# 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


2 de junio de 2024

# Abstract

The prime number theorem is the assetion that in the limit, the quotient $\dfrac{\pi(x)\log x}{x}$ goes to 1, which means that $\pi(x) \sim \dfrac{x}{\log x}$, 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 $\pi_{a,q}(x) \sim \dfrac{x}{\phi(q)\log x}$, 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 $\dfrac{\pi(x)\log x}{x}$ tiende a 1, es decir, que $\pi(x) \sim \dfrac{x}{\log x}$ 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 $\pi_{a,q}(x) \sim \dfrac{x}{\phi(q)\log x}$, 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

# 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**

La teoría de números fue llamada por Gauss, la reina de las matemáticas, quizá por la simplicidad de su objeto o la elegancia y diversidad de sus métodos, que la convierten en una de las áreas más fascinantes del universo matemático. Sin embargo no solo podemos resaltar la gran variedad de objetos matemáticos que intervienen en ella, sino la capacidad que tiene para conectarlos, que el teorema de Dirichlet junta de manera sorprendente ideas del álgebra, con el análisis de Fourier, que en un principio aparece para el estudio de las ecuaciones diferenciales parciales, que el teorema de los números primos resulte ser una consecuencia de la no nulidad de una función en una recta del plano complejo, que los ceros de una función controlen el comportamiento de los números primos... Estas entre muchas otras, forman parte de las fascinantes y inesperadas conexiones que aparecen al adentrarnos en las ideas un poco más modernas de la teoría de números.

Es sorprendente que el análisis y sus objetos sean capaces de decir algo sobre la naturaleza, en un principio discreta, de los números naturales, quizás la primera relación que me cautivó fue el producto de Euler, ver una función de variable compleja ser escrita como un producto sobre los números primos es algo maravilloso, el cómo eran posibles estas conexiones fue lo que siempre quise comprender, y que de cierto modo al adentrarme en la teoría analítica de números, pude lograr, pero para entender cómo nace esta relación debemos estudiar algunas de las ideas de Euler.

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 provenía de estudiar la serie de Taylor de la $\sin x$:

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

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 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:

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

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:

$$d = \lim_{n \to \infty} \frac{|\{m \le n \mid m \in N\}|}{n}, \quad \text{siempre que exista el límite}$$

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 $m \le n$ tal que $p \mid m$, sabemos por un simple conteo que:

$$\frac{n}{p} - 1 \le c \le \frac{n}{p} + 1$$

Luego, $d = \lim_{n \to \infty} \frac{c}{n} = \frac{1}{p}$ 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:

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

Queremos ver que esto crece como $\frac{1}{\log n}$, para esto podemos invertir el producto anterior, nuevamente tenemos que:

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

En el siguiente capítulo veremos justamente que $H(n) \sim \log n$, esto concluye lo que queríamos ver: la probabilidad de que un número sea primo es $\frac{1}{\log n}$, *es inversamente proporcional a su longitud.* ie:

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

Pero, ¿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 articulo "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 Hadammar 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 $\zeta$ no se anulaba en la recta vertical de los complejos con parte real 1, sobre el plano complejo, algo sencillamente maravilloso. Veremos al final de este trabajo la forma en que este teorema se extiende a progresiones aritmética $a + kq$ con $(a, q) = 1$:

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

Donde $\varphi$ es 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.

En el capítulo 1 presentaremos algunos preliminares que se pueden consultar en el contenido y estudiaremos un poco la función $\zeta(s)$ y su derivada logarítmica $\frac{\zeta'(s)}{\zeta(s)}$, veremos que el TNP es equivalente a la afirmación $\psi(x) \sim x$, función que también estudiaremos allí. El capítulo 2 será para presentar una prueba del teorema de Dirichlet, las ideas subyacentes y los preliminares de la prueba también se desarrollarán allí, en los capítulos 3 y 4 se desarrollarán las pruebas del TNP y el TNP sobre progresiones aritmética, estudiaremos la teoría Tauberiana, que nos permitirá dar una prueba sencilla del TNP y donde casi toda la variable compleja estará escondida en el teorema de Wiener-Ikehara que también presentaremos allí junto con algunas aplicaciones.

*Esta página se dejó intencionalmente en blanco*

# 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 rango $\mathbb{R}$ o $\mathbb{C}$, es decir $a$ es función aritmética si:

$$f : \mathbb{N} \to \mathbb{F}$$

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

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

- **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:

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

Ahora, si $f$ es multiplicativa:

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

□

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 identicamente nula, entonces para algún $n$, $f(1 \cdot n) = f(1) + f(n)$, así $f(1) = 0$, análogamente si $f$ es multiplicativa y no identicamente 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:

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

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

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

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 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 $\pi(x)$; de hecho, el TNP es equivalente a la afirmación

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

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.[**?**]

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

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

### 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... En efecto:

Consideremos la función:

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

Note que aplicando el teorema anterior:

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

Ahora 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 $d$ de orden en la doble suma (1.1) y conservaremos la condición $j \mid n$.

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

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 [2], 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 $G(\frac{x}{j})$ 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:

$$F(x) = \sum_{j \leqslant x} \mu(j) G\left(\frac{x}{j}\right) \tag{1.2}$$

Además de ello, ya tenemos algunos valores de $\mu$, $\mu(1) = 1$, $\mu(2) = \mu(3) = -1$, $\mu(4) = 0$ 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:

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

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

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

Finalmente:

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

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

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

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

**Teorema 1.3.** Sea $n \geqslant 1$, 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 $j \leqslant x$, 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:

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

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 $d = p_{i_1} \dots p_{i_j}$ donde $\mathcal{K} = \{i_1, \dots, i_j\} \subseteq \{1, \dots, k\}$, 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 menciono 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 formal 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 $g(1) = \dfrac{1}{f(1)}$, ahora supongamos que $g$ se ha definido para todos lo valores $1 < k < n$, luego como $f * g(n) = 0$:

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

Así:

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

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

□

Esto nos permite dotar a estas funciones aritmética de una estructura de grupo Abeliano, 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 $d \mid xy$ puede escribirse de manera única como $d = mn$ donde $m \mid x$ y $n \mid y$, 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. □

**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 [**?**]

**Demostración.** Queremos ver que:

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

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 $k_1k_2 \geq 2$ tal que $k_1k_2 < n$ y sean $n_1$ y $n_2$ tales que $n_1n_2 = n$ y $(n_1, n_2) = 1$, por (1.6) tenemos que:

$$\begin{aligned}
0 &= \sum_{d|n_1n_2} f(d)g\left(\frac{n_1n_2}{d}\right) \\
&= \sum_{\substack{d_1|n_1 \\ d_2|n_2 \\ d_1d_2<n}} f(d_1)f(d_2)g\left(\frac{n_1}{d_1}\right)g\left(\frac{n_2}{d_2}\right) + g(n_1n_2) \\
&= \sum_{\substack{d_1|n_1 \\ d_2|n_2}} f(d_1)f(d_2)g\left(\frac{n_1}{d_1}\right)g\left(\frac{n_2}{d_2}\right) + g(n_1n_2) - g(n_1)g(n_2) \\
&= (f * g)(n_1)(f * g)(n_2) + (g(n_1n_2) - g(n_1)g(n_2))
\end{aligned}$$

Luego:

$$g(n_1)g(n_2) = e(n_1)e(n_2) + g(n_1n_2)$$

Y como $n_1n_2 \geq 2$, entonces $n_1 \geq 2$ o $n_2 \geq 2$, así $e(n_1)e(n_2) = 0$, por tanto $g(n_1n_2) = g(n_1)g(n_2)$. □

**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 $\varphi$ de Euler**

La propiedad del teorema (1.3) nos permite manipular sumas con condiciones de coprimalidad, 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 $\varphi$ 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 $\varphi$ es multiplicativa, por el teorema (1.7) basta ver que en efecto $\mu$ lo es, algo interesante teniendo en cuenta que esta propiedad en cursos de álgebra se sigue de $\mathbb{Z}_{mn} = \mathbb{Z}_m \times \mathbb{Z}_n$ si $(m, n) = 1$.

**Teorema 1.10.** La función $\mu$ es multiplicativa:

**Demostración.** Supongamos que $n = n_1n_2$, 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 $k = k_1k_2$ tal que $1 < k < n$ y $(k_1, k_2) = 1$ y sean $n_1, n_2$ tales que $n_1n_2 = n$ y $(n_1, n_2) = 1$, tenemos que:

$$\begin{aligned}
0 &= \sum_{d|n_1n_2} \mu(d)\\
&= \sum_{\substack{d_1|n_1\\ d_2|n_2\\ d_1d_2<n}} \mu(d_1)\mu(d_2) + \mu(n_1n_2)\\
&= \sum_{d_1|n_1} \mu(d_1) \sum_{d_2|n_2} \mu(d_2) + \mu(n_1n_2) - \mu(n_1)\mu(n_2)\\
&= \mu(n_1n_2) - \mu(n_1)\mu(n_2).
\end{aligned}$$

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:

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

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:

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

□

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:

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

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 $\sigma$ y $\tau$ son multiplicativas por ser convolución de funciones multiplicativas. Observemos una última propiedad de estas funciones, que nos permite caracterizar la noción de ser primo.

**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 $\mu$ o $\varphi$ 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:

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

Tienden a ser suaves conforme $x \to \infty$ 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.

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

$$f(c-) = \lim_{x \to c^-} f(x), \; c \in (a, b]$$
$$f(c+) = \lim_{x \to c^+} f(x), \; c \in [a, b)$$

**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 $x$.

### 1.3.1. La integral de Riemann-Stieltjes

Sean $P = \{x_0, x_1, ..., x_n\} \in \mathcal{P}[a, b]$ (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 $P = \{x_0, x_1, ..., x_n\} \in \mathcal{P}[a, b]$ (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 $\alpha$ en $[a, b]$.

ii) Decimos que $f$ es **Riemann-Integrable** con respecto a $\alpha$ 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 $\alpha$ es llamada *integrador*.

Note que la integral de Riemann no es más que un caso particular de la de Riemann-Stieltjes, cuando $\alpha(x) = x$.

**Teorema 1.14** ([3], Teorema 7.11)**.** Sea $\alpha$ una función escalonada definida en $[a, b]$ con salto $\alpha_k$ en $x_k$.

Sea $f$ una función definida en $[a, b]$ tal que $f$ y $\alpha$ 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 [3], sin embargo, nos será útil explorar la idea.

Note que $\alpha$ 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 $\alpha$ tiene salto $\alpha_k$ en un punto $x_k \in [a, b]$, no es difícil ver que:

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

La prueba de esto se encuentra también en [3] [Teorema 7.9], en efecto si repetimos esto para cada $x_k$ obtenemos la suma deseada.

Sea $f$ continua en $[0, \infty]$, 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:

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

**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

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

Con ayuda de esto vamos a obtener una representación integral de la función contadora de primos y también la equivalencia esperada, estas propiedades se seguirán del teorema de sumación parcial de Abel, este teorema resultará ser una aplicación de la fórmula de integración por partes para integrales de Riemann-Stieltjes.

### 1.3.2. Algunas propiedades de la integral de Riemann-Stieltjes

Comencemos por la fórmula de integración por partes:

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

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

Por último, 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 $f \in R(\alpha)$ 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 [3], 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.** 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. □

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

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

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.** Tenemos las siguientes identidades:

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

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

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

Fijemos $x \geqslant 2$. 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 $\pi(x) = \sum_{n\leqslant x} \frac{\mathbb{1}_p(n)\log(n)}{\log(n)}$ y que $\vartheta(t) = 0$ para todo $t < 2$ tenemos que:

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

$\square$

# Bibliografía


[1] Bernhard Riemann. On the number of primes less than a given magnitude. *Complete Works. Kendrick Press*, 2004.

[2] Norman Levinson. A motivated account of an elementary proof of the prime number theorem. *The American Mathematical Monthly*, 76(3):225–245, 1969.

[3] Tom M Apostol. *Mathematical analysis; 2nd ed.* Addison-Wesley series in mathematics. Addison-Wesley, Reading, MA, 1974.

[4] Prapanpong Pongsriiam. *Analytic Number Theory for Beginners*, volume 103. American Mathematical Society, 2023.

[5] T.M. Apostol. *Introduction to Analytic Number Theory*. Undergraduate Texts in Mathematics. Springer New York, 1998.

[6] Graham James Oscar Jameson. *The prime number theorem*. Cambridge University Press, 2003.

[7] USR Murty. *Problems in analytic number theory*, volume 206. Springer Science & Business Media, 2007.

[8] Samuel J Patterson. *An introduction to the theory of the Riemann zeta-function*. Cambridge University Press, 1995.

[9] E.M. Stein and R. Shakarchi. *Complex Analysis*. Princeton lectures in analysis. Princeton University Press, 2010.

[10] Harold Davenport. *Multiplicative number theory*, volume 74. Springer Science & Business Media, 2013.

[11] Don Zagier. Newman's short proof of the prime number theorem. *The American mathematical monthly*, 104(8):705–708, 1997.

[12] Andrew Granville and Greg Martin. Prime number races. *The American Mathematical Monthly*, 113(1):1–33, 2006.

[13] M Ram Murty and V Kumar Murty. *Non-vanishing of L-functions and applications*. Springer Science & Business Media, 2012.

[14] 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.

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