$ no es divisible por ningún primo p_1, \dots, p_n , de esta manera siempre se puede construir un número primo adicional. En el siglo XVIII Euler prueba que hay infinitos primos usando la divergencia de la serie armónica, si asumimos que hay un número finito de números primos, entonces el siguiente producto es finito:

$$\prod_p \frac{1}{1 - p^{-1}}.$$

Ahora note que el término del producto es a lo que converge una serie geométrica y dado que $|p^{-1}| < 1$, entonces

$$\begin{aligned} \infty > \prod_p \frac{1}{1 - p^{-1}} &= \prod_p \left(\sum_{k=0}^{\infty} \frac{1}{p^k} \right) = \prod_p \left(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \dots \right) \\ &= \sum_{n=1}^{\infty} \frac{1}{n} \\ &= \infty, \end{aligned}$$

ya que todo número natural puede escribirse de manera única como producto de potencias de primos, esto nos lleva a una evidente contradicción. Euler consigue este argumento ya que venía de estudiar problemas similares, como la convergencia de la serie

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

La idea que tuvo Euler para este problema provenía de estudiar la serie de Taylor de la función $\sin x$

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} \pm \dots,$$

así

$$\frac{\sin x}{x} = 1 - \frac{x^2}{3!} + \frac{x^4}{5!} - \frac{x^6}{7!} \pm \dots$$

En este punto es donde hace un salto de fe, pensando que el polinomio de Taylor se puede escribir como un producto infinito si lo factorizamos sobre sus raíces, ie. Las raíces de $\frac{\sin x}{x}$, asume que lo que ocurre para polinomios finitos también se tiene para polinomios infinitos, obteniendo que

$$\begin{aligned} \frac{\sin x}{x} &= 1 - \frac{x^2}{3!} + \frac{x^4}{5!} - \frac{x^6}{7!} \pm \dots \\ &= \left(1 + \frac{x}{\pi}\right) \left(1 - \frac{x}{\pi}\right) \left(1 + \frac{x}{2\pi}\right) \left(1 - \frac{x}{2\pi}\right) \left(1 + \frac{x}{3\pi}\right) \left(1 - \frac{x}{3\pi}\right) \dots \\ &= \left(1 - \frac{x^2}{\pi^2}\right) \left(1 - \frac{x^2}{2^2\pi^2}\right) \left(1 - \frac{x^2}{3^2\pi^2}\right) \dots, \end{aligned}$$

luego comparando el coeficiente de x^2 en la serie con el de el producto:

$$\frac{1}{3!} = \frac{1}{\pi^2} \left(1 + \frac{1}{2^2} + \frac{1}{3^2} + \dots\right).$$

Esta idea que le daría la “solución” al problema se formaliza a través del teorema de factorización de Weierstrass. Euler seguiría estudiando este problema por mucho tiempo y lo generalizaría a través de la serie absolutamente convergente

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad s > 1.$$

Tiempo después encuentra una fórmula para obtener los valores de esta función en los números pares, ie. $\zeta(2s)$ y también obtuvo su desarrollo como producto:

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}.$$

Esto le permitió demostrar la divergencia de la serie $\sum_p \frac{1}{p}$, un argumento directo y totalmente analítico de que hay infinitos números primos.

Estas ideas llamaron la atención de dos matemáticos muy importantes, Dirichlet y Riemann. Dirichlet usó estas ideas para probar su teorema de progresiones aritmética, Riemann por otro lado estudió íntimamente la función $\zeta(s)$, le asignó a s un número complejo y también la llevó a tener su fama actual al lanzar su conocida conjetura, pero, ¿esto qué tiene que ver con el teorema de los números primos?.

Conjeturado de manera independiente por Gauss (1792) y Legendre (1798), el teorema de los números primos nos permite entender el comportamiento asintótico de la función

contadora de primos $\pi(x)$, nos dice que para números grandes, la cantidad de primos menores que x se puede aproximar por $\frac{x}{\log x}$, escrito de manera formal

$$\lim_{x \rightarrow \infty} \frac{\pi(x) \log x}{x} = 1 \quad \text{o en notación asintótica} \quad \pi(x) \sim \frac{x}{\log x}.$$

Una interpretación heurística de este teorema viene de estudiar la densidad de un conjunto de números naturales. Dado $N \subseteq \mathbb{N}$, la densidad natural de N la definimos como:

$$d = \lim_{n \rightarrow \infty} \frac{|\{m \leq n : m \in N\}|}{n}, \quad \text{siempre que exista el límite.}$$

Note que estudiar la probabilidad de, por ejemplo, que un entero sea divisible por un primo p será equivalente a calcular la densidad del conjunto de enteros que cumple esta propiedad, veamos esto. Dado n , sea c el número de enteros $m \leq n$ tal que $p \mid m$, sabemos por un simple conteo que:

$$\frac{n}{p} - 1 \leq c \leq \frac{n}{p} + 1.$$

Luego, $d = \lim_{n \rightarrow \infty} \frac{c}{n} = \frac{1}{p}$ por el criterio de comparación. Esto nos dice que la probabilidad de que un entero no sea divisible por p es $1 - \frac{1}{p}$, sabemos además que este evento es excluyente, así... La probabilidad de que un número sea primo viene dada por:

$$\prod_{p < n} \left(1 - \frac{1}{p}\right).$$

Para estimar el crecimiento asintótico de este producto una buena idea sería invertirlo, En efecto:

$$\prod_{p < n} \frac{1}{1 - p^{-1}} = \prod_{p < n} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \dots\right) = \sum_{k < n} \frac{1}{k} = H(n),$$

en el siguiente capítulo veremos justamente que $H(n) \sim \log n$, esto nos dice que la probabilidad de que un número sea primo es $(\log n)^{-1}$, más aún:

$$\pi(x) \sim \frac{x}{\log x}.$$

Pero esto no es una prueba del TNP, entonces ¿cómo se puede demostrar algo así?, el camino a seguir en un principio es sorprendente y viene del estudio de la función de $\zeta(s)$, vista como función de variable compleja absolutamente convergente si $\Re(s) > 1$. El primero en mostrar que estudiar esta función daba un camino hacia una prueba del teorema de los números primos fue Riemann en su famoso artículo "Sobre la cantidad de primos menores que una magnitud dada"[1]. Allí Riemann presentaría muchas ideas, pero no las desarrollaría y fue el trabajo de los matemáticos en los siguientes 50 años llegar a una demostración, trabajo que culminaría en las demostraciones Hadamard y de la Vallée Poussin que aparecen en 1896, la prueba, vendría del hecho de que $\zeta(1 + it) \neq 0$, es decir, la función ζ no se anula en la recta vertical de los complejos con parte real 1, algo

sencillamente maravilloso.

Veremos al final de este trabajo la forma en que este teorema se extiende a progresiones aritmética $a + kq$ con $(a, q) = 1$, donde

$$\pi(a, q, x) \sim \frac{x}{\varphi(q) \log x},$$

con φ denotando la función Phi de Euler, y como hay $\varphi(q)$ clases generadoras de primos, entonces los primos se distribuyen uniformemente en las clases módulo q . Esta es una versión más fuerte que el TNP original, y será nuestro objetivo conseguirla.

Sería ideal que el lector de este trabajo esté familiarizado con algunos conceptos del Análisis y del Álgebra, particularmente hago énfasis en un curso de Análisis II y de Variable Compleja, esto hará que la lectura sea mucho más agradable.

Lista de símbolos, notación:

Aquí se esclarecen algunas herramientas de notación importantes para este trabajo.

- \sum_p Denota que la suma se hace sobre el conjunto de los números primos, análogamente \prod_p .
- Denota $\log x$, la función logaritmo natural.
- $f(x) = O(g(x))$
Existe una constante $M > 0$ tal que $|f(x)| \leq Mg(x)$ para todo x en un dominio específico.
- $f(x) \ll g(x)$: $f(x) = O(g(x))$
- $f(x) = o(g(x))$: $\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 0$
- $f(x) \asymp g(x)$: $f(x) \ll g(x)$ y $g(x) \ll f(x)$
- $f(x) \sim g(x)$ denota $\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 1$
- Denotamos por (a, b) el máximo común divisor de a y b .
- $\mathbb{1}_{\mathcal{K}}$ denota la función indicadora (característica) de \mathcal{K} .
- Tomaremos $\mathbb{N} = \mathbb{Z}^+$: el conjunto de los enteros positivos.
- $a^k \parallel b$: $a^k \mid b$ y $a^{k+1} \nmid b$
- e^x o $\exp(x)$ denota la función exponencial.
- $\{x\} = x - \lfloor x \rfloor$: la función parte fraccionaria.
- $\chi(n)$: un carácter de Dirichlet.
- $\pi(x)$: la función contadora de primos.
- $\text{li}(x) = \int_2^x \frac{dt}{\log t}$: la función logaritmo integral.
- $\sum_{p \equiv a(n)}$ en este trabajo denota $\sum_{p \equiv a \pmod{n}}$.

6 • Introducción

- Sea $f : (a, b) \longrightarrow \mathbb{R}$ una función real, denotamos:

$$f(c-) = \lim_{x \rightarrow c^-} f(x), \quad c \in (a, b]$$

$$f(c+) = \lim_{x \rightarrow c^+} f(x), \quad c \in [a, b).$$

Nota. Algunas de estas herramientas de notación se abordarán de manera más detallada más adelante.

Preliminares

” *Hasta el día de hoy, los matemáticos han intentado en vano descubrir algún orden en la secuencia de números primos, y tenemos razones para creer que es un misterio al que la mente humana nunca penetrará*

— Leonhard Euler

Para comenzar con este capítulo presentaremos el teorema fundamental de la aritmética (TFA), una pieza crucial en cualquier trabajo sobre teoría de números.

Teorema 1.1 (TFA). Todo entero $n > 1$ se puede escribir como producto de primos de manera única salvo el orden de los factores, es decir:

$$n = \prod_{j=1}^m p_j^{k_j}.$$

Escribiremos $p^m \parallel n$ siempre que si $p^m \mid n$ entonces $p^{m+1} \nmid n$, es decir, p^m es la potencia exacta que divide a n , esto nos permite escribir el TFA como:

$$n = \prod_{p^m \parallel n} p^m.$$

1.1 Funciones aritmética

Definición. Una función aritmética es una función con dominio los naturales y codominio \mathbb{R} o \mathbb{C} , es decir a es función aritmética si

$$a : \mathbb{N} \rightarrow \mathbb{F},$$

con $\mathbb{F} = \mathbb{C}$ o $\mathbb{F} = \mathbb{R}$.

Esta definición nos muestra que las funciones aritmética no son más que sucesiones de números reales o complejos, en algunos casos será útil considerarlas de esta manera y de manera análoga a las sucesiones las denotaremos como a_n , donde cada a_n representa $f(n)$. Veamos algunos ejemplos importantes:

- **Función constante k :**

$$k(n) = k, \text{ para todo } n \in \mathbb{N}.$$

- **Función unidad:**

$$e(n) = \begin{cases} 1 & n = 1 \\ 0 & n \neq 1. \end{cases}$$

- **Función número de divisores:** $\tau(n)$, el número de divisores positivos de n (incluyendo 1 y n)

$$\tau(n) = \sum_{j|n} 1.$$

- **Función suma de divisores:** $\sigma(n)$, la suma de los divisores positivos de n

$$\sigma(n) = \sum_{j|n} j.$$

- **Función de Möbius:** $\mu(n)$, se define como

$$\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & \text{si } n \text{ no es libre de cuadrados} \\ (-1)^k & \text{si } n \text{ tiene } k \text{ factores primos.} \end{cases}$$

- **Función phi de Euler:** $\varphi(n)$, el número de enteros positivos $m \leq n$ que son primos relativos a n ($(m, n) = 1$)

$$\varphi(n) = \sum_{\substack{m=1 \\ (m,n)=1}}^n 1.$$

- **Función de Von Mangoldt:** $\Lambda(n)$, se define como

$$\Lambda(n) = \begin{cases} \log p & n = p^m \\ 0 & \text{en otro caso.} \end{cases}$$

- **Función identidad:** $N(n)$, la función identidad se define como:

$$N(n) = n.$$

Por la naturaleza de \mathbb{N} , existen dos clases importantes de funciones aritmética, las funciones aditivas y multiplicativas:

- Las funciones aditivas que satisfacen

$$f(mn) = f(m) + f(n) \quad \text{siempre que } (m, n) = 1,$$

- las funciones multiplicativas que satisfacen

$$f(mn) = f(m)f(n) \text{ siempre que } (m, n) = 1.$$

Si una función aditiva o multiplicativa satisface la propiedad para cualquier par de números naturales m y n , se dirá que la función es completamente aditiva o completamente multiplicativa, respectivamente, las funciones aditivas y multiplicativas están determinadas por sus valores en las potencias de los números primos.

Demostración. Supongamos que f es aditiva y $n > 1$, por el TFA:

$$f(n) = f\left(\prod_{p^m \parallel n} p^m\right) = \sum_{p^m \parallel n} f(p^m).$$

Ahora, si f es multiplicativa:

$$f(n) = f\left(\prod_{p^m \parallel n} p^m\right) = \prod_{p^m \parallel n} f(p^m).$$

□

Si además la función es completamente multiplicativa:

$$f(n) = f\left(\prod_{i=1}^m p_i^{k_i}\right) = \prod_{i=1}^m f(p_i)^{k_i},$$

lo que también ocurre para funciones completamente aditivas, cambiando el producto por una suma. Una propiedad adicional que será útil para caracterizar estas funciones es que si f es aditiva y no idénticamente nula, entonces para algún n , $f(1 \cdot n) = f(1) + f(n)$, así $f(1) = 0$, análogamente si f es multiplicativa y no idénticamente nula $f(1 \cdot n) = f(1)f(n)$, $f(1) = 1$.

Ahora veamos que aunque la función de Von Mangoldt, parece extraña, su definición es natural y nos permite obtener una versión logarítmica del teorema fundamental de la aritmética.

Teorema 1.2. Dado $n \in \mathbb{N}$, $n > 1$ entonces:

$$\log(n) = \sum_{j \mid n} \Lambda(j).$$

Demostración. Note que si $n > 1$, entonces por el TFA:

$$\log(n) = k_1 \log(p_1) + \dots + k_m \log(p_m),$$

donde los p_j de la igualdad son los primos de su descomposición y k_j sus potencias respectivas. Así, esta igualdad nos dice que en el cálculo de $\log(n)$ solo importan los valores del log en los divisores primos o potencias de primos, luego:

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

□

Sin embargo, la principal motivación para introducir la función de Von Mangoldt es que sus sumas parciales $\sum_{n \leq x} \Lambda(n)$ son la suma ponderada de las potencias de primos $p^m \leq x$, tomando como peso $\log p$, el peso correcto para compensar la densidad de primos. No es difícil demostrar que las potencias p^m con $(m \geq 2)$ contribuyen poco en la suma anterior.

De hecho, estudiar el comportamiento asintótico de la suma anterior resultará equivalente a estudiar el de la función de contadora de primos $\pi(x)$; aún más, el TNP es equivalente a la afirmación

$$\lim_{x \rightarrow \infty} \frac{1}{x} \sum_{n \leq x} \Lambda(n) = 1.$$

Esta equivalencia nos dará el camino a la prueba del teorema de los números primos, lo que la convierte en una función aritmética muy importante.[2]

Definición. Las funciones $\psi(x)$ y $\vartheta(x)$ de Chevyshev se definen como sigue:

$$\vartheta(x) = \sum_{p \leq x} \log p, \quad \psi(x) = \sum_{n \leq x} \Lambda(n).$$

1.1.1. La función de Möbius

Es natural preguntarse por la definición de la función de Möbius, ya que de todas parece ser la más extraña, uno se preguntaría si hay una forma de motivarla...

Consideremos la función:

$$L(x) = \sum_{n \leq x} \log(n).$$

Note que aplicando el teorema anterior

$$L(x) = \sum_{n \leq x} \log(n) = \sum_{n \leq x} \sum_{j|n} \Lambda(j). \quad (1.1)$$

Vamos a aplicar una técnica muy útil y frecuente en teoría de números, el cambio de orden de sumación, para esto vamos a cambiar n y j de orden en la doble suma (1.1) y conservaremos la condición $j | n$.

$$\begin{aligned}
L(x) &= \sum_{n \leq x} \log(n) = \sum_{n \leq x} \sum_{j|n} \Lambda(j) \\
&= \sum_{j \leq x} \sum_{\substack{n \leq x \\ j|n}} \Lambda(j) \\
&= \sum_{j \leq x} \Lambda(j) \sum_{\substack{n \leq x \\ j|n}} 1,
\end{aligned}$$

ahora, ¿cuántos enteros positivos $n \leq x$ hay tal que $j \mid n$?, pues exactamente $\frac{x}{j}$, así

$$L(x) = \sum_{j \leq x} \Lambda(j) \sum_{m \leq \frac{x}{j}} 1,$$

y cambiando nuevamente el orden de sumación

$$\begin{aligned}
L(x) &= \sum_{m \leq x} \sum_{j \leq \frac{x}{m}} \Lambda(j) \\
&= \sum_{m \leq x} \psi\left(\frac{x}{m}\right).
\end{aligned}$$

Esta identidad la abordaremos más adelante, pero de momento sabemos que podemos escribir a $L(x)$ en términos de $\psi(x)$, ¿y si queremos lo opuesto?, ie. a $\psi(x)$ en términos de $L(x)$, ¿podemos **invertir** el papel de las funciones?. Vamos a abordar esta pregunta poniéndola en un contexto más general.

Siguiendo a [3], supongamos $F(x)$ y $G(x)$ funciones aritmética con $G(x) = \sum_{n \leq x} F\left(\frac{x}{n}\right)$, tenemos que:

$$G\left(\frac{x}{2}\right) = F\left(\frac{x}{2}\right) + F\left(\frac{x}{4}\right) + F\left(\frac{x}{6}\right) + \dots,$$

así:

$$G(x) - G\left(\frac{x}{2}\right) = F(x) + F\left(\frac{x}{3}\right) + F\left(\frac{x}{5}\right) + \dots,$$

podemos pensar que continuar restando los términos $G\left(\frac{x}{j}\right)$ nos permitirá obtener la inversión, sin embargo el término $G\left(\frac{x}{3}\right)$ contiene a $F\left(\frac{x}{6}\right)$, por tanto

$$G(x) - G\left(\frac{x}{2}\right) - G\left(\frac{x}{3}\right) = F(x) + F\left(\frac{x}{5}\right) - F\left(\frac{x}{6}\right) + F\left(\frac{x}{7}\right) + \dots,$$

así, en los siguientes pasos debemos eliminar $-F\left(\frac{x}{6}\right)$. Esto se lograría sumando $G\left(\frac{x}{6}\right)$ y no restándolo. La suma anterior nos muestra además que no necesitamos restar

$G\left(\frac{x}{4}\right)$ pues $F\left(\frac{x}{4}\right)$ ya desapareció al restar $G\left(\frac{x}{2}\right)$.

Así, podemos intuir que necesitamos multiplicar $G\left(\frac{x}{j}\right)$ en cada sumando, por una función que nos de el signo adecuado (sume y reste, según se necesite) o anule el término, como ocurre en el caso de $G\left(\frac{x}{4}\right)$. Denotemos esta función que estamos buscando como $\mu(x)$. Si suponemos que existe dicha función, entonces

$$F(x) = \sum_{j \leq x} \mu(j) G\left(\frac{x}{j}\right). \quad (1.2)$$

Además, ya tenemos algunos valores de μ , $\mu(1) = 1$, $\mu(2) = \mu(3) = -1$, $\mu(4) = 0$ y $\mu(6) = 1$. Podemos de momento darnos cuenta que estos valores parecen coincidir con los que obtendríamos al evaluar la función de Möbius, lo cual no es ninguna coincidencia, sin embargo aún no podemos afirmar que son en esencia la misma función. Note que por la definición de G

$$G\left(\frac{x}{j}\right) = \sum_{k \leq \frac{x}{j}} F\left(\frac{x}{jk}\right), \quad (1.3)$$

por tanto al reemplazar (1.3) en (1.2), obtenemos:

$$\begin{aligned} F(x) &= \sum_{j \leq x} \mu(j) \sum_{jk \leq x} F\left(\frac{x}{jk}\right) = \sum_{jk \leq x} \mu(j) F\left(\frac{x}{jk}\right) \\ &= \sum_{n \leq x} F\left(\frac{x}{n}\right) \sum_{jk=n} \mu(j). \end{aligned}$$

Finalmente

$$F(x) = F(x) + \sum_{1 < n \leq x} F\left(\frac{x}{n}\right) \sum_{jk=n} \mu(j). \quad (1.4)$$

Para obtener la inversión necesitamos que la doble suma en (1.4) se anule, y dado que no tenemos condiciones sobre F , la función μ debe cumplir que si $n \neq 1$

$$\sum_{jk=n} \mu(j) = 0$$

En efecto, *la función que cumple esta propiedad es... la función de Möbius.*

Teorema 1.3. Sea $n \geq 1$, entonces

$$\sum_{d|n} \mu(d) = e(n).$$

Antes de continuar con la prueba de este resultado notemos que la suma en (1.2) en realidad no recorre los $j \leq x$, sino los j que son divisores de x ya que G es función aritmética y por tanto $\frac{x}{j}$ es necesariamente un número natural. Así

$$F(x) = \sum_{j|x} \mu(j) G\left(\frac{x}{j}\right) \quad (1.5)$$

Esta suma sobre los divisores de n llevará el nombre de convolución o producto de Dirichlet y nos permitirá darle al conjunto de las funciones aritmética una estructura de monoide abeliano, estas ideas sin embargo las estudiaremos en la siguiente sección. Ahora continuemos con la prueba.

Demostración. Si $n = 1$, entonces $1 = e(1) = \mu(1)$, si $n \neq 1$, entonces por el teorema fundamental de la aritmética $n = \prod_{i=1}^k p_i^{\alpha_i}$, note que los únicos divisores d tales que $\mu(d) \neq 0$ son los que toman la forma $d = p_{i_1} \dots p_{i_r}$ donde $\mathcal{K} = \{i_1, \dots, i_r\} \subseteq \{1, \dots, k\}$, en este caso $\mu(d) = (-1)^{|\mathcal{K}|}$. Necesitamos saber cuántas veces va a aparecer este valor en la suma, es decir dado un $0 \leq r \leq k$ fijo, ¿cuántos subconjuntos de $\{1, \dots, k\}$ tienen cardinal r ?, exactamente $\binom{k}{r}$. Así la suma toma la forma:

$$\begin{aligned} \sum_{d|n} \mu(d) &= 1 + \sum_i \mu(p_i) + \sum_{i,j} \mu(p_i p_j) + \dots + \mu(p_1 \dots p_k) \\ &= 1 - k + \binom{k}{2} + \dots + (-1)^k \\ &= \sum_{r=1}^k \binom{k}{r} (-1)^r = (1 - 1)^k = 0. \end{aligned}$$

□

Aplicando esto a la función $L(x)$, obtenemos que

$$\psi(x) = \sum_{j|n} \mu(j) L\left(\frac{n}{j}\right).$$

La fórmula en (1.5) se conoce como inversión de Möbius, las ideas aquí sin embargo fueron abordadas de manera informal, para poder presentar un argumento riguroso, necesitamos, como se menciona antes, introducir la convolución de Dirichlet, que además nos permitirá obtener propiedades importantes de algunas de las funciones aritmética que hemos presentado en esta sección.

1.2 Convolución de Dirichlet

Siguiendo las ideas de la sección anterior, presentamos la siguiente definición:

Definición. Sean f y g funciones aritméticas. Definimos la convolución o producto de Dirichlet como

$$(f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

O simplemente $f * g$.

Algunos resultados del capítulo anterior se pueden escribir en términos de convolución, por ejemplo, el TFA se puede presentar como

$$\log n = \sum_{j|n} \Lambda(j) = \Lambda * 1,$$

donde 1 , denota la función constante 1 , también $\psi(x) = \mu * L$, pero la convolución no solo se introduce como una manera de simplificar notación, como mencionamos antes, esta tiene propiedades importantes que nos permitirán darle una estructura algebraica a las funciones aritmética.

Teorema 1.4. Sean f y g funciones aritméticas. Entonces se cumple lo siguiente

- $f * g = g * f$.
- $(f * g) * h = f * (g * h)$.
- $e * f = f * e = f$.

Demostración. Primero note que $\sum_{j|n} f(j)g\left(\frac{n}{j}\right) = \sum_{jk=n} f(j)g(k)$, ya que en ambos casos la suma recorre los divisores de n , luego

$$\begin{aligned} (f * g)(n) &= \sum_{j_1 j_2 = n} f(j_1)g(j_2) = \sum_{j_1 j_2 = n} g(j_1)f(j_2) \\ &= (g * f)(n). \end{aligned}$$

Ya que no importa el orden en el la suma recorra los divisores, lo que prueba la conmutatividad. Ahora, recordemos que $e(n) = 1$ si $n = 1$ y 0 si $n \neq 1$, por tanto

$$(e * f)(n) = (f * e)(n) = \sum_{j|n} f(j)e\left(\frac{n}{j}\right).$$

Así, como $e\left(\frac{n}{j}\right) = 0$ si $j \neq n$, los términos de la suma son cero excepto cuando $j = n$,

$$(e * f)(n) = (f * e)(n) = \sum_{j|n} f(j)e\left(\frac{n}{j}\right) = f(n) = f.$$

Para probar la asociatividad, considere $N = g * h$ y $M = f * g$, luego

$$\begin{aligned}
(f * N)(n) &= \sum_{j|n} f(j) N\left(\frac{n}{j}\right) \\
&= \sum_{j_1 j_2 = n} f(j_1) N(j_2) \\
&= \sum_{j_1 j_2 = n} f(j_1) \left(\sum_{j_3 j_4 = j_2} g(j_3) h(j_4) \right) \\
&= \sum_{j_1 j_3 j_4 = n} f(j_1) g(j_3) h(j_4) \\
&= \sum_{j_1 j_3 j_4 = n} f(j_3) g(j_4) h(j_1) \\
&= \sum_{j_1 j_2 = n} \left(\sum_{j_3 j_4 = j_2} f(j_3) g(j_4) \right) h(j_1) \\
&= \sum_{j_1 j_2 = n} M(j_2) h(j_1) \\
&= (M * h)(n).
\end{aligned}$$

□

Hemos probado en particular que la función e es el elemento neutro de la convolución, sabemos además que $\mu * 1 = e$, es decir la función de Möbius tiene inverso multiplicativo, con estas nuevas herramientas podemos presentar una prueba corta y rigurosa de la fórmula de inversión de Möbius (1.5).

Teorema 1.5 (Fórmula de inversión de Möbius). Sean f y g funciones aritmética, entonces $f = g * 1$ si y solo si $g = \mu * f$.

Demostración. Note que $f = g * 1$ si y solo si $\mu * f = \mu * g * 1 = g * \mu * 1 = g * e = g$ □

Sin embargo, no toda función aritmética tiene inverso multiplicativo, el caso más evidente es tomar la función constante $N = 0$, note que para toda f , $f * N = N$. Esto nos lleva a la pregunta: ¿bajo qué condiciones una función aritmética tiene inverso multiplicativo?, la respuesta podría venir de estudiar las características que no permiten que N lo tenga... A saber, N *se anula en todo punto*, ¿bastaría con que esta función no se anule en todo su dominio para que tenga inversa?, o ¿en algún punto en particular?, la respuesta nos viene del siguiente teorema, basta con que la función no se anule en 1 para poder garantizar además la *unicidad*.

Teorema 1.6. Sea f una función aritmética tal que $f(1) \neq 0$. Entonces existe una única función aritmética g tal que $f * g = e$.

Demostración. Note que si $n = 1$, entonces $f(1)g(1) = e(1) = 1$, así $g(1) = \frac{1}{f(1)}$, ahora supongamos que g se ha definido para todos los valores $1 < k < n$, luego como $f * g(n) = 0$:

$$0 = \sum_{d|n} g(d) f\left(\frac{n}{d}\right) = \sum_{\substack{d|n \\ d < n}} f\left(\frac{n}{d}\right) g(d) + f(1)g(n), \quad (1.6)$$

así

$$g(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d < n}} f\left(\frac{n}{d}\right) g(d), 1$$

Esto nos define g de manera recursiva, lo que concluye el resultado. \square

Esto nos permite dotar a estas funciones aritmética de una estructura de grupo Abelian, ya que si $f(1) \neq 0$ y $g(1) \neq 0$, entonces $f * g(1) = f(1)g(1) \neq 0$.

Teorema 1.7. Sean f y g funciones aritméticas multiplicativas, entonces $f * g$ también es multiplicativa.

Demostración. Sean $x, y \in \mathbb{N}$ tal que $(x, y) = 1$. Note que cada divisor $d | xy$ puede escribirse de manera única como $d = mn$ donde $m | x$ y $n | y$, además $(m, n) = 1$ y $\left(\frac{x}{m}, \frac{y}{n}\right) = 1$, por lo tanto

$$\begin{aligned} (f * g)(xy) &= \sum_{d|xy} f(d)g\left(\frac{xy}{d}\right) \\ &= \sum_{\substack{m|x \\ n|y}} f(mn)g\left(\frac{xy}{mn}\right) \\ &= \sum_{\substack{m|x \\ n|y}} f(m)g\left(\frac{x}{m}\right) f(n)g\left(\frac{y}{n}\right) \\ &= \sum_{m|x} f(m)g\left(\frac{y}{m}\right) \sum_{n|y} f(n)g\left(\frac{y}{n}\right) \\ &= (f * g)(x)(f * g)(y). \end{aligned}$$

Así $f * g$ es multiplicativa. \square

Teorema 1.8. Si f es multiplicativa, entonces $g = f^{-1}$ también es multiplicativa.

Donde f^{-1} denota su inversa, presentaremos una prueba siguiendo a [2]

Demostración. Queremos ver que:

$$g(n_1 n_2) = g(n_1)g(n_2) \quad \text{si} \quad (n_1, n_2) = 1. \quad (1.7)$$

Procedamos por inducción matemática. Sea $n = n_1 n_2$, si $n_1 n_2 = 1$, entonces $n_1 = n_2 = 1$, luego

$$g(1 \cdot 1) = g(1) = \frac{1}{f(1)} = 1 = g(1)g(1).$$

Supongamos ahora que g satisface (1.7) para todo $k_1 k_2 \geq 2$ tal que $k_1 k_2 < n$ y sean n_1 y n_2 tales que $n_1 n_2 = n$ y $(n_1, n_2) = 1$, por (1.6) tenemos que:

$$\begin{aligned} 0 &= \sum_{d|n_1 n_2} f(d)g\left(\frac{n_1 n_2}{d}\right) \\ &= \sum_{\substack{d_1|n_1 \\ d_2|n_2 \\ d_1 d_2 < n}} f(d_1)f(d_2)g\left(\frac{n_1}{d_1}\right)g\left(\frac{n_2}{d_2}\right) + g(n_1 n_2) \\ &= \sum_{\substack{d_1|n_1 \\ d_2|n_2}} f(d_1)f(d_2)g\left(\frac{n_1}{d_1}\right)g\left(\frac{n_2}{d_2}\right) + g(n_1 n_2) - g(n_1)g(n_2) \\ &= (f * g)(n_1)(f * g)(n_2) + (g(n_1 n_2) - g(n_1)g(n_2)), \end{aligned}$$

luego:

$$g(n_1)g(n_2) = e(n_1)e(n_2) + g(n_1 n_2),$$

y como $n_1 n_2 \geq 2$, entonces $n_1 \geq 2$ o $n_2 \geq 2$, así $e(n_1)e(n_2) = 0$, por tanto $g(n_1 n_2) = g(n_1)g(n_2)$. \square

Corolario 1.9. Sea \mathcal{M} el conjunto de funciones aritmética multiplicativas, entonces $(\mathcal{M}, *)$ es un grupo Abeliano.

1.2.1. Propiedades de algunas funciones aritmética

Finalizaremos esta sección con algunas propiedades importantes de las funciones aritmética que definimos el inicio del capítulo.

La función φ de Euler

La propiedad del teorema (1.3) nos permite manipular sumas con condiciones de coprimidad, es decir sumas sobre los n que son coprimos con un entero k fijo. Considere el conjunto $C_k = \{n \mid (n, k) = 1\}$, note que la función característica del conjunto C_k es:

$$\mathbb{1}_{C_k}(n) = \sum_{d|(n,k)} \mu(d) = e((n, k)),$$

Una aplicación de esto, nos permite obtener la siguiente propiedad de la función φ de Euler:

$$\begin{aligned}
 \varphi(n) &= \sum_{\substack{m \leq n \\ (m,n)=1}} 1 = \sum_{m \leq n} \mathbb{1}_{C_n}(m) \\
 &= \sum_{m \leq n} \sum_{d|(m,n)} \mu(d) \\
 &= \sum_{d|n} \mu(d) \sum_{\substack{m \leq n \\ d|m}} 1 \\
 &= \sum_{d|n} \mu(d) \frac{n}{d} \\
 &= \mu * N(n) = n \sum_{d|n} \frac{\mu(d)}{d}.
 \end{aligned}$$

Es claro que la función N es multiplicativa por definición, luego esta propiedad nos permite probar que la función φ es multiplicativa, por el teorema (1.7) basta ver que en efecto μ lo es.

Teorema 1.10. La función μ es multiplicativa:

Demostración. Supongamos que $n = n_1 n_2$, si $n = 1$, entonces $n_1 = n_2 = 1$, $\mu(n) = \mu(n_1)\mu(n_2) = 1$. Ahora supongamos que $\mu(k) = \mu(k_1)\mu(k_2)$, para todo $k = k_1 k_2$ tal que $1 < k < n$ y $(k_1, k_2) = 1$ y sean n_1, n_2 tales que $n_1 n_2 = n$ y $(n_1, n_2) = 1$, tenemos que

$$\begin{aligned}
 0 &= \sum_{d|n_1 n_2} \mu(d) \\
 &= \sum_{\substack{d_1|n_1 \\ d_2|n_2 \\ d_1 d_2 < n}} \mu(d_1)\mu(d_2) + \mu(n_1 n_2) \\
 &= \sum_{d_1|n_1} \mu(d_1) \sum_{d_2|n_2} \mu(d_2) + \mu(n_1 n_2) - \mu(n_1)\mu(n_2) \\
 &= \mu(n_1 n_2) - \mu(n_1)\mu(n_2).
 \end{aligned}$$

Así, por el principio de inducción matemática se sigue el resultado. □

Corolario 1.11. La función $\varphi(n)$ tiene las siguientes propiedades:

- i) $\varphi(mn) = \varphi(m)\varphi(n)$ si $(m, n) = 1$
- ii) $\varphi(p^n) = p^n - p^{n-1}$
- iii) $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$

Demostración. i) Como $\varphi = \mu * N$, se sigue del teorema anterior.

ii) Note que si $n = p^k$, entonces

$$\begin{aligned}\varphi(p^k) &= p^k \sum_{j|p^k} \frac{\mu(j)}{j} \\ &= p^k \left(1 + \frac{\mu(p)}{p} + \frac{\mu(p^2)}{p^2} + \dots + \frac{\mu(p^k)}{p^k} \right) \\ &= p^k \left(1 - \frac{1}{p} \right) = p^k - p^{k-1}.\end{aligned}$$

iii) Sea $n > 1$, por el TFA se sigue que

$$\begin{aligned}\varphi(n) &= \varphi \left(\prod_{p^m | n} p^m \right) \\ &= \prod_{p^m | n} \varphi(p^m) \\ &= \prod_{p^m | n} p^m - p^{m-1} \\ &= n \prod_{p|n} \left(1 - \frac{1}{p} \right).\end{aligned}$$

□

Al inicio del capítulo mencionamos que las funciones aritmética están totalmente determinadas por sus valores en las potencias de primos, esta propiedad nos permite probar de manera sencilla afirmaciones del estilo $f * g = h$, siempre que f, g y h sean funciones multiplicativas, basta ver que $f * g(p^m) = h(p^m)$, veamos un ejemplo:

Teorema 1.12. La función $\varphi(n)$ satisface la propiedad:

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

Demostración. La afirmación se puede escribir como $N = \varphi * 1$, como estas funciones son multiplicativas, entonces basta ver que la identidad se tiene en las potencias de primos, en efecto

$$\begin{aligned}\sum_{j|p^m} \varphi(j) &= \varphi(1) + \varphi(p) + \varphi(p^2) + \varphi(p^3) + \dots + \varphi(p^m) \\ &= 1 + (p - 1) + (p^2 - p) + (p^3 - p^2) + \dots + (p^m - p^{m-1}) \\ &= p^m.\end{aligned}$$

□

Esta identidad también puede probarse usando propiedades de la convolución

$$\sum_{j|n} \varphi(j) = \varphi * 1(n) = (N * \mu) * 1(n) = N * (\mu * 1)(n) = N * e(n) = n.$$

Las funciones número y suma de divisores

También podemos aplicar la convolución para obtener también propiedades de la funciones suma y número de divisores, por ejemplo:

$$\sigma(n) = \sum_{j|n} j = N * 1(n) \quad \text{y} \quad \tau(n) = \sum_{j|n} 1 = 1 * 1(n). \quad (1.8)$$

Note que $\sigma * \varphi = (N * 1) * (\mu * N) = (N * e) * N = N * N$, en efecto:

$$\sigma * \varphi(n) = N * N(n) = \sum_{j|n} j \cdot \frac{n}{j} = n \sum_{j|n} 1 = n\tau(n).$$

Con lo que obtenemos una propiedad interesante que relaciona estas 3 funciones aritmética, pero además (1.8) nos dice también que las funciones σ y τ son multiplicativas por ser convolución de funciones multiplicativas. Observemos una última propiedad de estas funciones, que nos permite caracterizar la noción de primalidad.

Proposición 1.13. Un entero n es primo si y solo si $\sigma(n) + \varphi(n) = n\tau(n)$.

Demostración. Si n es primo, entonces $\varphi(n) = n - 1$, $\sigma(n) = n + 1$ y $\tau(n) = 2$, luego es claro que $\sigma(n) + \varphi(n) = n\tau(n)$. Veamos ahora que si n no es primo entonces no se sigue el teorema

Si n no es primo entonces $\varphi(n) < n - 1$, ahora note que

$$\sigma(n) = \sum_{j|n} j = 1 + \sum_{\substack{j|n \\ j>1}} j \leq 1 + n(\tau(n) - 1).$$

Luego:

$$\sigma(n) + \varphi(n) < n - 1 + 1 + n\tau(n) - n = n\tau(n).$$

□

1.3 Sumación Parcial

Los resultados que hemos podido obtener hasta el momento solo se centran en casos finitos, en sumas sobre los divisores de un entero n fijo o sobre los k que son primos relativos a n , estos son casos privilegiados, nuestro objetivo sigue siendo el TNP, para esto necesitamos poder obtener relaciones asintóticas, algunas funciones como μ o φ aparentan comportamientos caóticos al graficarlas en función de n y por tanto no tiene

mucho sentido estudiar un comportamiento asintótico para ellas, sin embargo, algunas funciones aritmética $f(n) = a_n$ tienen buen comportamiento en la media, en el sentido de que sus sumas parciales:

$$A(x) = \sum_{n \leq x} a_n.$$

Tienden a ser suaves conforme $x \rightarrow \infty$ y frecuentemente podemos estudiarlas de manera precisa, ejemplo de esto son $\pi(x)$ o $\psi(x)$. En esta sección estudiaremos algunos de los métodos principales para obtener dichas estimaciones, estimaciones que nos darán un camino a la prueba del TNP.

Definición. Sea f una función real definida en $[a, b]$. Suponga que $f(x+)$ y $f(x-)$ existen para todo $x \in (a, b)$. Definimos

- $f(x) - f(x-)$: Salto a izquierda de f en x .
- $f(x+) - f(x)$: Salto a derecha de f en x .
- $[f(x) - f(x-)] + [f(x+) - f(x)] = f(x+) - f(x-)$: Salto de f en x .

Nota. Diremos que $f(x) = O(g(x))$ cuando existen constantes $M > 0$ y x_0 tales que para todo $x > x_0$, se cumple que $|f(x)| \leq M|g(x)|$, es decir, nuestro dominio específico es $x > x_0$.

Una **fórmula asintótica** para $f(x)$ es una expresión de la forma $f(x) \sim g(x)$, mientras que una **estimación asintótica** para $f(x)$ es una expresión del tipo $f(x) = g(x) + O(R(x))$, donde $g(x)$ representa el término principal y $R(x)$ el término de error. La notación O grande nos permite entonces controlar el error de estimaciones asintóticas de manera precisa, cosa que no ocurre con o pequeña, recordemos que:

$$f(x) = o(g(x)) : \lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 0.$$

Esto intuitivamente nos dice que $f(x)$ “crece más lento” que $g(x)$, pero esto no nos da tanta información acerca de f con O grande, ya que no sabemos la “velocidad” con la que este cociente tiende a 0.

Las estimaciones con O también son más fáciles de trabajar y manipular que las estimaciones con o . Por ejemplo, las O se pueden “sacar” de integrales o sumas, siempre que las funciones involucradas sean no negativas, mientras que tales manipulaciones generalmente no se permiten con las o .

1.3.1. La integral de Riemann-Stieltjes

Sean $P = \{x_0, x_1, \dots, x_n\} \in \mathcal{P}[a, b]$ (las particiones del intervalo $[a, b]$) y $t_k \in [x_{k-1}, x_k]$ cualesquiera. Una suma de la forma

$$S(P, f) = \sum_{k=1}^n f(t_k) \Delta x_k,$$

se denomina **suma de Riemann** de f en $[a, b]$, recordamos que $\Delta x_k = x_k - x_{k-1}$.

La integral usual se define como el límite de las sumas de Riemann, esta definición nos da una correspondencia importante: Toda integral de Riemann se puede ver como el límite de una suma, una serie.

Sin embargo, no toda suma se puede ver como una integral bajo esta definición, si tenemos una con una condición de sumación sobre, por ejemplo, los números primos, no hay un camino claro para expresarla como una integral, la solución a este problema viene de generalizar la noción de integral.

La propiedad deseada la obtendremos de la integral de Riemann-Stieltjes.

Definición.

- i) Sean $P = \{x_0, x_1, \dots, x_n\} \in \mathcal{P}[a, b]$ (las particiones del intervalo $[a, b]$) y $t_k \in [x_{k-1}, x_k]$ cualesquiera.

Una suma de la forma

$$S(P, f, \alpha) = \sum_{k=1}^n f(t_k) \Delta \alpha_k,$$

se denomina **suma de Riemann-Stieltjes** de f con respecto a α en $[a, b]$.

- ii) Decimos que f es **Riemann-Integrable** con respecto a α en $[a, b]$, y escribimos “ $f \in \mathcal{R}(\alpha)$ en $[a, b]$ ”, si existe $A \in \mathbb{R}$ que satisface que

Para todo $\varepsilon > 0$ existe $P_\varepsilon \in \mathcal{P}[a, b]$ tal que si para toda $P \supset P_\varepsilon$ y para cualquier elección de puntos $t_k \in [x_{k-1}, x_k]$, entonces

$$|S(P, f, \alpha) - A| < \varepsilon.$$

Donde $\Delta \alpha_k = \alpha(x_k) - \alpha(x_{k-1})$, cuando A existe, es único y se denota por

$$\int_a^b f d\alpha \quad \text{o} \quad \int_a^b f(x) d\alpha(x).$$

La función f es llamada *integrando* y la función α es llamada *integrador*.

Note que la integral de Riemann no es más que un caso particular de la de Riemann-Stieltjes, cuando $\alpha(x) = x$, esta integral y sus propiedades se suelen estudiar en un curso

de Análisis II, aquí recordaremos algunas de las más importantes.

Teorema 1.14 ([4], Teorema 7.11). Sea α una función escalonada definida en $[a, b]$ con salto α_k en x_k .

Sea f una función definida en $[a, b]$ tal que f y α no sean ambas discontinuas a la derecha o a la izquierda de cada x_k . Entonces $\int_a^b f d\alpha$ existe y se tiene que:

$$\int_a^b f(x) d\alpha(x) = \sum_{k=1}^n f(x_k) \alpha_k.$$

La prueba de esto se encuentra en [4], sin embargo, nos será útil explorar la idea.

Note que α es constante en los intervalos (x_{k-1}, x_k) , luego por intervalos la integral es 0 ya que para cualquier suma de Riemann-Stieltjes, $S(P, f, \alpha) = 0$. Así, para conocer el valor de la integral entonces solo tendríamos que sumar el valor que toma alrededor de cada x_k .

Supongamos que α tiene salto α_k en un punto $x_k \in [a, b]$, no es difícil ver que:

$$\int_a^b f d\alpha = f(x_k)[\alpha(x_k+) - \alpha(x_k-)] = f(x_k)\alpha_k. \quad (1.9)$$

La prueba de esto se encuentra también en [4] [Teorema 7.9], en efecto si repetimos esto para cada x_k obtenemos la suma deseada.

Sea f continua en $[0, N]$, el teorema anterior nos permite expresar la suma $\sum_{n=1}^N a_n f(n)$ como una integral de Riemann Stieltjes considerando sus sumas parciales

$$\sum_{n=1}^N a_n f(n) = \int_0^N f(x) dA(x).$$

Ya que al aplicar (1.9) tomando como integrador las sumas parciales tenemos que $A(n+) - A(n-) = A(n) - A(n-1) = a_n$, luego en cada paso la integral toma el valor $a_n f(n)$.

Nota. El límite inferior de la integral puede ser cualquier número en el intervalo $[0, 1)$ y el superior cualquier número en $[N, N+1)$

Ejemplo.

- Si se toma $\alpha(x) = [x]$, entonces

$$\int_a^b f(x) d[x] = \sum_{a < n \leq b} f(n).$$

- Si se toma $\alpha(x) = \pi(x)$, la función contadora de primos, que tiene un salto de 1 en cada p primo, entonces

$$\int_a^b f(x) d\pi(x) = \sum_{a < p \leq b} f(p).$$

1.3.2. Algunas propiedades de la integral de Riemann-Stieltjes

Teorema 1.15 (Integración por partes). Si $f \in \mathcal{R}(\alpha)$ en $[a, b]$ entonces $\alpha \in \mathcal{R}(f)$ en $[a, b]$ y

$$\int_a^b f(x) d\alpha(x) + \int_a^b \alpha(x) df(x) = f(b)\alpha(b) - f(a)\alpha(a).$$

Bajo ciertas condiciones una integral de Riemann-Stieltjes se puede reducir a una integral de Riemann usual, esto es muy útil puesto que estamos más familiarizados con el cálculo de estas, dichas condiciones son presentadas en el siguiente teorema:

Teorema 1.16. Sea $f \in \mathcal{R}(\alpha)$ en $[a, b]$, donde $\alpha \in C^1[a, b]$, entonces, $\int_a^b f(x) \alpha'(x) dx$ existe y

$$\int_a^b f d\alpha = \int_a^b f(x) \alpha'(x) dx.$$

Las pruebas de estos teoremas se encuentran también en [4], por lo que no las presentaremos aquí para no extendernos demasiado en la teoría de esta sección, con estas propiedades ya podemos presentar una prueba del teorema de sumación de Abel.

Teorema 1.17 (Sumación parcial de Abel). Sea a_n función aritmética y $f \in C^1[1, x]$, entonces:

$$\sum_{n \leq x} a_n f(n) = A(x)f(x) - \int_1^x A(t)f'(t) dt.$$

Demostración. Tenemos que:

$$\sum_{n \leq x} a_n f(n) = \int_0^x f(t) dA(t) = f(x)A(x) - \int_0^x A(t) df(t),$$

ya que $A(x) = 0$ para todo $x \in [0, 1)$, en efecto

$$\begin{aligned} \sum_{n \leq x} a_n f(n) &= f(x)A(x) - \int_1^x A(t) df(t) \\ &= f(x)A(x) - \int_1^x A(t) f'(t) dt. \end{aligned}$$

Por el teorema 1.16. □

1.4 Algunas estimaciones básicas

Vamos a ver algunas aplicaciones de la teoría que hemos presentado, algunas de estas ya las habíamos mencionado antes, por ejemplo, el comportamiento asintótico de las sumas de la serie armónica.

Vamos a ver que $\sum_{n \leq x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right)$, donde $\gamma = \lim_{n \rightarrow \infty} \left(\sum_{n=1}^n \frac{1}{n} - \log n \right)$ conocida como la constante de Euler-Mascheroni.

Sea $a_n = 1$ y $f(x) = \frac{1}{x}$, así $A(x) = [x]$ y al usar la sumación parcial tenemos que

$$\begin{aligned} \sum_{n \leq x} \frac{1}{n} &= \frac{[x]}{x} + \int_1^x \frac{[t]}{t^2} dt \\ &= \frac{x - \{x\}}{x} + \int_1^x \frac{t - \{t\}}{t^2} dt. \end{aligned}$$

Donde $\{x\}$ denota la parte fraccionaria de x , es decir $\{x\} = x - [x]$, note que $\{x\} = O(1)$, luego

$$\begin{aligned} \sum_{n \leq x} \frac{1}{n} &= 1 + O\left(\frac{1}{x}\right) + \log x - \int_1^x \frac{\{t\}}{t^2} dt \\ &= 1 + O\left(\frac{1}{x}\right) + \log x - \left(\int_1^\infty \frac{\{t\}}{t^2} dt - \int_x^\infty \frac{\{t\}}{t^2} dt \right). \end{aligned}$$

Basta ver que $1 - \int_1^\infty \frac{\{x\}}{x^2} dx = \gamma$ ya que la otra integral también es del orden de $O\left(\frac{1}{x}\right)$, en efecto

$$\begin{aligned}
 \gamma &= \lim_{n \rightarrow \infty} \left(\sum_{k=1}^n \frac{1}{k} - \log n \right) \\
 &= \lim_{n \rightarrow \infty} \left(1 + \sum_{1 < k \leq n} \frac{1}{k} - \log n \right) \\
 &= 1 + \lim_{n \rightarrow \infty} \left(\int_1^n \frac{1}{x} d[x] - \int_1^n \frac{1}{x} dx \right) \\
 &= 1 + \lim_{n \rightarrow \infty} \left(\int_1^n \frac{[x]}{x^2} dx - \int_1^n \frac{1}{x} dx \right) \\
 &= 1 - \int_1^\infty \frac{\{x\}}{x^2} dx.
 \end{aligned}$$

Esto concluye el resultado que mencionamos en la introducción, $H(n) \sim \log n$. Veamos otro ejemplo:

Ejemplo. Estimación de las sumas parciales de $\log n$:

Sea $a_n = 1$ y $f(x) = \log x$, así $A(x) = [x]$, luego:

$$\begin{aligned}
 \sum_{n \leq x} \log n &= [x] \log x - \int_1^x \frac{[t]}{t} dt \\
 &= (x - O(1)) \log x - \int_1^x \frac{t - O(1)}{t} dt \\
 &= x \log x - O(\log x) - (x - 1) + O(\log x) \\
 &= x \log x - x + O(\log x).
 \end{aligned}$$

1.4.1. Una equivalencia importante

Vamos a obtener finalmente que el TNP es equivalente a la afirmación $\psi(x) \sim x$

Definición. Sea $x \in \mathbb{N}$, con $x > 1$, definimos la función contadora de primos $\pi(x)$ como:

$$\pi(x) = \sum_{p \leq x} 1.$$

Como vimos antes, la fórmula de sumación de Abel tiene un gran poder teórico que explotaremos en distintos lugares de este trabajo. Por lo pronto ella será esencial para para estimar $\vartheta(x)$ y $\pi(x)$, de donde obtendremos la equivalencia deseada.

Teorema 1.18. Dado $x \geq 2$

$$\begin{aligned}\vartheta(x) &= \pi(x) \log x - \int_2^x \frac{\pi(t)}{t} dt, \\ \pi(x) &= \frac{\vartheta(x)}{\log x} + \int_2^x \frac{\vartheta(t)}{t \log^2 t} dt.\end{aligned}$$

Demostración. Sea $\mathbb{1}_p$ la función característica del conjunto de primos. Tenemos entonces las siguientes igualdades:

$$\vartheta(x) = \sum_{n \leq x} \mathbb{1}_p(n) \log(n) \quad \text{y} \quad \pi(x) = \sum_{n \leq x} \mathbb{1}_p(n).$$

Fijemos $x \geq 2$. Por la fórmula de sumación de Abel y como $\pi(t) = 0$ para todo $t < 2$, tenemos que

$$\begin{aligned}\vartheta(x) &= \pi(x) \log(x) - \int_1^x \frac{\pi(t)}{t} dt \\ &= \pi(x) \log(x) - \int_2^x \frac{\pi(t)}{t} dt.\end{aligned}$$

Notando que $\pi(x) = \sum_{n \leq x} \frac{\mathbb{1}_p(n) \log(n)}{\log(n)}$ y que $\vartheta(t) = 0$ para todo $t < 2$ tenemos que

$$\begin{aligned}\pi(x) &= \frac{\vartheta(x)}{\log(x)} + \int_1^x \frac{\vartheta(t)}{t \log^2(t)} dt \\ &= \frac{\vartheta(x)}{\log(x)} + \int_2^x \frac{\vartheta(t)}{t \log^2(t)} dt.\end{aligned}$$

□

Ahora vamos a establecer una conexión entre las dos funciones de Chebyshev que definimos antes, en efecto

$$\psi(x) = \sum_{n \leq x} \Lambda(n) = \sum_{m=1}^{\infty} \sum_{p^m \leq x} \Lambda(p^m) = \sum_{m=1}^{\infty} \sum_{p \leq x^{\frac{1}{m}}} \log p.$$

Note que la suma sobre m realmente es finita porque la suma sobre p , se detiene cuando $x^{\frac{1}{m}} < 2$, es decir, cuando $m > \log_2(x)$, entonces

$$\psi(x) = \sum_{m \leq \log_2 x} \sum_{p \leq x^{\frac{1}{m}}} \log p = \sum_{m \leq \log_2 x} \vartheta\left(x^{\frac{1}{m}}\right). \quad (1.10)$$

Teorema 1.19. Si $x > 0$ se tiene que:

$$0 \leq \frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} \leq \frac{\log^2 x}{\sqrt{x} \log 4}.$$

Demostración. Por (1.10) se sigue que:

$$\psi(x) = \sum_{2 \leq m \leq \log_2 x} \vartheta\left(x^{\frac{1}{m}}\right) + \vartheta(x).$$

Ya que si $m = 1$ entonces $\vartheta(x^{\frac{1}{m}}) = \vartheta(x)$, luego

$$\psi(x) - \vartheta(x) = \sum_{2 \leq m \leq \log_2 x} \vartheta\left(x^{\frac{1}{m}}\right) \geq 0.$$

Ahora por definición de ϑ

$$\vartheta(x) = \sum_{p \leq x} \log p \leq x \log x.$$

Entonces

$$\begin{aligned} 0 \leq \psi(x) - \vartheta(x) &\leq \sum_{2 \leq m \leq \log_2 x} x^{\frac{1}{m}} \log x^{\frac{1}{m}} \\ &\leq \sqrt{x} \sum_{2 \leq m \leq \log_2 x} \log x^{\frac{1}{m}} \\ &\leq \sqrt{x} (\log_2(x) \log(\sqrt{x})) \\ &= \frac{\sqrt{x} \log^2 x}{\log(4)}. \end{aligned}$$

□

Teorema 1.20. La afirmación $\psi(x) \sim x$ es equivalente a $\vartheta(x) \sim x$.

Demostración. Por el teorema anterior:

$$0 \leq \frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} \leq \frac{\log^2(x)}{\sqrt{x} \log(4)}$$

y como $\lim_{x \rightarrow \infty} \frac{\log^2(x)}{\sqrt{x} \log(4)} = 0$, entonces cuando $x \rightarrow \infty$ se tiene que $\frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} = 0$, lo que concluye el resultado. □

Teorema 1.21. Las siguientes afirmaciones son equivalentes:

- i) $\pi(x) \sim \frac{x}{\log(x)}.$
- ii) $\vartheta(x) \sim x.$
- iii) $\psi(x) \sim x.$

Por el teorema anterior basta ver que i es equivalente a ii

Demostración. Por el teorema 1.18 y dado que estamos trabajando con aproximaciones asintóticas, podemos asumir que $x \geq 2$, se sigue que

$$\frac{\vartheta(x)}{x} = \frac{\pi(x) \log(x)}{x} - \frac{1}{x} \int_2^x \frac{\pi(t)}{t} dt. \quad (1.11)$$

$$\frac{\pi(x) \log(x)}{x} = \frac{\vartheta(x)}{x} + \frac{\log(x)}{x} \int_2^x \frac{\vartheta(t)}{t \log^2(t)} dt. \quad (1.12)$$

Basta con ver que las integrales de (1.11) y (1.12) van a 0, cuando $x \rightarrow \infty$.

(\rightarrow) Por hipótesis $\frac{\pi(x)}{x} \left(\frac{1}{\log(x)} \right)^{-1} = 1$ cuando $x \rightarrow \infty$. Esto es equivalente a decir que $\frac{\pi(t)}{t} = O\left(\frac{1}{\log(t)}\right)$. Luego para todo $x \geq 2$ positivo fijo tenemos que

$$\frac{1}{x} \int_2^x \frac{\pi(t)}{t} dt = O\left(\frac{1}{x} \int_2^x \frac{1}{\log(t)} dt\right).$$

Note que

$$\begin{aligned} \int_2^x \frac{1}{\log(t)} dt &\leq \int_2^{\sqrt{x}} \frac{1}{\log(t)} dt + \int_{\sqrt{x}}^x \frac{1}{\log(t)} dt \\ &\leq \frac{\sqrt{x}}{\log(2)} + \frac{x - \sqrt{x}}{\log(\sqrt{x})}, \end{aligned}$$

luego

$$\frac{1}{x} \int_2^x \frac{1}{\log(t)} dt \leq \frac{1}{\sqrt{x} \log(2)} + \frac{1}{\log(\sqrt{x})} - \frac{1}{\sqrt{x} \log(\sqrt{x})},$$

así, cuando $x \rightarrow \infty$, $\frac{1}{x} \int_2^x \frac{1}{\log(t)} dt = 0$.

(\leftarrow) Análogamente $\vartheta(t) = O(t)$. Por tanto

$$\frac{\log(x)}{x} \int_2^x \frac{\vartheta(t)}{t \log^2(t)} dt = O\left(\frac{\log(x)}{x} \int_2^x \frac{1}{t \log^2(t)} dt\right),$$

La integral en O se puede acotar de manera análoga a la anterior:

$$\begin{aligned} \int_2^x \frac{1}{t \log^2(t)} dt &= \int_2^{\sqrt{x}} \frac{1}{t \log^2(t)} dt + \int_{\sqrt{x}}^x \frac{1}{t \log^2(t)} dt \\ &\leq \frac{\sqrt{x}}{\log^2(2)} + \frac{x - \sqrt{x}}{\log^2(\sqrt{x})}. \end{aligned}$$

Multiplicando ambos lados por $\frac{\log(x)}{x}$, podemos ver que si $x \rightarrow \infty$, $\frac{\log(x)}{x} \int_2^x \frac{1}{t \log^2(t)} dt = 0$. □

Finalizaremos con una aplicación interesante de la fórmula de sumación de Abel:

Proposición 1.22 (Fórmula de Stirling). Si n es un entero positivo, entonces

$$n! = C\sqrt{n}n^n e^{-n} \left(1 + O\left(\frac{1}{n}\right)\right).$$

Demostración. Por el teorema 1.17:

$$\begin{aligned} \sum_{k \leq n} \log k &= n \log n - n + 1 + \int_1^n \frac{\{t\}}{t} dt \\ &= n \log n - n + 1 + \frac{1}{2} \log n + \int_1^n \frac{s(t)}{t} dt, \end{aligned}$$

donde $s(t) = \{t\} - \frac{1}{2}$, note que aplicando integración por partes

$$\int_1^n \frac{s(t)}{t} dt = \frac{S(t)}{t} \Big|_1^n + \int_1^n \frac{S(t)}{t^2} dt,$$

donde $S(t) = \int_1^t s(y) dy$, tenemos que $\frac{S(t)}{t} \Big|_1^n = 0$ ya que $s(t)$ es una función periódica de periodo 1 y $\int_k^{k+1} s(t) dt = 0$ para todo entero k . Note que $|S(t)| \leq \frac{1}{2}$, de esto se sigue que

$$\begin{aligned} \int_1^n \frac{s(t)}{t} dt &= \int_1^n \frac{S(t)}{t^2} dt = \int_1^\infty \frac{S(t)}{t^2} dt - \int_n^\infty \frac{S(t)}{t^2} dt \\ &= c + O\left(\frac{1}{n}\right). \end{aligned} \quad \left(|S(t)| \leq \frac{1}{2}\right)$$

Por tanto:

$$\sum_{k \leq n} \log k = n \log n - n + \frac{1}{2} \log n + c + O\left(\frac{1}{n}\right),$$

en efecto

$$\begin{aligned} n! &= \exp\left(\sum_{k \leq n} \log k\right) \\ &= \exp\left(n \log n - n + \frac{1}{2} \log n + c + O\left(\frac{1}{n}\right)\right) \\ &= C\sqrt{n}n^n e^{-n} \left(1 + O\left(\frac{1}{n}\right)\right). \end{aligned}$$

□

Se puede ver que $C = \sqrt{2\pi}$, sin embargo no abordaremos eso en este trabajo.

1.5 Series de Dirichlet

Dada una función aritmética f , se le pueden asignar a esta dos tipos de series importantes:

$$E(z) = \sum_{n=1}^{\infty} f(n)z^n,$$

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

estas son llamadas funciones generatrices de f . Las series de potencia generatrices fueron introducidas por Euler con el propósito de estudiar problemas de naturaleza aditiva, esto ya que tienen la siguiente propiedad:

$$E_f(z)E_g(z) = \sum_{n=1}^{\infty} h(n)z^n,$$

donde

$$h(n) = \sum_{a+b=n} f(a)g(b).$$

Note que $h(n)$ se parece la convolución de Dirichlet, pero en una versión aditiva, por eso estas series toman un papel importante para este tipo de problemas.

Sin embargo, nuestro interés son las series $F(s)$, estas fueron introducidas por Dirichlet en su trabajo sobre primos en progresiones aritmética y son particularmente útiles cuando f es una función multiplicativa ya que entre muchas cosas, en el producto de dos de estas aparece la convolución multiplicativa que vimos antes, por lo que a través de estas podemos obtener propiedades de $f(n)$ como en la sección 1.2.

Con lo que se mencionó antes parece que toda la teoría se conecta, y que de cierta forma esto solo es una forma diferente de atacar los mismos problemas, sin embargo, este no es el caso, las propiedades analíticas de una serie de Dirichlet, vista como función de variable compleja s pueden ser explotadas para obtener información importante acerca del comportamiento de las sumas parciales de funciones aritmética

$$\sum_{n \leq x} f(n).$$

Definición. Sea f una función aritmética, la serie

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

es llamada *serie de Dirichlet asociada a f* .

La variable s es usualmente escrita como $s = \sigma + it$ con $\sigma = \Re(s)$ y $t = \Im(s)$, la serie de Dirichlet más popular es la función zeta de Riemann $\zeta(s)$, definida como la serie de Dirichlet asociada a la constante 1:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \quad (\sigma > 1)$$

1.5.1. Propiedades algebraicas

Teorema 1.23. Sean f y g las funciones aritmética asociadas a $F(s)$ y $G(s)$. Sea $h = f * g$ la convolución de f y g y $H(s)$ su serie de Dirichlet asociada. Si $F(s)$ y $G(s)$ convergen absolutamente en algún punto s , entonces también $H(s)$ y $H(s) = F(s)G(s)$.

Demostración. Note que por la convergencia absoluta:

$$\begin{aligned} F(s)G(s) &= \sum_{k=1}^{\infty} \frac{f(k)}{k^s} \sum_{m=1}^{\infty} \frac{g(m)}{m^s} \\ &= \sum_{k=1}^{\infty} \sum_{m=1}^{\infty} \frac{f(k)g(m)}{k^s m^s} \\ &= \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{km=n} f(k)g(m) = \sum_{n=1}^{\infty} \frac{f * g(n)}{n^s}, \end{aligned}$$

además:

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

□

Es muy importante tener en cuenta que esto no se puede garantizar sin la convergencia absoluta, ya que los reordenamientos que realizamos en la prueba no son posibles.

Corolario 1.24. Sean f una función aritmética con serie de Dirichlet asociada $F(s)$, g tal que $f * g = e$ y $G(s)$ la serie de Dirichlet asociada a g , entonces $G(s) = \frac{1}{F(s)}$ en cualquier punto s en el que $F(s)$ y $G(s)$ sean ambas absolutamente convergentes.

Demostración. Note que la serie de Dirichlet asociada a e es 1, luego por el teorema anterior:

$$1 = \sum_{n=1}^{\infty} \frac{e(n)}{n^s} = \sum_{n=1}^{\infty} \frac{f * g(n)}{n^s} = F(s)G(s).$$

□

Nota. La convergencia absoluta de $F(s)$ no implica la de la serie de Dirichlet asociada con su inversa. Por ejemplo, la función definida por $f(1) = 1$, $f(2) = -1$, y $f(n) = 0$ para $n \geq 3$ tiene la serie de Dirichlet $F(s) = 1 - 2^{-s}$, que converge para todo s . Sin embargo, la serie de Dirichlet de la inversa de Dirichlet de f es $\frac{1}{F(s)} = (1 - 2^{-s})^{-1} = \sum_{k=0}^{\infty} 2^{ks}$, que converge absolutamente en $\sigma > 0$, pero no en el semiplano $\sigma \leq 0$, ya que es una serie geométrica. [2]

Si tomamos una serie de potencias $F(x)$, sabemos por lo menos tres cosas de ella:

- F tiene un disco de convergencia,
- En el interior del disco, F converge absolutamente.
- En el interior del disco, F es una función analítica [4]

Nuestro objetivo ahora es lograr obtener propiedades similares para series de Dirichlet.

1.5.2. Propiedades analíticas

Primero note que $x^s = e^{s \log x} = e^{(\sigma + it) \log x} = x^\sigma e^{it \log x}$, por tanto $|x^s| = |x^\sigma|$ ya que:

$$\begin{aligned} |e^{it\theta}| &= |\cos(\theta) + i \sin(\theta)| \\ &= 1. \end{aligned}$$

luego $|e^{it \log x}| = 1$. Esto muestra que la convergencia absoluta de una serie de Dirichlet está determinada únicamente por σ .

Ejemplo (Convergencia de $\zeta(s)$). Note que

$$\sum_{n=1}^{\infty} \left| \frac{1}{n^s} \right| = \sum_{n=1}^{\infty} \left| \frac{1}{n^\sigma} \right| = \sum_{n=1}^{\infty} \frac{1}{n^\sigma}.$$

Si $\sigma = 1$ sabemos que la serie diverge, en otro caso, la serie converge si y solo si la integral:

$$\int_1^{\infty} \frac{1}{x^\sigma} dx = \lim_{n \rightarrow \infty} \left. \frac{x^{1-\sigma}}{1-\sigma} \right|_1^n = \lim_{n \rightarrow \infty} \frac{n^{1-\sigma}}{1-\sigma} - \frac{1}{1-\sigma}.$$

Luego, es claro que $\zeta(s)$ converge absolutamente si $\sigma > 1$ y diverge si $\sigma \leq 1$.

Definición. Sea Ω un abierto en \mathbb{C} y $f : \Omega \rightarrow \mathbb{C}$, la *derivada* de f en $z_0 \in \Omega$ está dada por

$$f'(z_0) = \lim_{z \rightarrow z_0} \frac{f(z) - f(z_0)}{z - z_0}$$

Si el límite existe. Diremos que f es *diferenciable* en z_0 .

Si f es diferenciable en todo punto de una vecindad de z_0 , entonces diremos que f es *holomorfa* en z_0 . Si f es holomorfa en todo punto de un abierto $U \subseteq \Omega$, diremos que f es holomorfa en U . Finalmente si f es holomorfa en Ω , diremos que es holomorfa.

Por otro lado, f se dice *analítica* en z_0 , si existe un abierto $U \subseteq \Omega$ tal que $z_0 \in U$ y

$$f(z) = \sum_{n=0}^{\infty} a_n (z - z_0)^n,$$

para todo $z \in U$, si f es analítica en todo punto de U , entonces decimos que es analítica en U .

El conjunto de puntos $s = \sigma + it$ con $\sigma > \alpha$ es llamado *semiplano*, veremos que toda serie de Dirichlet tiene un semiplano $\sigma > \sigma_c$ en el que la serie converge y otro semiplano $\sigma > \sigma_a$ en el que la serie converge absolutamente. Las constantes σ_c y σ_a son llamadas *abscisa de convergencia* y *abscisa de convergencia absoluta* respectivamente. Si la serie de Dirichlet converge para todo $s \in \mathbb{C}$, decimos que $\sigma_c = -\infty$, si no converge para todo $s \in \mathbb{C}$, decimos que $\sigma_c = \infty$, de manera análoga lo haremos con la convergencia absoluta.[5]

Teorema 1.25. Sea $f : \mathbb{N} \rightarrow \mathbb{C}$, supongamos que la serie

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

no converge, ni diverge para todo $s \in \mathbb{C}$, entonces existe un $\sigma_a \in \mathbb{R}$ tal que $F(s)$ converge para todo $\sigma > \sigma_a$ y diverge para todo $\sigma < \sigma_a$

Demostración. Sea $|n^s| = n^\sigma$, si $\sigma > \sigma_0$, entonces $|n^s| \geq n^{\sigma_0}$, así $|f(n)n^{-s}| \leq |f(n)|n^{-\sigma_0}$. Por el criterio de comparación, si $F(s)$ converge para $s = \sigma_0 + it_0$, entonces converge para todo s con parte real $\sigma \geq \sigma_0$. Considere el conjunto

$$A : \left\{ \alpha \in \mathbb{R} : \sum_{n=1}^{\infty} \left| \frac{f(n)}{n^\alpha} \right| < \infty \right\}.$$

Como $F(s)$ no diverge para todo $s \in \mathbb{C}$, entonces A es no vacío, además tiene un mínimo ya que $F(s)$ no converge para todo $s \in \mathbb{C}$, sea σ_a el mínimo de A . Si $s \in \mathbb{C}$ tiene parte real $\sigma < \sigma_a$, entonces $\sigma \notin A$, $F(s)$ diverge. Análogamente si s tiene parte real $\sigma > \sigma_a$, entonces $\sigma > \alpha$ para algún $\alpha \in A$, $F(s)$ converge.

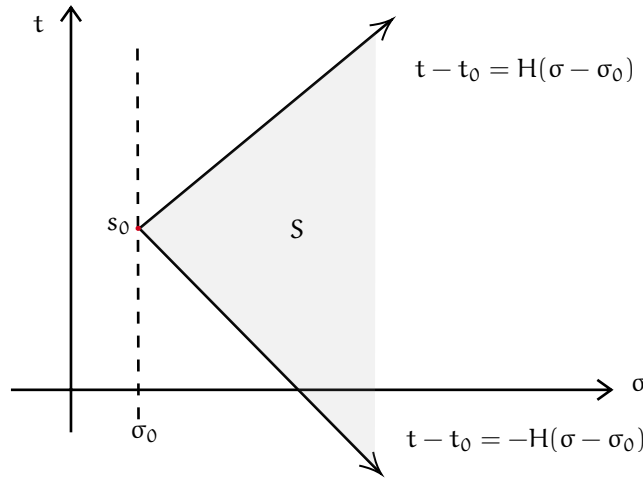
□

Teorema 1.26. Sean Ω un abierto en \mathbb{C} , (f_n) una sucesión de funciones analíticas definidas en Ω , y $f : \Omega \rightarrow \mathbb{C}$. Si (f_n) converge absolutamente a f en cualquier subconjunto compacto de Ω , entonces f es analítica en Ω y la sucesión (f'_n) también converge uniformemente a f' en cualquier subconjunto compacto de Ω .

No entraremos en los detalles de esta prueba aquí, el lector interesado la puede consultar en [6].

Teorema 1.27. Suponga que la serie $F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ converge en el punto $s = s_0$ y sea $H > 0$, entonces $F(s)$ converge uniformemente en S , donde S es el conjunto:

$$S = \{s \in \mathbb{C} : \sigma > \sigma_0 \text{ y } |t - t_0| \leq H(\sigma - \sigma_0)\}.$$



Demostración. Sean $H > 0$, $\varepsilon > 0$ dado y $1 < M < N$, como la serie converge en $s = s_0$, entonces

$$\sum_{M < n \leq N} f(n)n^{-s_0}n^{s_0-s} = \int_M^N t^{s_0-s} dA(t) = \int_M^N t^{s_0-s} d(A(t) - A(M)),$$

con $A(t) = \sum_{n \leq t} f(n)n^{-s_0}$, luego

$$\begin{aligned} \sum_{M < n \leq N} f(n)n^{-s} &= \frac{A(N) - A(M)}{N^{s-s_0}} - \int_M^N (A(t) - A(M)) d(t^{s_0-s}) \\ &= \frac{A(N) - A(M)}{N^{s-s_0}} - (s_0 - s) \int_M^N (A(t) - A(M)) t^{s_0-s-1} dt. \end{aligned}$$

Tenemos que $A(t)$ converge cuando $t \rightarrow \infty$, luego $A(N) - A(M)$ y $A(t) - A(M)$ convergen a 0 cuando $M, N \rightarrow \infty$. Así, para M, N suficientemente grandes y $\sigma > \sigma_0$

$$|A(N) - A(M)| < \frac{\varepsilon}{(H+2)}, \quad |A(t) - A(M)| < \frac{\varepsilon}{H+2},$$

de esto se sigue que:

$$\begin{aligned} \left| \sum_{M < n \leq N} \frac{f(n)}{n^s} \right| &< \frac{\varepsilon}{H+2} + \frac{\varepsilon}{H+2} |s - s_0| \int_M^\infty t^{\sigma_0 - \sigma - 1} dt \\ &= \frac{\varepsilon}{H+2} + \frac{\varepsilon |s - s_0|}{(H+2)(\sigma - \sigma_0) M^{\sigma - \sigma_0}} \\ &\leq \left(1 + \frac{|s - s_0|}{\sigma - \sigma_0} \right) \frac{\varepsilon}{H+2}. \end{aligned}$$

Queremos ver que $\left| \sum_{M < n \leq N} f(n)n^{-s} \right| < \varepsilon$, así el teorema se sigue de el teorema de Cauchy para convergencia uniforme de series, en efecto

$$|s - s_0| = |(\sigma - \sigma_0) + i(t - t_0)| \leq \sigma - \sigma_0 + |t - t_0| \leq \sigma - \sigma_0 + H(\sigma - \sigma_0) \leq (H+1)(\sigma - \sigma_0),$$

así:

$$\left| \sum_{M < n \leq N} \frac{f(n)}{n^s} \right| < (1 + (H+1)) \frac{\varepsilon}{H+2} = \varepsilon.$$

□

Note que haciendo H suficientemente grande obtenemos que $F(s)$ converge para todo s en el semiplano $\sigma > \sigma_0$, geométicamente lo que hacemos es abrir el cono de la región S para obtener este semiplano.[7]

Teorema 1.28. Supongamos que $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ no converge para todo $s \in \mathbb{C}$ ni diverge para todo $s \in \mathbb{C}$, entonces existe $\sigma_c \in \mathbb{R}$ tal que $F(s)$ converge para todo s con $\sigma > \sigma_0$ y diverge para todo $\sigma < \sigma_0$.

Demostración. Como mencionamos antes, tomando H suficientemente grande vemos que si $F(s)$ converge en $s = s_0$, entonces por el teorema anterior $F(s)$ converge para todo $\sigma > \sigma_0$, por tanto, de manera análoga a la prueba del teorema 1.25, consideremos el conjunto:

$$A = \left\{ \alpha \in \mathbb{R} : \sum_{n=1}^{\infty} f(n)n^{-\alpha} \text{ converge} \right\}.$$

Nuevamente consideremos σ_c el mínimo de A , si s tiene parte real $\sigma > \sigma_c$, entonces $\sigma > \alpha$ para algún $\alpha \in A$, luego $F(s)$ converge, si s tiene parte real $\sigma < \sigma_c$, entonces $\sigma < \frac{\sigma + \sigma_c}{2} < \sigma_c$ y como σ_c es el mínimo, $\frac{\sigma + \sigma_c}{2} \notin A$, lo que implica que $F(s)$ diverge. □

Ejemplo. Supongamos que la suma

$$\sum_{n \leq x} f(n) \text{ está acotada para todo } x \in [1, \infty).$$

Tenemos que n^{-s} para $\sigma > 0$ es decreciente, luego dado $\sigma_0 > 0$, tenemos que $\sum_{n=1}^{\infty} f(n)n^{-\sigma_0}$ converge por el criterio de Dirichlet y por el teorema anterior $F(s)$ converge para todo s con $\sigma > \sigma_0$, haciendo σ_0 arbitrariamente pequeño, obtenemos que $F(s)$ converge en el semiplano $\sigma > 0$.

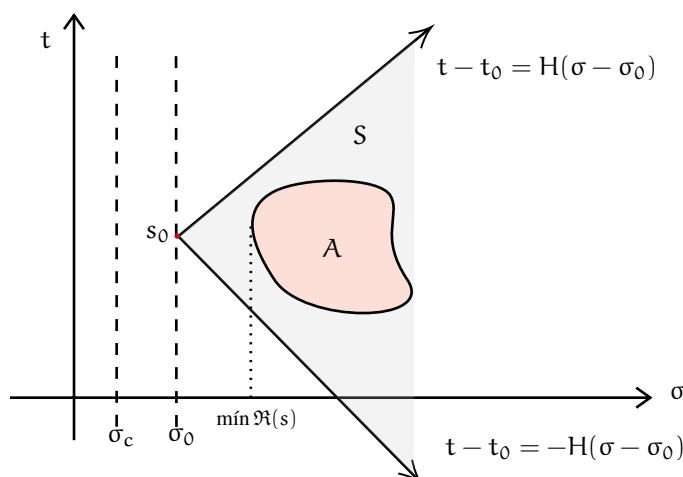
El siguiente resultado nos da una propiedad que esperábamos, podemos derivar término a término:

Corolario 1.29. Sea $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ para todo $s \in \mathbb{C}$ con $\sigma > \sigma_c$, entonces $F(s)$ es analítica en el semiplano $\sigma > \sigma_c$ y $F'(s)$ se puede obtener derivando término a término, es decir:

$$F'(s) = - \sum_{n=1}^{\infty} \frac{f(n) \log n}{n^s} \quad \text{para todo } s \text{ con } \sigma > \sigma_c.$$

Demostración. Sea A un compacto en el semiplano $\sigma > \sigma_c$, tomemos s_0 con parte real σ_0 tal que $\sigma_c < \sigma_0 < \min\{\Re(s) : s \in A\}$, como $F(s)$ converge en s_0 , entonces por el Teorema 1.27, $F(s)$ converge uniformemente en la región $S = \{s \in \mathbb{C} : \sigma > \sigma_0 \text{ y } |t - t_0| \leq H(\sigma - \sigma_0)\}$. Sabemos que A es acotado porque es compacto, luego existe un $H > 0$ tal que $A \subset S$, basta tomar un H suficientemente grande. De esto se sigue que $F(s)$ converge uniformemente en cualquier compacto A del semiplano $\sigma > \sigma_c$, por el Teorema 1.26, $F(s)$ es analítica en el semiplano $\sigma > \sigma_0$, $F'(s)$ se puede obtener derivando término a término:

$$F'(s) = - \sum_{n=1}^{\infty} f(n)(\log n)n^{-s}.$$



□

Nota. Por lo anterior, $F'(s)$ tiene la misma abscisa de convergencia que $F(s)$, note que el corolario anterior también se tiene si consideramos s en el semiplano de convergencia absoluta, la prueba es exactamente la misma, resaltamos esto porque además nos dice que $F'(s)$ tiene la misma abscisa de convergencia absoluta que $F(s)$, esto nos será útil después.[8]

Corolario 1.30. La función zeta de Riemann es analítica en el semiplano $\sigma > 1$. Luego

$$\zeta'(s) = - \sum_{n=1}^{\infty} \frac{\log n}{n^s} \text{ para todo } s \in \mathbb{C} \text{ con } \sigma > 1.$$

Recordemos que el TFA en términos de convolución nos dice que $\log n = \Lambda * 1$, por tanto

$$\zeta'(s) = - \sum_{n=1}^{\infty} \frac{\log n}{n^s} = - \sum_{n=1}^{\infty} \frac{\Lambda * 1(n)}{n^s} = - \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} \sum_{k=1}^{\infty} \frac{1}{k^s}.$$

El paso anterior, en el que separamos la convolución como un producto depende de que ambas series sean absolutamente convergentes en el punto s . No tenemos de momento una abscisa de convergencia absoluta para la serie de Dirichlet asociada a la función de Von Mangolth, Afortunadamente, no es difícil ver que también $\sigma_a = 1$. Note que para todo $n \in \mathbb{N}$, $|\Lambda(n)| \leq \log n$ y como la serie de Dirichlet de $\log(n)$ es $-\zeta'(s)$ que tiene abscisa de convergencia absoluta $\sigma_a = 1$, entonces

$$\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} \text{ converge absolutamente si } \sigma > 1.$$

El paso que hicimos es válido en el semiplano $\sigma > 1$, por tanto:

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

Esta es la derivada logarítmica de $\zeta(s)$, una serie de Dirichlet que será muy importante en la prueba del teorema de los números primos. El siguiente teorema nos da una relación importante entre σ_c y σ_a .

Teorema 1.31. Sea $F(s)$ una serie de Dirichlet, entonces $\sigma_c \leq \sigma_a \leq \sigma_c + 1$

Demostración. Es claro que si $F(s)$ es absolutamente convergente, entonces $\sigma_a \geq \sigma_c$, veamos la otra desigualdad. Note que la serie $\sum_{n=1}^{\infty} f(n)n^{-\sigma_c-\varepsilon}$ converge para todo $\varepsilon > 0$, por tanto $f(n)n^{-\sigma_c-\varepsilon}$ converge a 0 cuando $n \rightarrow \infty$. Es decir, existe un $N > 0$ tal que $|f(n)| < n^{\sigma_c+\varepsilon}$ para todo $n \geq N$, luego

$$\left| \frac{f(n)}{n^{\sigma+1+2\varepsilon}} \right| < \frac{1}{n^{1+\varepsilon}}.$$

Tenemos que la serie $\sum_{n=1}^{\infty} n^{-1-\varepsilon}$ converge, luego por criterio de comparación, la serie

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^{\sigma_c+2\varepsilon+1}} \quad \text{converge absolutamente,}$$

esto es, $\sigma_a \leq \sigma_c + 1 + 2\varepsilon$, para todo $\varepsilon > 0$, luego obtenemos $\sigma_a \leq \sigma_c + 1$. \square

Teorema 1.32 (Unicidad). Sean $F(s)$ y $G(s)$ las series de Dirichlet asociadas a f y g respectivamente, si $F(s)$ y $G(s)$ tienen abscisa de convergencia finita y además $F(s) = G(s)$ para todo s con σ suficientemente grande. Entonces $f(n) = g(n)$.

Demostración. Sea $h(n) = f(n) - g(n)$ y $H(s) = F(s) - G(s)$ su serie de Dirichlet, por hipótesis, existe un σ_0 tal que $H(s)$ converge en el semiplano $\sigma > \sigma_0$ y $H(s)$ es idénticamente nula en este semiplano, queremos ver que $h(n) = 0$ para todo $n \in \mathbb{N}$. Supongamos que $h(n)$ no es idénticamente nula y sea N el mínimo entero positivo tal que $h(n) \neq 0$, entonces

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

$$h(N) = N^s H(s) - N^s \sum_{n=N+1}^{\infty} h(n)n^{-s}.$$

De esto se sigue que para todo $\sigma > \sigma_0$, $h(N) = -N^\sigma \sum_{n=N+1}^{\infty} h(n)n^{-\sigma}$. y por tanto

$$|h(N)| \leq \sum_{n=N+1}^{\infty} |h(n)| \left(\frac{N}{n}\right)^\sigma,$$

tomando $\sigma = \sigma_0 + \lambda$ con $\lambda \geq 0$, tenemos que para todo $n \geq N+1$

$$\left(\frac{N}{n}\right)^\sigma = \left(\frac{N}{n}\right)^\lambda \left(\frac{N}{n}\right)^{\sigma_0} \leq \left(\frac{N}{N+1}\right)^\lambda \left(\frac{N}{n}\right)^{\sigma_0},$$

luego:

$$|h(N)| \leq \left(\frac{N}{N+1}\right)^\lambda \sum_{n=N+1}^{\infty} |h(n)| \left(\frac{N}{n}\right)^{\sigma_0} = N^{\sigma_0} \left(\frac{N}{N+1}\right)^\lambda \sum_{n=N+1}^{\infty} |h(n)| n^{-\sigma_0}$$

$$= C \left(\frac{N}{N+1}\right)^\lambda,$$

donde C es una constante que no depende de λ dado que la serie $\sum_{n=N+1}^{\infty} |h(n)| n^{-\sigma_0}$ converge.

Note que

$$\lim_{\lambda \rightarrow \infty} C \left(\frac{N}{N+1} \right)^\lambda = 0.$$

Luego $h(N) = 0$, contradicción. $f(n) = g(n)$ para todo $n \in \mathbb{N}$. □

Con estas propiedades nos basta para lo que queremos mostrar en este trabajo, sin embargo hay muchas otras propiedades analíticas de las series de Dirichlet que son útiles en otros contextos y además muy interesantes, algunas fuentes en las que se pueden consultar son [8] y [7].

1.5.3. El producto de Euler

Ya habíamos mencionado antes que las series de Dirichlet son particularmente útiles cuando f es una función multiplicativa, ya que en este caso vemos a ver que

$$F(s) = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \frac{f(p^3)}{p^{3s}} + \cdots \right),$$

siempre que las series sobre los primos y el producto converjan absolutamente. Adicionalmente, si f es completamente multiplicativa

$$F(s) = \prod_p (1 - f(p))^{-1}.$$

Este resultado es llamado producto de Euler, curiosamente no porque Euler lo haya demostrado, sino porque el primer resultado de este estilo fue dado por Euler, para la función $\zeta(s)$, $s > 1$. Como sabemos, este resultado es muy importante para poder probar la divergencia de la serie de los recíprocos de los números primos, por lo que requerimos la versión general para poder presentar una prueba del teorema de Dirichlet en nuestro siguiente capítulo.

Para este punto debemos asumir algunos resultados de convergencia de productos infinitos, resultados que son bien conocidos, sin embargo, vamos a recordarlos por completitud. Dicho esto no presentaremos pruebas, estos resultados se estudian bien a detalle en [4], allí se encuentran pruebas detalladas y el lector interesado puede consultarlas.

Definición. Decimos que el producto $\prod_{n=1}^{\infty} a_n$ converge si:

- Existe $k \in \mathbb{N}$ tal que $a_n \neq 0$ para todo $n \geq k$ y
- $\lim_{m \rightarrow \infty} \prod_{n=k}^m a_n$ existe y es no nulo.

De la definición anterior tenemos que un producto $\prod_{n=1}^{\infty} a_n$ converge a 0 si y solo si existe

un n tal que $a_n = 0$ y hay solo una cantidad finita de a_n de esta forma, así tomando $N = \max\{n : a_n = 0\}$ el $\lim_{m \rightarrow \infty} \prod_{k=N+1}^m a_k$ existe y es no nulo. Por ejemplo, el producto

$$(0)(1)(1)(1)(1) \cdots \text{ converge a } 0,$$

pero los productos $(0)(1)(0)(1)(0)(1) \cdots$ y $(0)(1)(2)(3)(4) \cdots$ no convergen [5]. De manera análoga a lo que ocurre con series, si el producto $\prod_{n=1}^{\infty} a_n$ converge, entonces a_n converge a 1. Nos interesa caracterizar la convergencia de los productos de la forma $\prod_{n=1}^{\infty} (1 + a_n)$, note que por lo anterior a_n converge a 0.

Definición. Sea a_n una sucesión de números complejos. El producto $\prod_{n=1}^{\infty} (1 + a_n)$ es absolutamente convergente si $\prod_{n=1}^{\infty} (1 + |a_n|)$ es convergente.

En productos infinitos también la convergencia absoluta implica convergencia.

Teorema 1.33. Si la serie $\sum_{n=1}^{\infty} |a_n|$ converge, entonces el producto $\prod_{n=1}^{\infty} (1 + |a_n|)$ converge.

Como mencionamos, no se presentará una prueba de este resultado, el lector puede consultarla en [4].

Teorema 1.34. Sea f una función aritmética multiplicativa si $\sum_{n=1}^{\infty} f(n)$ converge absolutamente, entonces

$$\sum_{n=1}^{\infty} f(n) = \prod_p (1 + f(p) + f(p^2) + \cdots).$$

Si f es completamente multiplicativa, entonces

$$\sum_{n=1}^{\infty} f(n) = \prod_p (1 - f(p))^{-1}.$$

Demostración. Note que:

$$\sum_p |f(p) + f(p^2) + \cdots| \leq \sum_p |f(p)| + \sum_p |f(p^2)| + \cdots \leq \sum_{n=2}^{\infty} |f(n)|. \quad (1.13)$$

La serie en la derecha de (1.13) converge, entonces $\prod_p (1 + f(p) + f(p^2) + \dots)$ converge absolutamente. Como f es multiplicativa tenemos que

$$\begin{aligned}
 P(x) &= \prod_{p \leq x} (1 + f(p) + f(p^2) + \dots) = \prod_{p \leq x} \left(1 + \sum_{k=1}^{\infty} f(p^k) \right) \\
 &= 1 + \sum_{k_1=1}^{\infty} f(p_1^{k_1}) + \sum_{k_2=1}^{\infty} f(p_2^{k_2}) + \sum_{k_1=1}^{\infty} f(p_1^{k_1}) \sum_{k_2=1}^{\infty} f(p_2^{k_2}) + \dots \\
 &= \sum_{k_1=0}^{\infty} \dots \sum_{k_t=0}^{\infty} (f(p_1^{k_1}) \dots f(p_t^{k_t})) \\
 &= \sum_{k_1=0}^{\infty} \dots \sum_{k_t=0}^{\infty} (f(p_1^{k_1} \dots p_t^{k_t})).
 \end{aligned} \tag{1.14}$$

En efecto podemos obtener el término 1 tomando $k_1 = k_2 = \dots = k_t = 0$ ya que $f(1) = 1$ porque f es multiplicativa. Note ahora que dado el conjunto A de los enteros positivos con todos sus factores primos menores o iguales a x , el producto se puede escribir de manera compacta como

$$P(x) = \sum_{n \in A} f(n),$$

luego, dado B el conjunto de los enteros positivos con al menos un factor primo mayor que x

$$\left| \sum_{n=1}^{\infty} f(n) - P(x) \right| \leq \sum_{n \in B} |f(n)| \leq \sum_{n > x} |f(n)| = \sum_{n=1}^{\infty} |f(n)| - \sum_{n \leq x} |f(n)|.$$

Lo que converge a 0 cuando $x \rightarrow \infty$, luego $P(x)$ converge a $\sum_{n=1}^{\infty} f(n)$ cuando $x \rightarrow \infty$. Si f es completamente multiplicativa, $f(p^k) = f(p)^k$, aplicando esto a (1.14) obtenemos lo deseado:

$$P(x) = \prod_p (1 + f(p) + (f(p))^2 + (f(p))^3 + \dots) = \prod_p (1 - f(p))^{-1},$$

ya que las series $\sum_{k=0}^{\infty} f(p_t^k)$ en (1.14) se vuelven geométricas, cada una convergiendo a $(1 - f(p_t))^{-1}$, $|f(p_t)| < 1$, luego

$$\sum_{n=1}^{\infty} f(n) = \prod_{n=1}^{\infty} (1 - f(p))^{-1}.$$

□

Corolario 1.35 (Producto de Euler). Sea f una función aritmética y $F(s)$ su serie de Dirichlet, supongamos que $F(s)$ converge absolutamente para $\sigma > \sigma_a$. Si f es multiplicativa

$$\sum_{n=1}^{\infty} f(n)n^{-s} = \prod_p (1 + f(p)p^{-s} + f(p^2)p^{-2s} + \dots).$$

Si f es completamente multiplicativa

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

y cada producto es absolutamente convergente para $\sigma > \sigma_a$.

La prueba es esencialmente trivial, basta considerar

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

y aplicar el teorema anterior a f_s , note que si f es multiplicativa o completamente multiplicativa, también f_s .

Corolario 1.36. Sea $s \in \mathbb{C}$ tal que $\sigma > 1$, entonces

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

Observemos lo siguiente

$$\begin{aligned} \frac{1}{\zeta(s)} &= \prod_p \left(1 - \frac{1}{p^s}\right) \\ &= \left(1 - \frac{1}{2^s}\right) \left(1 - \frac{1}{3^s}\right) \left(1 - \frac{1}{5^s}\right) \dots \\ &= 1 - \sum_p p^{-s} + \sum_{\substack{p,q \\ p \neq q}} p^{-s} q^{-s} - \dots \\ &= \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}. \end{aligned}$$

Hemos probado unicidad en series de Dirichlet, esto nos permite obtener una prueba alternativa de $\mu * 1 = e$. En efecto

$$\sum_{n=1}^{\infty} \frac{e(n)}{n^s} = 1 = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \zeta(s) = \sum_{n=1}^{\infty} \frac{\mu * 1(n)}{n^s}.$$

Otro ejemplo de esto es:

$$\begin{aligned}
\frac{\zeta(s-1)}{\zeta(s)} &= \prod_p \frac{(1-p^{-s})}{(1-p^{-s+1})} \\
&= \prod_p \left(1 - \frac{1}{p^s}\right) \left(\sum_{k=0}^{\infty} \frac{p^k}{p^{ks}}\right) \\
&= \prod_p \left(1 - \frac{1}{p^s}\right) \left[1 + \frac{p}{p^s} + \frac{p^2}{p^{2s}} + \dots\right] \\
&= \prod_p \left(\left[1 + \frac{p}{p^s} + \frac{p^2}{p^{2s}} + \dots\right] - \left[\frac{1}{p^s} + \frac{p}{p^{2s}} + \frac{p^2}{p^{3s}} + \dots\right]\right) \\
&= \prod_p \left[1 + \left(1 - \frac{1}{p}\right) \left(\frac{p}{p^s} + \frac{p^2}{p^{2s}} + \dots\right)\right] \\
&= \prod_p \left[1 + \frac{p-1}{p^s} + \frac{p^2-p}{p^{2s}} + \dots\right] \\
&= \sum_{n=1}^{\infty} f(n)n^{-s},
\end{aligned}$$

donde $f(n)$ es tal que $f(p^k) = p^k - p^{k-1}$, luego, $f(n) = \varphi(n)$, ahora note que

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

así:

$$\frac{\zeta(s-1)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \sum_{n=1}^{\infty} \frac{n}{n^s} \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \sum_{n=1}^{\infty} \frac{\mu * N(n)}{n^s},$$

por el teorema de unicidad, obtenemos que $\mu * N = \varphi$. Esto muestra el poder teórico de las series de Dirichlet, cuando tenemos propiedades adecuadas, podemos obtener mucha información de las funciones aritméticas asociadas. Pero esto no es todo, mostraré una propiedad adicional, toda serie de Dirichlet se puede ver como una integral de Riemann-Stieltjes y bajo ciertas condiciones esta integral tomará la forma de una transformada de Laplace. Este hecho tomará particular importancia en la prueba del TNP.

Lema 1.37 (Kronecker). Sean f una función aritmética y $s \in \mathbb{C}$ con $\sigma > 0$ tal que $F(s)$ converge, entonces

$$\lim_{x \rightarrow \infty} \frac{1}{x^s} \sum_{n \leq x} f(n) = 0.$$

Demostración. Sea f fija pero arbitraria y $s \in \mathbb{C}$ con $\sigma > 0$. Consideremos

$$S(x) = \sum_{n \leq x} f(n), \quad D(x) = \sum_{n \leq x} \frac{f(n)}{n^s},$$

por hipótesis $D(x)$ converge a un D cuando $x \rightarrow \infty$, queremos ver que $\lim_{x \rightarrow \infty} \frac{S(x)}{x^s} = 0$.
Dado $\varepsilon > 0$, existe un $x_0 \geq 1$, tal que para todo $x \geq x_0$

$$|D(x) - D| < \frac{\varepsilon}{2}.$$

Sea $x \geq x_0$, aplicando sumación parcial a $S(x)$ tenemos que

$$\begin{aligned} S(x) &= \sum_{n \leq x} \frac{f(n)}{n^s} n^s = \int_1^x t^s d(D(t)) = D(x)x^s - \int_1^x D(t)st^{s-1} dt \\ &= \int_0^x D(x)st^{s-1} dt - \int_1^x D(t)st^{s-1} dt. \end{aligned}$$

Note que $D(t) = 0$ para todo $t \in [0, 1)$, luego en la segunda integral podemos cambiar el límite inferior por 0, obteniendo que

$$\begin{aligned} |S(x)| &= \left| \int_0^x (D(x) - D(t))st^{s-1} dt \right| \\ &\leq \int_0^x |D(x) - D(t)| |s| t^{s-1} dt, \end{aligned}$$

para $x_0 \leq t \leq x$ tenemos que:

$$|D(t) - D(x)| \leq |D(t) - D| + |D - D(x)| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

y si $0 \leq t \leq x_0$, entonces

$$\begin{aligned} |D(t) - D(x)| &\leq |D(t)| + |D| + |D - D(x)| \\ &< \sum_{n \leq x_0} \left| \frac{f(n)}{n^s} \right| + |D| + \frac{\varepsilon}{2} = M, \end{aligned}$$

donde M depende de ε , pero no de x . De esto se sigue que

$$\begin{aligned} |S(x)| &\leq \varepsilon \int_{x_0}^x |s| t^{s-1} dt + M \int_0^{x_0} |s| t^{s-1} dt \\ &\leq \frac{|s|}{\sigma} (\varepsilon (x^\sigma - x_0^\sigma) + M x_0^\sigma), \end{aligned}$$

así

$$\left| \frac{S(x)}{x^s} \right| \leq \frac{|s|}{\sigma} \left(\varepsilon + \frac{M x_0^\sigma}{x^\sigma} \right). \quad (1.15)$$

Como M no depende de x , entonces tomando $x \rightarrow \infty$, el último término en (1.15) tiende a 0, luego para todo $\varepsilon > 0$

$$\lim_{x \rightarrow \infty} \left| \frac{S(x)}{x^s} \right| \leq \frac{\varepsilon |s|}{\sigma},$$

y como ε es arbitrario, $\lim_{x \rightarrow \infty} \frac{S(x)}{x^s} = 0$.

□

Sea $F(s)$ una serie de Dirichlet con abscisa de convergencia $\sigma_c > 0$, para todo $s \in \mathbb{C}$ con $\sigma > \sigma_c$

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{f(n)}{n^s} &= \lim_{N \rightarrow \infty} \int_1^N x^{-s} d(S(x)) \\ &= \lim_{N \rightarrow \infty} \frac{S(N)}{N^s} - \lim_{N \rightarrow \infty} \int_1^N S(x) d(x^{-s}) \\ &= s \int_1^{\infty} \frac{S(x)}{x^{s+1}} dx. \end{aligned}$$

El término de borde se anula por el lema de Kronecker. Así obtenemos una representación integral para cualquier serie de Dirichlet con abscisa de convergencia positiva. Aplicando esto a $\zeta(s)$ obtenemos una extensión analítica de la función zeta de Riemann al semiplano $\sigma > 0$ con un polo simple en $s = 1$ con residuo 1.

Note que tomando $x = e^t$, $dx = e^t dt$

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = s \int_0^{\infty} S(e^t) e^{-st} dt.$$

La serie de Dirichlet toma forma de transformada de Laplace. Aunque esto parezca una propiedad cualquiera, Korevaar y Zagier aplicaron esto para obtener una prueba corta del TNP en la que no es necesario todo el poder del teorema Tauberiano de Wiener-Ikehara [9], estas ideas también se siguen en el libro de Pongsriam [5].

1.6 La función zeta de Riemann

Teorema 1.38 (Propiedades). Sea $s \in \mathbb{C}$ tal que $\sigma > 1$, entonces

- i) $\zeta(s) \neq 0$
- ii) $\zeta'(s) = - \sum_{n=1}^{\infty} \frac{\log n}{n^s}$
- iii) $\frac{\zeta'(s)}{\zeta(s)} = - \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$

Las propiedades (ii) y (iii) ya las hemos probado antes, basta ver (i).

Demostración. Como $\sigma > 1$, entonces

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}},$$

donde el producto es absolutamente convergente, note que

$$\frac{1}{1 - p^{-s}} = \frac{p^s}{p^s - 1} = 1 + \frac{1}{p^s - 1},$$

entonces el producto no tiene factores nulos, luego no converge a 0, $\zeta(s) \neq 0$. \square

Teorema 1.39. Sea $s \in \mathbb{C}$ tal que $\sigma > 1$, entonces

$$\zeta(s) = \frac{s}{s-1} - s \int_1^\infty \frac{\{t\}}{t^{s+1}} dt.$$

Demostración. Tenemos que $\zeta(s) = s \int_1^\infty \frac{[t]}{t^{s+1}} dt$, como $[t] = t - \{t\}$, entonces

$$\begin{aligned} \zeta(s) &= s \int_1^\infty \frac{t - \{t\}}{t^{s+1}} dt \\ &= s \int_1^\infty \frac{1}{t^s} dt - s \int_1^\infty \frac{\{t\}}{t^{s+1}} dt \\ &= \frac{s}{s-1} - s \int_1^\infty \frac{\{t\}}{t^{s+1}} dt. \end{aligned}$$

\square

Teorema 1.40 (Extensión analítica). La representación integral de $\zeta(s)$ nos da una extensión analítica al semiplano $\sigma > 0$ con un polo simple en $s = 1$ con residuo 1.

Demostración. Note que $\frac{s}{s-1} = 1 + \frac{1}{s-1}$ es analítica en el semiplano $\sigma > 0$ excepto por un polo simple en $s = 1$ con residuo 1. Basta ver que la función

$$f(s) = \int_1^\infty \frac{\{t\}}{t^{s+1}} dt,$$

es analítica en el semiplano $\sigma > 0$. Para cada $n \in \mathbb{N}$, sea $f_n(s) = \int_1^n \frac{\{t\}}{t^{s+1}} dt$, tenemos que

$$f_n(s) = \int_1^n \{t\} e^{-(s+1) \log t} dt = \int_1^n \sum_{n=0}^\infty \frac{\{t\} (-\log t)^n (s+1)^n}{n!} dt,$$

donde la suma dentro de la integral es la serie de Taylor de e^x que sabemos tiene radio de convergencia infinito. Queremos ver que f_n es una sucesión de funciones analíticas, para lo que basta ver que podemos introducir la integral en la serie de potencias, además queremos ver que $f_n \rightarrow f$ uniformemente en cualquier subconjunto compacto de $\sigma > 0$. En efecto

$$\begin{aligned} \sum_{m=0}^{\infty} \left| \frac{\{t\}(-\log t)^m (s+1)^m}{m!} \right| &\leq \sum_{m=0}^{\infty} \frac{(|\log t|(|s|+1))^m}{m!} \\ &= e^{|\log t|(|s|+1)} = t^{|s|+1}, \end{aligned}$$

entonces

$$\int_1^n \sum_{m=0}^{\infty} \left| \frac{\{t\}(-\log t)^m (s+1)^m}{m!} \right| dt \leq \int_1^n t^{|s|+1} dt < \infty,$$

luego por convergencia absoluta

$$f_n(s) = \sum_{m=0}^{\infty} \frac{(s+1)^m}{m!} \int_1^n \{t\}(-\log t)^m dt.$$

Sea $s \in \mathbb{C}$ con $\sigma \geq \delta > 0$. Dado $\varepsilon > 0$, sea $N = (\delta\varepsilon)^{-\frac{1}{\delta}}$, entonces para todo $n > N$:

$$\begin{aligned} |f(s) - f_n(s)| &\leq \int_n^{\infty} \left| \frac{\{t\}}{t^{s+1}} \right| dt \leq \int_n^{\infty} \frac{1}{t^{\sigma+1}} dt \leq \frac{1}{\sigma n^{\sigma}} \\ &\leq \frac{1}{\delta n^{\delta}} \\ &< \frac{1}{\delta(\delta\varepsilon)^{-\frac{1}{\delta}\delta}} = \varepsilon. \end{aligned}$$

como N no depende de s , f_n converge uniformemente a f en el semiplano $\sigma \geq \delta$, en particular sobre cualquier compacto de $\sigma > 0$, por el Teorema 1.26 $f(s)$ es analítica en el semiplano $\sigma > 0$.

□

El teorema de Dirichlet

” *...Dirichlet creó una parte nueva en las matemáticas, la aplicación de las series infinitas que Fourier ha introducido en la teoría del calor en la exploración de las propiedades de los números primos. Él ha descubierto una variedad de teoremas que ... son los pilares de las nuevas teorías*

— C. G. J. Jacobi

El teorema de Dirichlet afirma que dados $a, n, k \in \mathbb{N}$ tal que $(a, n) = 1$, hay infinitos primos de la forma $ak + n$. El primer resultado sobre la infinitud de los números primos se remonta a Euclides. Supongamos que hay una cantidad finita de primos, podemos contarlos... p_1, p_2, \dots, p_n , note que $p_1 p_2 \dots p_n + 1$ es primo ya que si $p_i \mid p_1 p_2 \dots p_n + 1$ para algún $1 \leq i \leq n$, entonces

$$1 = p_i(K - (p_1 \dots p_{i-1} p_{i+1} \dots p_n)),$$

luego $p_i \mid 1$, una contradicción, es decir, siempre podemos construir un primo p_{n+1} con los n primos anteriores, entonces son infinitos.

Intentemos replicar este argumento para probar que hay infinitos primos de la forma $4k + 1$, supongamos que hay finitos primos de la forma $4k + 1$, digamos p_1, p_2, \dots, p_n , debemos construir un nuevo primo de la forma $4k + 1$ para que funcione el argumento de Euclides, sin embargo la expresión $p_1 p_2 \dots p_n + 1$ no siempre es de la forma $4k + 1$, por ejemplo $5 \times 13 + 1 = 66$, que es congruente a 2 módulo 4, de hecho con esta expresión siempre conseguimos pares. Requerimos una expresión nueva, por ejemplo, podríamos hacer $2p_1 \dots p_n + 1$, pero también falla, note que $2 \times 5 \times 13 + 1 = 131$ que es un primo de la forma $4k + 3$.

Proposición 2.1. Sea $n \in \mathbb{Z}$, todo divisor primo impar de $n^2 + 1$ es de la forma $4k + 1$.

Demostración. Suponga que existe $p = 4k + 3$ primo tal que $p \mid n^2 + 1$, entonces $n^2 \equiv -1 \pmod{p}$, luego por el pequeño teorema de Fermat

$$\pmod{p} : 1 \equiv n^{p-1} \equiv (n^2)^{2k+1} \equiv (-1)^{2k+1} \equiv -1,$$

así $2 \equiv 0 \pmod{p}$, esto es $p = 2$, contradicción.

□

Con el teorema anterior sabemos que la expresión que buscamos es $N = (2p_1 \dots p_n)^2 + 1$ ya que de esta forma obtenemos un número cuyos divisores primos son de la forma $4k + 1$,

basta ver que ningún p_i con $1 \leq i \leq n$ divide a N .

Supongamos que $p_i \mid N$, luego $p_i(K - 4p_1^2 \dots p_i \dots p_n^2) = 1$ una contradicción, entonces N es un primo de la forma $4k + 1$. Continuar replicando este argumento es inviable cuando trabajamos con primos módulo un entero n arbitrario, además no nos sirve para atacar el panorama general, la prueba de este teorema llegaría de una idea totalmente distinta...

Teorema 2.2 (Euler). La serie $\sum_p \frac{1}{p}$ diverge.

Demostración. Por el producto de Euler:

$$\log(\zeta(s)) = \sum_p \left(\sum_{k=1}^{\infty} \frac{1}{k(p)^{ks}} \right) = \sum_p \frac{1}{p^s} + \sum_p \left(\sum_{k=2}^{\infty} \frac{1}{kp^{ks}} \right), \quad \Re(s) > 1$$

note que:

$$\begin{aligned} \sum_p \left(\sum_{k=2}^{\infty} \frac{1}{kp^{ks}} \right) &\leq \sum_p \left(\sum_{k=2}^{\infty} \frac{1}{p^{ks}} \right) \\ &\leq \sum_p \frac{1}{p^s} \left(\frac{1}{p^s - 1} \right) \\ &\leq \sum_p \frac{1}{p^s(p^s - 1)} \leq \sum_{n=1}^{\infty} \frac{1}{n^s(n^s - 1)}. \end{aligned}$$

¹La última serie converge siempre que $\Re(s) > \frac{1}{2}$, entonces por la divergencia de la serie armónica, tomando el límite cuando $s \rightarrow 1^+$

$$\infty = \lim_{s \rightarrow 1^+} \log(\zeta(s)) = \lim_{s \rightarrow 1^+} \sum_p \frac{1}{p^s} + \sum_p \left(\sum_{k=2}^{\infty} \frac{1}{kp^{ks}} \right) = \sum_p \frac{1}{p} + O(1),$$

lo cual nos dice que la suma de los recíprocos de los primos diverge, y por lo tanto podemos decir que los primos son infinitos. \square

La idea de Dirichlet es replicar este argumento de Euler para probar que hay infinitos primos de la forma $4k + 1$, para ello define la siguiente serie

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

donde, $\chi(n)$ es la función indicadora:

¹La convergencia de esta serie nos llegó haciendo cuentas en una clase de estructuras algebraicas, Santiago me dijo “Mateo esa serie es geométrica.”

$$\chi(a) = \begin{cases} 0 & \text{si } a \text{ es par} \\ 1 & \text{si } a \equiv 1 \pmod{4} \\ -1 & \text{si } a \equiv 3 \pmod{4} \end{cases}$$

note que χ es completamente multiplicativa, entonces

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

Siguiendo los pasos de la prueba anterior obtenemos

$$\begin{aligned} \log L(s, \chi) &= \sum_p \frac{\chi(p)}{p^s} + \sum_p \sum_{k=2}^{\infty} \frac{\chi(k)}{kp^{ks}} \\ &= \sum_{p \equiv 1(4)} \frac{1}{p^s} - \sum_{p \equiv 3(4)} \frac{1}{p^s} + g_1(s, \chi), \end{aligned}$$

donde no es difícil ver que $g_1(s, \chi)$ es convergente cuando $s \rightarrow 1^+$ ya que la serie de Dirichlet de $|\chi(n)|$ es menor o igual que $\zeta(s)$, además

$$\log \zeta(s) = \sum_p \frac{1}{p^s} + g(s),$$

así

$$\begin{aligned} \log \zeta(s) + \log L(s, \chi) &= 2 \sum_{p \equiv 1(4)} \frac{1}{p^s} + \left(\frac{1}{2^s} + g(s) + g_1(s, \chi) \right), \\ \log \zeta(s) - \log L(s, \chi) &= 2 \sum_{p \equiv 3(4)} \frac{1}{p^s} + \left(\frac{1}{2^s} + g(s) - g_1(s, \chi) \right). \end{aligned}$$

Tomando $\lim_{s \rightarrow 1^+}$ como antes se verifica que hay infinitos primos de la forma $4k + 1$ y $4k + 3$ ya que el término restante converge, sin embargo debemos garantizar algo, que $L(1, \chi)$ converge y es distinto de 0. Para esto note que

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n} = \sum_{n=1}^{\infty} \frac{(-1)^n}{2n+1} = \arctan(1) = \frac{\pi}{4}.$$

Este camino parece fructífero, intentemos replicar esto en un caso general, sea $f(n)$ la función característica de la progresión aritmética, es decir

$$f(n) = \begin{cases} 1, & n \equiv a \pmod{m} \\ 0, & n \not\equiv a \pmod{m} \end{cases}$$

en el caso de que $f(n)$ sea completamente multiplicativa tendríamos un producto de Euler

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \left(1 - \frac{f(p)}{p^s} \right)^{-1}, \quad \Re(s) > 1$$

y así por argumentos análogos a los de Euler se tendría que

$$\log \left(\sum_{n=1}^{\infty} \frac{f(n)}{n^s} \right) = \sum_{p \equiv a(m)} \frac{1}{p^s} + O(1)$$

Lamentablemente, $f(n)$ generalmente no es multiplicativa, dicho esto, tenemos dos problemas importantes para obtener una prueba por este camino y que debemos resolver.

- 1) La función f como característica de la progresión no siempre resulta completamente multiplicativa módulo n
- 2) Nuestro argumento depende de probar que la serie de Dirichlet asociada a f no se anula en $s = 1$.

Para el primero de estos inconvenientes estudiaremos los caracteres de un grupo y en particular los caracteres de Dirichlet, estos veremos que poseen propiedades de ortogonalidad, lo que nos permitirá hacer ¡Análisis de Fourier! y representar a la función f característica de la progresión en su serie de Fourier como una combinación lineal finita de funciones completamente multiplicativas (los caracteres), con esto en mente veamos primero unos preliminares sobre caracteres que necesitaremos en la prueba.

2.1 Caracteres y el teorema de Dirichlet

Primero vamos a presentar definición formal de la idea de carácter.

Definición. Sea G un grupo, χ es un carácter de G si $\chi : G \rightarrow \mathbb{C}^\times$ y satisface que para todo $a, b \in G$, $\chi(ab) = \chi(a)\chi(b)$, es decir, un homomorfismo de G en \mathbb{C}^\times .

El homomorfismo trivial que mapea a todo $g \in G$ al 1 lo llamaremos “carácter trivial” denotado χ_0 .

Definición. Dado un grupo G , definimos el conjunto de todos los caracteres de G , denotado como \hat{G} . También definimos la multiplicación en \hat{G} como

$$\chi_1 \chi_2(g) = \chi_1(g) \chi_2(g) \quad \text{para todo } \chi_1, \chi_2 \in \hat{G} \quad \text{y } g \in G$$

Decimos $e(x)$ para denotar $e^{2\pi i x}$. Por ejemplo, $e(1/n)$ es una raíz n -ésima de la unidad. Una caracterización de los caracteres de un grupo cíclico finito es la siguiente.

Teorema 2.3. Sea G un grupo cíclico de orden n generado por g , $G = \langle g \rangle$, entonces hay exactamente n caracteres $\chi_0, \dots, \chi_{n-1}$ de G , dados por $\chi_m(g^k) = e((mk)/n)$ para todo $0 \leq m \leq n-1$ y $k \in \mathbb{Z}$, esto es

$$\chi_0(g^k) = 1, \chi_1(g^k) = e(k/n), \chi_2(g^k) = e(2k/n), \dots, \chi_{n-1}(g^k) = e((n-1)k/n).$$

Demostración. Sea χ un carácter de G , tenemos que $\chi(g)^n = \chi(g^n) = \chi(1) = 1$, esto es que $\chi(g)$ es una raíz n -ésima de la unidad, luego $\chi(g) = e(m/n)$ para algún $0 \leq m \leq n-1$, dado que G es cíclico y generado por g , entonces χ está totalmente determinado por $\chi(g)$ y $\chi(g)^k = \chi(g^k) = e((km)/n)$ para todo $k \in \mathbb{Z}$, esto es $\chi = \chi_m$. Así si χ es un carácter de G , χ debe ser uno de los $\chi_0, \dots, \chi_{n-1}$. Ahora veamos que $\chi_0, \dots, \chi_{n-1}$ están bien definidos y son caracteres distintos de G .

En efecto si $g^{k_1} = g^{k_2}$ entonces $k_1 \equiv k_2 \pmod{n}$, luego $\chi_m(g^{k_1}) = e((mk_1)/n) = e((mk_2)/n) = \chi_m(g^{k_2})$ para todo $0 \leq m \leq n-1$, por tanto $\chi_0, \dots, \chi_{n-1}$ están bien definidos en G . Dados $0 \leq m_1, m_2 \leq n-1$ con $m_1 \neq m_2$, entonces

$$\chi_{m_1}(g) = e\left(\frac{m_1}{n}\right) \neq e\left(\frac{m_2}{n}\right) = \chi_{m_2}(g),$$

como χ_{m_1} y χ_{m_2} están totalmente determinados por $\chi_{m_1}(g)$ y $\chi_{m_2}(g)$, entonces $\chi_0, \dots, \chi_{n-1}$ son todos distintos.

Finalmente debemos ver que dado χ_m con $0 \leq m \leq n-1$, χ_m es homomorfismo de G en \mathbb{C}^\times , en efecto dados $a, b \in G$, $a = g^{k_1}$ y $b = g^{k_2}$. Note que

$$\begin{aligned} \chi_m(ab) &= \chi_m(g^{k_1}g^{k_2}) \\ &= \chi_m(g^{k_1+k_2}) \\ &= e\left(\frac{m(k_1+k_2)}{n}\right) \\ &= e\left(\frac{mk_1}{n}\right) e\left(\frac{mk_2}{n}\right) \\ &= \chi_m(a)\chi_m(b). \end{aligned}$$

Esto es, χ_m es homomorfismo. □

Teorema 2.4. Sea G un grupo, el conjunto \widehat{G} es un grupo abeliano bajo la multiplicación.

Demostración. El carácter principal χ_0 de G es la identidad de \widehat{G} ya que dado $a \in G$ $\chi_m\chi_0(a) = \chi_m(a)\chi_0(a) = \chi_m(a)$ con $0 \leq m \leq n-1$, además note que la función $\chi^{-1} = 1/\chi(g)$ es también un carácter y por lo tanto tenemos inversos en \widehat{G} , Además \widehat{G} es cerrado bajo la multiplicación, note que:

$$\begin{aligned} \chi_{m_1}\chi_{m_2}(ab) &= \chi_{m_1}(ab)\chi_{m_2}(ab) \\ &= \chi_{m_1}(a)\chi_{m_1}(b)\chi_{m_2}(a)\chi_{m_2}(b) \\ &= \chi_{m_1}\chi_{m_2}(a)\chi_{m_1}\chi_{m_2}(b). \end{aligned}$$

La conmutatividad y asociatividad se siguen de manera análoga usando la conmutatividad y asociatividad de \mathbb{C}^\times . □

Nota. Por el teorema anterior, dado que \widehat{G} es grupo, lo llamaremos grupo dual de G .

La inversa de χ en la prueba del anterior, denotada como χ^{-1} en algunos casos se escribe también como $\bar{\chi}$, la razón de esto es que si G es un grupo abeliano finito entonces $|\chi(g)| = 1$, así $\chi^{-1}(g) = 1/\chi(g) = \overline{\chi(g)}$ por propiedad de la norma en los complejos. Así la función $\bar{\chi}$ definida como $\bar{\chi}(g) = \overline{\chi(g)}$ y la función χ^{-1} son iguales. [5]

Teorema 2.5. Sea $G = \langle g \rangle$ un grupo cíclico de orden n , entonces:

(i) Dado un carácter χ de G

$$\sum_{g \in G} \chi(g) = \begin{cases} n, & \text{si } \chi = \chi_0 \\ 0, & \text{e.o.c} \end{cases}$$

(ii) Dado $a \in G$

$$\sum_{\chi \in \widehat{G}} \chi(a) = \begin{cases} n, & \text{si } a = 1 \\ 0, & \text{e.o.c} \end{cases}$$

(iii) \widehat{G} es un grupo cíclico generado por χ_1 .

Demostración. (i) Note que dado un carácter χ no trivial de G , existe un $0 \leq m \leq n-1$ tal que $\chi = \chi_m$. Si $m \neq 0$

$$\sum_{g \in G} \chi(g) = \sum_{k=0}^{n-1} \chi_m(g_0^k) = \sum_{k=0}^{n-1} e\left(\frac{mk}{n}\right) = \sum_{k=0}^{n-1} \left(e\left(\frac{m}{n}\right)\right)^k = \frac{1 - e\left(\frac{m}{n}\right)^n}{1 - e\left(\frac{m}{n}\right)},$$

y $1 - e\left(\frac{m}{n}\right)^n = 1 - \cos(2\pi m) = 0$ para todo $m = 1, \dots, n-1$, si $m = 0$ entonces

$$\sum_{k=0}^{n-1} \chi_m(g_0^k) = \sum_{k=0}^{n-1} 1 = n.$$

(ii) Sea $a \in G$, $a = g^k$ para algún $k = 0, 1, \dots, n-1$, en efecto

$$\sum_{\chi \in \widehat{G}} \chi(a) = \sum_{m=0}^{n-1} \chi_m(a) = \sum_{m=0}^{n-1} \chi_m(g^k) = \sum_{m=0}^{n-1} e\left(\frac{mk}{n}\right),$$

análogamente se ve que esta suma es n si $k = 0$ y es 0 si $k \neq 0$, y el valor $k = 0$ corresponde a $g^0 = 1$. Para (iii) note que por el teorema 2.3

$$\widehat{G} = \{\chi_0, \chi_1, \dots, \chi_{n-1}\} = \{\chi_1^0, \chi_1, \chi_1^2, \dots, \chi_1^{n-1}\} = \langle \chi_1 \rangle.$$

Esto completa la prueba. □

Observe que el teorema anterior nos permite establecer lo siguiente, dado G un grupo cíclico de orden n , entonces G es isomorfo a su grupo dual \hat{G} , esto no es exclusivo de los grupos cíclicos, sabemos que todo grupo abeliano finito se puede escribir como suma directa de grupos cíclicos, Dirichlet probó lo siguiente

Teorema 2.6 (Dualidad). Sea G un grupo abeliano finito de orden n , entonces G tiene exactamente n caracteres. Más aún, sea

$$G = \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_\ell\mathbb{Z},$$

entonces los caracteres de G son de la forma

$$\chi((a_1, a_2, \dots, a_\ell)) = e\left(\frac{a_1 k_1}{m_1}\right) e\left(\frac{a_2 k_2}{m_2}\right) \cdots e\left(\frac{a_\ell k_\ell}{m_\ell}\right),$$

donde $k_i = 0, 1, \dots, m_i - 1$ para todo $i = 1, 2, \dots, \ell$. Adicionalmente, \hat{G} es un grupo abeliano finito de orden n , $|\hat{G}| = |G| = m_1 m_2 \cdots m_\ell$, y \hat{G} es isomorfo a G :

$$\begin{aligned} \hat{G} &\simeq \widehat{\mathbb{Z}/m_1\mathbb{Z}} \times \widehat{\mathbb{Z}/m_2\mathbb{Z}} \times \cdots \times \widehat{\mathbb{Z}/m_\ell\mathbb{Z}} \\ &\simeq \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_\ell\mathbb{Z} \simeq G. \end{aligned} \tag{2.1}$$

Demostración. Primero consideremos el caso en que G es la suma directa de $\mathbb{Z}/m_i\mathbb{Z}$ para cada $i = 1, 2, 3, \dots, \ell$, sea $e_i = (0, 0, \dots, 1, 0, 0, \dots, 0)$ donde 1 está en la posición i . Entonces e_i tiene orden m_i y por lo tanto $\chi(e_i)$ es una m_i -ésima raíz de la unidad, así pues

$$\begin{aligned} \chi((a_1, \dots, a_\ell)) &= \chi(a_1 e_1 + \dots + a_\ell e_\ell) \\ &= \chi(e_1)^{a_1} \cdots \chi(e_\ell)^{a_\ell} \\ &= e\left(\frac{a_1 k_1}{m_1}\right) e\left(\frac{a_2 k_2}{m_2}\right) \cdots e\left(\frac{a_\ell k_\ell}{m_\ell}\right), \end{aligned}$$

donde $k_i = 0, 1, \dots, m_i - 1$ para todo $i = 1, 2, \dots, \ell$. De esto además vemos que χ se escribe como un producto de caracteres de $\mathbb{Z}/m_1\mathbb{Z}, \dots, \mathbb{Z}/m_\ell\mathbb{Z}$, esto es, se tiene (2.1) y $|\hat{G}| = |G| = m_1 m_2 \cdots m_\ell$ dado que hay m_i posibles elecciones para k_i . Como G es abeliano finito entonces:

$$G \simeq \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_\ell\mathbb{Z}.$$

lo que completa la prueba. □

2.1.1. Ortogonalidad de los caracteres

Los caracteres de un grupo abeliano finito satisfacen relaciones de ortogonalidad, cuando $G = (\mathbb{Z}/m\mathbb{Z})^\times$ estas relaciones de ortogonalidad nos permiten hacer análisis de Fourier, tenemos transformada y representación en “serie de Fourier”, en nuestro caso esta serie será en realidad una suma finita, por lo que no nos preocuparemos por la convergencia de

la misma. Las relaciones de ortogonalidad que veremos en esta sección son generalizaciones del teorema 2.5, recordemos que la idea es poder expresar la función característica de una clase de residuos módulo m como combinación lineal de caracteres, funciones completamente multiplicativas.

Teorema 2.7. Sea G un grupo abeliano finito. Entonces

(i) Dado un carácter χ de G

$$\sum_{g \in G} \chi(g) = \begin{cases} |G|, & \text{si } \chi = \chi_0 \\ 0, & \text{e.o.c.} \end{cases}$$

(ii) Dado $g \in G$

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |G|, & \text{si } g = 1 \\ 0, & \text{e.o.c.} \end{cases}$$

Demostración. Si $\chi = \chi_0$ entonces $\chi(g) = 1$ para todo $g \in G$ por tanto la suma (i) es igual a $|G|$. Dado $\chi \neq \chi_0$, existe $h \in G$ tal que $\chi(h) \neq 1$, luego

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg) = \sum_{g \in G} \chi(g),$$

ya que la suma se hace sobre todos los elementos del grupo, hg solo me permuta los elementos de la suma, así

$$(\chi(h) - 1) \sum_{g \in G} \chi(g) = 0,$$

y como $\chi(h) \neq 1$, obtenemos lo requerido. De manera análoga obtenemos (ii), si $g = 1$, entonces $\chi(g) = 1$ para todo $\chi \in \widehat{G}$ y la suma (ii) es igual a $|\widehat{G}| = |G|$ por el teorema 2.6. Suponga que $g \neq 1$, entonces existe $\psi \in \widehat{G}$ tal que $\psi(g) \neq 1$. Nuevamente

$$\psi(g) \sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} (\psi\chi)(g) = \sum_{\chi \in \widehat{G}} \chi(g).$$

De donde se sigue el resultado. □

Corolario 2.8 (Ortogonalidad). Sea G un grupo abeliano finito. Entonces

(i) Si χ y ψ son caracteres de G

$$\sum_{g \in G} \psi(g) \overline{\chi}(g) = \begin{cases} |G|, & \text{si } \psi = \chi; \\ 0, & \text{e.o.c.} \end{cases}$$

(ii) Si g y h son elementos de G

$$\sum_{\chi \in \widehat{G}} \chi(g) \overline{\chi}(h) = \begin{cases} |G|, & \text{si } g = h \\ 0, & \text{e.o.c.} \end{cases}$$

Nota. Un lector familiarizado con algunos conceptos del análisis de Fourier podría notar que la suma presentada en (i) es muy similar al producto interno en $\ell^2(\mathbb{Z})$, esto no es para nada coincidencia, en esencia son el mismo producto interno.

Sea G un grupo abeliano finito se puede verificar que el espacio de funciones $f : G \rightarrow \mathbb{C}$, es un espacio vectorial de dimensión finita con el producto interno

$$\langle g, h \rangle = \sum_{g \in G} f(g) \overline{h(g)}.$$

Además podemos ver a \widehat{G} como un subconjunto del espacio, ahora sí procedamos con la prueba.

Demostración. La suma en (i) se puede escribir como $\sum_{g \in G} (\psi \chi^{-1})(g)$ y

$$\psi \chi^{-1} = \chi_0 \quad \text{si y solo si} \quad \psi = \chi.$$

La suma en (ii) es igual a $\sum_{\chi \in \widehat{G}} \chi(gh^{-1})$, luego el resultado es una consecuencia inmediata del teorema anterior. □

Como mencionamos antes, la ortogonalidad de los caracteres nos permite hacer Análisis de Fourier, procedamos formalmente suponiendo que tenemos

$$f(g) = \frac{1}{|G|} \sum_{\psi \in \widehat{G}} \widehat{f}(\psi) \psi(g),$$

por la ortogonalidad de los caracteres

$$\begin{aligned}
\langle f, \chi \rangle &= \frac{1}{|G|} \sum_{g \in G} \sum_{\psi \in \widehat{G}} \widehat{f}(\psi) \psi(g) \overline{\chi}(g) \\
&= \frac{1}{|G|} \sum_{\psi \in \widehat{G}} \widehat{f}(\psi) \sum_{g \in G} \psi(g) \overline{\chi}(g) \\
&= \widehat{f}(\chi).
\end{aligned}$$

Esto motiva la siguiente definición de transformada de Fourier.

Definición (Transformada de Fourier). Sea $f : G \rightarrow \mathbb{C}$, definimos su transformada de Fourier como la función $\widehat{f} : \widehat{G} \rightarrow \mathbb{C}$ dada por

$$\widehat{f}(\chi) = \sum_{g \in G} f(g) \overline{\chi}(g).$$

Teorema 2.9 (Representación de Fourier). Dada $f : G \rightarrow \mathbb{C}$, tenemos la representación en “serie” de Fourier

$$f(g) = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \widehat{f}(\chi) \chi(g).$$

Así toda función se puede escribir como combinación lineal de caracteres (funciones completamente multiplicativas).

Demostración. Dada $f : G \rightarrow \mathbb{C}$, por la ortogonalidad

$$\begin{aligned}
\frac{1}{|G|} \sum_{\chi \in \widehat{G}} \widehat{f}(\chi) \chi(g) &= \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \sum_{h \in G} f(h) \overline{\chi}(h) \chi(g) \\
&= \frac{1}{|G|} \sum_{h \in G} f(h) \sum_{\chi \in \widehat{G}} \overline{\chi}(h) \chi(g) \\
&= f(g).
\end{aligned}$$

□

Antes de seguir con la prueba del teorema de Dirichlet necesitamos estudiar los caracteres de Dirichlet y algunas propiedades de las series de Dirichlet asociadas a estos, a las que llamaremos L-funciones.

2.1.2. Caracteres de Dirichlet

En esta sección nos restringimos a estudiar los caracteres del grupo $(\mathbb{Z}/q\mathbb{Z})^\times$, sabemos que este es un grupo multiplicativo formado por las unidades del grupo aditivo $(\mathbb{Z}/q\mathbb{Z})$,

las clases de residuos módulo q , conocemos un par de cosas de este grupo, por ejemplo, su orden está determinado por el número de elementos de $(\mathbb{Z}/q\mathbb{Z})^\times$ que son primos relativos con q , esto es $\varphi(q)$.

Un carácter de Dirichlet es un carácter del grupo $(\mathbb{Z}/q\mathbb{Z})^\times$, sin embargo es útil presentarlo como una función aritmética que extiende un carácter de $(\mathbb{Z}/q\mathbb{Z})^\times$ a todos los naturales.

Definición (Carácter de Dirichlet). Un carácter de Dirichlet es un carácter del grupo $(\mathbb{Z}/m\mathbb{Z})^\times$. Más generalmente, un carácter de Dirichlet módulo m es una función aritmética que extiende un carácter de $(\mathbb{Z}/m\mathbb{Z})^\times$ mediante

$$f(n) = \begin{cases} \chi(a) & \text{si } n \equiv a \pmod{m}, 1 \leq a \leq m, \text{ y } (a, m) = 1, \\ 0 & \text{si } (n, m) > 1. \end{cases}$$

Por ejemplo el carácter trivial se extiende de la siguiente manera:

$$\chi_0(n) = \begin{cases} 1, & \text{si } (n, m) = 1 \\ 0, & \text{si } (n, m) > 1. \end{cases}$$

En algunos casos simplificaremos la notación como antes, solo escribiremos si $(n, m) = 1$ y no la condición $1 \leq a \leq m$ y $n \equiv a \pmod{m}$ ya que estas condiciones se pueden asumir que están presentes dado que estamos trabajando sobre clases de residuos, de todas manera es importante aclarar que solo es una herramienta de notación.

Teorema 2.10. Sea χ un carácter de Dirichlet módulo q , entonces $\chi(mn) = \chi(m)\chi(n)$ y $\chi(n + q) = \chi(n)$ para todo $m, n \in \mathbb{N}$.

Esto es que en efecto cuando se extiende el carácter sobre todos los naturales, obtenemos una función periódica de periodo q y además esta sigue siendo completamente multiplicativa.

Demostración. Sea χ un carácter de Dirichlet módulo q y sean $m, n \in \mathbb{N}$. Sea f el carácter de $(\mathbb{Z}/q\mathbb{Z})^\times$ que induce χ , esto es, para todo $n \in \mathbb{N}$,

$$\chi(n) = \begin{cases} f(n), & \text{si } (n, q) = 1 \\ 0, & \text{si } (n, q) > 1 \end{cases}$$

si $(m, q) > 1$ o $(n, q) > 1$, entonces $(mn, q) > 1$ y por tanto $\chi(mn) = 0 = \chi(m)\chi(n)$. Si $(m, q) = (n, q) = 1$, entonces $(mn, q) = 1$ y

$$\chi(m)\chi(n) = f(m)f(n) = f(mn) = \chi(mn).$$

Esto prueba que χ es completamente multiplicativa, tenemos que $(n + q, q) = (n, q)$ se sigue que si $(n + q, q) = 1$, entonces $(n, q) = 1$ y por tanto $\chi(n + q) = f(n + q) = f(n) = \chi(n)$. Análogamente, si $(n + q, q) > 1$, entonces $(n, q) > 1$ y $\chi(n + q) = 0 = \chi(n)$, entonces χ es periódica de periodo q .

□

Bibliografía

- [1] Bernhard Riemann. On the number of primes less than a given magnitude. *Complete Works*. Kendrick Press, 2004.
- [2] Adolf J Hildebrand. Introduction to analytic number theory math 531 lecture notes, fall 2005. URL: <http://www.math.uiuc.edu/hildebr/ant>. Version, 1, 2006.
- [3] Norman Levinson. A motivated account of an elementary proof of the prime number theorem. *The American Mathematical Monthly*, 76(3):225–245, 1969.
- [4] Tom M Apostol. *Mathematical analysis; 2nd ed.* Addison-Wesley series in mathematics. Addison-Wesley, Reading, MA, 1974.
- [5] Prapanpong Pongsriiam. *Analytic Number Theory for Beginners*, volume 103. American Mathematical Society, 2023.
- [6] E.M. Stein and R. Shakarchi. *Complex Analysis*. Princeton lectures in analysis. Princeton University Press, 2010.
- [7] Hugh L Montgomery and Robert C Vaughan. *Multiplicative number theory I: Classical theory*. Number 97. Cambridge university press, 2007.
- [8] T.M. Apostol. *Introduction to Analytic Number Theory*. Undergraduate Texts in Mathematics. Springer New York, 1998.
- [9] Don Zagier. Newman’s short proof of the prime number theorem. *The American mathematical monthly*, 104(8):705–708, 1997.
- [10] Graham James Oscar Jameson. *The prime number theorem*. Cambridge University Press, 2003.
- [11] USR Murty. *Problems in analytic number theory*, volume 206. Springer Science & Business Media, 2007.
- [12] Samuel J Patterson. *An introduction to the theory of the Riemann zeta-function*. Cambridge University Press, 1995.
- [13] Harold Davenport. *Multiplicative number theory*, volume 74. Springer Science & Business Media, 2013.
- [14] Andrew Granville and Greg Martin. Prime number races. *The American Mathematical Monthly*, 113(1):1–33, 2006.
- [15] M Ram Murty and V Kumar Murty. *Non-vanishing of L-functions and applications*. Springer Science & Business Media, 2012.

- [16] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53. American Mathematical Soc., 2021.