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 mayo de 2024

Abstract

The prime number theorem is the assetion 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

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*
>
> **— B. 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, por ejemplo, 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, el 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 detrás de este problema viene de estudiar la serie de Taylor de $\sin x$:

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

Así:

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

Euler 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...

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

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

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

Lo que le daría la "solución" al problema y lo motivaría a generalizarlo con la serie absolutamente convergente:

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

Euler encuentra una fórmula para obtener los valores de esta función en los 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 Dirichlet y Riemann, siendo este último quien estudió íntimamente la función ζ y la llevó a la fama que posee actualmente, 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:

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

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 ζ no se anulaba en la recta vertical de los complejos con parte real 1, sobre el plano complejo, algo sencillamente maravilloso.

Dirichlet por otro lado, en 1837 había probado que dados $a, q \in \mathbb{N}$ tales que $(a, q) = 1$, entonces hay infinitos primos en la progresión $a + kq$. La prueba sería basada en las ideas de Euler, estudiar la divergencia de:

$$\sum_{p\equiv a \text{ mód } q} \frac{1}{p}$$

Sin embargo, Dirichlet, en el artículo de su prueba del teorema de progresiones aritmética afirma que en un principio la prueba que presentó no era la que originalmente pensó; comenta que la prueba usaba argumentos un poco más indirectos y dependía del hecho de que la función $L(s,\chi)$, no se anulaba en los complejos con $\Re(s) = 1$, por lo que finalmente, al no poder probarlo, optó por un argumento distinto.

Algo natural que se preguntaron los matemáticos es cómo se distribuyen los primos de dicho conjunto o si aquí es válido el TNP, de la Vallée Poussin también en 1896 demostraría que la función contadora de primos restringida sobre la progresión aritmética, ie. $\pi_{a,q}(x)$ tiene el comportamiento asintótico:

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

Donde φ 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.

La prueba de este resultado no es distinta de la del teorema de los números primos ya que en esencia depende del hecho de que $L(s,\chi) \neq 0$ si $\Re(s) = 1$. Así, nuestro trabajo será construir las herramientas para esclarecer estas ideas que concluirán cuando probemos la no nulidad de $L(\chi, s)$ y $\zeta(s)$ en $\Re(s) = 1$, la idea es que al final de este trabajo para el lector no sea confuso que el TNP se siga de esto, para ello estudiar las ideas subyacentes será muy importante. Resultará conveniente que el lector esté familiarizado con algunos conceptos de variable compleja, análisis real y teoría de grupos, ya que aunque presentaremos gran parte de los preliminares aquí, no profundizaremos en ellos como sí se haría en un curso de análisis o álgebra.

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 $\dfrac{\zeta'(s)}{\zeta(s)}$, 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 $p^m \,||\, n$ 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:

$$n = \prod_{p^m \| n} p^m$$

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:

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

Note que si f es completamente aditiva:

$$f(n) = f\left(\prod_{i=1}^{m} p_i^{k_i}\right) = k_1 f(p_1) + \ldots + k_m f(p_k) = \sum_{i=1}^{m} f(p_i) k_i$$

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 es completamente multiplicativa:

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

□

Una propiedad adicional que será útil para caracterizar estas funciones 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 $f(1 \cdot n) = f(1)f(n)$, $f(1) = 1$.

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:

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

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.[2]

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 en (2.1) 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 [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 $G(\frac{x}{j})$ 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 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:

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

Por tanto al reemplazar (2.3) en (2.2), 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 (2.4) se anule, y dado que no tenemos condiciones sobre F, la función μ 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 (2.2) 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:

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

La fórmula en (2.5) 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:

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

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 (2.5).

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?, 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 $\left(\dfrac{x}{m}, \dfrac{y}{n}\right) = 1$. 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 [2]

Demostración. Queremos ver que:

$$g(n_1n_2) = g(n_1)g(n_2) \quad \text{si} \quad (n_1, n_2) = 1. \tag{1.7}$$

Procedamos por inducción matemática. Sea $n = n_1n_2$, si $n_1n_2 = 1$, 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 (2.7) 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 (2.6) tenemos que:

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

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.

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

1.2.1. La función φ de Euler

La propiedad del teorema (2.3) 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 esta propiedad es 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 (2.7) basta ver que en efecto μ lo es, algo en un principio sorprendente teniendo en cuenta que esta propiedad en cursos de álgebra se sigue de:

$$\mathbb{Z}_{mn} = \mathbb{Z}_m \times \mathbb{Z}_n \quad \text{si} \quad (m,n) = 1$$

Teorema 1.10. La función μ 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:

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

□

Esta identidad también puede probarse usando propiedades de la convolución:

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

1.2.2. Las funciones número y suma de divisores

Podemos usar la convolución de manera conveniente para reescribir algunas funciones aritmética, por ejemplo:

$$\sigma(n) = \sum_{j|n} j = N * 1(n)$$

Bibliografía

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

[2] A.J. Hildebrand. *Introduction to Analytic Number Theory Lecture Notes*. 2005 url: `https://bit.ly/3V7a7G0`.

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

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

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

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

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

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

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

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

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

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