Introducción a la Teoría Analítica de Números

Pablo De Nápoli

clase 1

1. Introducción

La teoría analítica de números es una rama de la matemática donde se utilizan los métodos del análisis, tales como el análisis de variable compleja o la transformada de Fourier, para estudiar las propiedades de los números enteros.

En este curso, nos centraremos en uno de los problemas principales de la teoría: el estudio de la distribución de los números primos (y problemas relacionados). A fin de poder enunciar el teorema principal a este respecto, introduzcamos la función de conteo de primos $\pi(x)$, definida como la cantidad de números primos que son menores o iguales que x.

Entonces, el teorema sobre la distribución de los números primos (que será uno de los teoremas centrales de este curso) afirma que:

$$\pi(x) \sim \frac{x}{\log x} \text{ cuando } x \to +\infty \tag{1}$$

Esta relación es un ejemplo de una relación asintótica.

El símbolo $\sim$ tiene el significado que definimos a continuación:

Definición 1.1 *Sean $f, g : \mathbb{R} \to \mathbb{R}$. Decimos que f y g son asintóticamente equivalemntes cuando $x \to +\infty$ y escribimos*

$$f(x) \sim g(x) \text{ cuando } x \to +\infty$$

si y sólo si

$$\lim_{x \to +\infty} \frac{f(x)}{g(x)} = 1$$

de modo que la relación (1) signfica que:

$$\lim_{x \to +\infty} \frac{\pi(x)}{\left(\frac{x}{\log x}\right)} = 1 \text{ cuando } x \to +\infty$$

Este teorema fue conjeturado empíricamente por Gauss (1792-3) y Legendre (1808) a partir de la evidencia empírica proporcionada por las tablas de números primos disponibles en aquella época.

La siguiente tabla, confeccionada con el programa Pari/Gp, muestra cuál es la bondad de estas aproximaciones para $x \leq 10^9$:

x	$\pi(x)$	$x/\log x$	$\frac{\pi(x)}{(x/\log x)}$
10^1	4	4,3429	0,9210
10^2	25	21,7147	1,1513
10^3	168	144,7648	1,1605
10^4	1229	1085,7362	1,1320
10^5	9592	8685,8896	1,1043
10^6	78498	72382,4137	1,0845
10^7	664579	620420,6884	1,0712
10^8	5761455	5428681,0238	1,0613
10^9	50847534	48254942,4337	1,0537

2. La función zeta de Riemann

Para $s > 1$, definimos la *función zeta de Riemann* por

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

(Se sabe desde análisis I que esta serie converge si $s > 1$ y diverge si $= 1$).

Un paso decisivo para demostrar el teorema de los números primos fue dado por Riemann quien en su célebre trabajo publicado en 1859 (¡de apenas ocho páginas!), en el que Riemann desarrolló un método para conectar las propiedades de esta función con los números primos.

En él, Riemann tuvo la idea de considerar la función zeta para valores complejos de la variable s, y estudiarla utilizando los métodos de variable compleja.

Recordamos que para valores complejos de la variable s, n^s se define por:

$$n^s = e^{s \log n}$$

(Aquí $\log n$ designa el logaritmo usual en los reales). Entonces, dado que

$$|n^s| = n^{\mathrm{Re}(s)}$$

la serie que define la función zeta converge si $\mathrm{Re}(s) > 1$, por lo que tiene sentido definirla en el semiplano $\mathrm{Re}(s) > 1$ del plano complejo.

Además, por el test de Weierstrass, dicha serie converge uniformenete en cada semiplano $\mathrm{Re}(s) \geq 1 + \varepsilon$ (con $\varepsilon > 0$); y en particular esto significa que la serie converge uniformente sobre los compactos del semiplano $\mathrm{Re}(s) > 1$. En particular, esto implica que la función zeta de Riemann es una función analítica en dicho semiplano.

La conexión entre la función zeta y los números primos se debe a una notable identidad descubierta por Euler en 1737, que puede considerarse como una versión analítica del teorema fundamental de la aritmética:

Teorema 2.1 *Para $Re(s) > 1$, la función zeta admite la siguiente representación en producto infinito*

$$\zeta(s) = \prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-s}} \tag{2}$$

donde $\mathbb{P}$ denota el conjunto de los números primos.

Prueba: Para comprender la idea de este teorema, comenzamos con un argumento formal (no riguroso), que después formalizaremos. Consideramos la identidad (serie geométrica):

$$\frac{1}{1-z} = 1 + z + z^2 + \ldots + z^k + \ldots$$

válida si $|z| < 1$. Poniendo $z = p^{-s}$ obtenemos que:

$$\frac{1}{1-p^{-s}} = 1 + p^{-s} + p^{-2s} + \ldots + p^{-ks} + \ldots$$

Si multiplicamos esta expresión sobre todos los primos, y efectuamos formalmente la distributiva, obtenemos que:

$$\prod_{p \in \mathbb{P}} \frac{1}{1-p^{-s}} = \prod_{p \in \mathbb{P}} \left(1 + p^{-s} + p^{-2s} + \ldots + p^{-ks} + \ldots\right) = \sum_{n=1}^{\infty} n^{-s} = \zeta(s)$$

ya que en virtud del teorema fundamental de la aritmética, cada entero $n \geq 1$ se escribe de manera única como producto de potencias de primos distintos.

Para efectuar la prueba de la proposición anterior de un modo riguroso, procedemos del siguiente modo. Para cualquier N finito,

$$\prod_{p \leq N} \frac{1}{1-p^{-s}} = \prod_{p \leq N} \left(1 + p^{-s} + p^{-2s} + \ldots + p^{-ks} + \ldots\right) = \sum_{n \in A_N} \frac{1}{n^s}$$

por tratarse del producto de finitas series absolutamente convergentes, donde la última suma se extiende sobre aquellos enteros cuyos factores son todos menores o iguales que N:

$$A_N = \left\{ n = \prod_{p \leq N} p^{e_p} \text{ con } e_p \geq 0 \right\}$$

Entonces

$$\left| \prod_{p \leq N} \frac{1}{1-p^{-s}} - \zeta(s) \right| \leq \sum_{n > N} \frac{1}{n^{\sigma}}$$

con $\sigma = \mathrm{Re}(s)$. Pero entonces, como la serie

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

converge, podemos hacer que que

$$\left| \prod_{p \leq N} \frac{1}{1-p^{-s}} - \zeta(s) \right| < \varepsilon$$

con tal de elegir $N \geq N_0(\varepsilon)$. (Notar que un producto infinito se interpreta como el límite de los productos parciales, del mismo modo que una serie es el límite de sus sumas parciales.) □

Observación: La misma demostración muestra que la convergencia del producto infinito en la fórmula (2) es unifome en cada semiplano $\mathrm{Re}(s) \geq 1 + \varepsilon$.

Euler utilizó esta fórmula para dar una demostración analítica de la existencia de finitos primos. Para ello observó que:

$$\lim_{s \to 1^+} \zeta(s) = +\infty \ (s \in \mathbb{R}) \tag{3}$$

En efecto para cada N,

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

Como la serie armónica diverge, haciendo que $N \to +\infty$, obtenemos (3). Euler observó entonces que que la fórmula (2) implica que existen infinitos primos, puesto que si sólo existieran finitos primos el limíte $\lim_{s \to 1^+} \zeta(s)$ debería ser finito.

Un razonamiento similar permite obtener un resultado más fuerte:

Teorema 2.2 (Euler) *La serie*

$$\sum_{p \in \mathbb{P}} \frac{1}{p} \tag{4}$$

diverge.

Prueba: Utilizando el mismo razonamiento del teorema anterior:

$$\prod_{p \leq N} \frac{1}{1-p^{-1}} = \sum_{n \in A_N} \frac{1}{n} \geq \sum_{n \leq N} \frac{1}{n}$$

Por otra parte, si utilizamos la desigualdad

$$\frac{1}{1-x} \leq e^{2x} \ \forall \ x \in \left[0, \frac{1}{2}\right]$$

con $x = \frac{1}{p}$, obtenemos que:

$$\prod_{p \leq N} \frac{1}{1-p^{-1}} \leq \prod_{p \leq N} e^{2/p} = \exp\left(2 \sum_{p \leq N} \frac{1}{p}\right)$$

Cuando $N \to +\infty$, como la serie armónica diverge, concluimos que (4) también diverge. □

3. El teorema de Dirichlet

Esta demostración analítica de la infinitud de los primos es sin duda más sofisticada que la demostración de Euclides (por reducción al absurdo) de este hecho.

Sin embargo, el argumento de Euler fue adaptado por Dirichlet para probar el teorema siguiente

Teorema 3.1 (Dirichlet) *Supongamos que $a, b \in \mathbb{N}$ son coprimos. Entonces, en la progresión aritmética $an + b$ existen infinitos primos (Es decir: existen infinitos primos que son congruentes a b módulo a).*

Si bien existen argumentos elementales similares al de Euclides para probar casos particulares de este teorema, todas las demostraciones conocidas de este teorema en toda su generalidad emplean métodos analíticos. Dirichlet dedujo su teorema probando que la serie

$$\sum_{p \equiv b \pmod{a}} \frac{1}{p}$$

(donde la suma recorre los primos en la progresión aritmética considerada) diverge.

También existe una versión del teorema de los números primos para progresiones aritméticas. Para enunciarlo introducimos la indicatriz de Euler $\varphi(a)$ definida como la cantidad de enteros b con $1 \leq b \leq a$ tales que b es coprimo con a.

También definimos la función de conteo $\pi(x; a, b)$ como la cantidad de primos de la forma $ab + n$ que son menores o iguales que x. Entonces el teorema de los números primos para progresiones aritméticas establece que:

$$\pi(x; a, b) \sim \frac{1}{\varphi(a)} \frac{x}{\log x} \text{ cuando } x \to +\infty$$

Esto significa que, fijado $a \in \mathbb{N}$, los números primos se encuentran (asintóticamente) repartidos en forma "pareja" entre las $\varphi(a)$ progresiones progresiones aritméticas correspondientes a las distintas elecciones de un b coprimo con a.

4. Funciones aritméticas

Definición 4.1 *Una función aritmética es una función $f : \mathbb{N} \to \mathbb{C}$. Generalmente el valor $f(n)$ expresará alguna propiedad aritmética del número $n \in \mathbb{N}$*

Algunos ejemplos de funciones aritméticas:

1. La función $\varphi(n)$ de Euler.
2. La función $d(n)$ que cuenta el número de divisores (positivos) de n.

3. La función $\sigma(n)$ que devuelve la suma de los divisores de n. O más generalmente las funciones $\sigma_k(n)$ que devuelven la suma de las potencias k-ésimas de los divisores de n. Simbólicamente podemos escribir la definición de σ_k por

$$\sigma_k(n) = \sum_{d|n} d^k$$

(Notamos que $\sigma_0 = d$ y $\sigma_1 = \sigma$.)

4. La función μ de Möbius que se define del siguiente modo:

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ (-1)^k & \text{si } n = p_1 p_2 \dots p_k \text{ siendo los } p_i \text{ primos distintos} \\ 0 & \text{en otro caso, es decir si n es divisible por un cuadrado} \end{cases}$$

Definición 4.2 *Definimos la función aritmética $I(n)$, llamada* función aritmética identidad *por*

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

Muchas identidades con funciones aritméticas involucran sumas sobre los divisores positivos de un entero $n \in \mathbb{N}$. Veamos algunos ejemplos:

Teorema 4.1 *Para todo $n \in \mathbb{N}$,*

$$\sum_{d|n} \mu(d) = I(n) \tag{5}$$

Prueba: Para $n = 1$ el resultado es trivial, luego podemos suponer $n > 1$. Al calcular la suma del enunciado, sólo resultan no nulos los términos correspondientes a divisores de n que son el producto de primos distintos que aparezcan en la factorización de n. Luego, si n posee k factores primos distintos

$$\sum_{d|n} \mu(d) = 1 + \sum \mu(p_{i_1}) + \sum \mu(p_{i_1} p_{i_2}) + \dots + \sum \mu(p_{i_1} p_{i_2} \dots p_{i_k})$$

donde $p_{i_1} p_{i_2} \dots p_{i_j}$ representa una elección de j factores primos distintos entre los k posibles.

Pero por definición de μ, $\mu(p_{i_1} p_{i_2} \dots p_{i_j}) = (-1)^j$, y hay $\binom{k}{j}$ elecciones posibles de j factores primos entre k. Queda pues:

$$\sum_{d|n} \mu(d) = 1 - \binom{k}{1} + \binom{k}{2} + \dots + (-1)^k \binom{k}{k} = (1 + (-1))^k = 0$$

utilizando el teorema del binomio de Newton. □

Teorema 4.2 *Para cada $n \in \mathbb{N}$,*

$$\sum_{d|n} \varphi(d) = n \tag{6}$$

Prueba: Para cada divisor d de n, consideramos el conjunto

$$A_d = \{b \in \mathbb{N} : 1 \leq b \leq n, (b, n) = d\}$$

Los conjuntos A_d forman una partición del conjunto $\{1, 2, \ldots, n\}$, de modo que:

$$\sum_{d|n} \#(A_d) = n \tag{7}$$

Por otra parte si $b \in A_d$, d es divisible por n y como

$$d\left(\frac{b}{d}, \frac{n}{d}\right) = (b, n)$$

tenemos que la función $f : A_d \to B_d$ definida por $f(b) = \frac{b}{d}$ establece una biyección entre A_d y el conjunto

$$B_d = \left\{c \in \mathbb{N} : 1 \leq c \leq \frac{n}{d}, \left(c, \frac{n}{d}\right) = 1\right\}$$

En consecuencia, $\#(A_d) = \#(B_d) = \varphi\left(\frac{n}{d}\right)$, por la definición de φ. Reemplazando en (7), vemos que:

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

lo que, llamando $d' = \frac{n}{d}$, se puede rescribir equivalentemente como:

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

□

Definición 4.3 *Sean $f, g : \mathbb{N} \to \mathbb{C}$ funciones aritméticas. Definimos su* ***convolución de Dirichlet*** *como una nueva función aritmética $f * g : \mathbb{N} \to \mathbb{C}$ dada por*

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

Esto puede escribirse equivalentemente

$$(f * g)(n) = \sum_{n=d_1 d_2} f(d_1) g(d_2)$$

(llamando $d_1 = d, d_2 = \frac{n}{d}$). Notamos que en esta expresión los roles de f y g son simétricos. En consecuencia, la convolución de Dirichlet es conmutativa, es decir

$$f * g = g * f$$

.

Observación: Se tiene que

$$f * I = I * f = f$$

Esto significa que la función aritmética I es el elemento neutro para la convolución de Dirichlet. Esto justifica la denominación que le hemos dado de función aritmética identidad.

Observación: La convolución de Dirichlet es asociativa, esto significa que si f, g y h son tres funciones aritméticas, entonces:

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

Prueba:

$$(f * g) * h(n) = \sum_{cd_3=n} (f * g)(c)h(d_3) = \sum_{cd_3=n} \left\{ \sum_{d_1 d_2 = c} f(d_1)g(d_2) \right\} h(d_3)$$

$$= \sum_{d_1 d_2 d_3 = n} f(d_1)f(d_2)f(d_3)$$

Si asociamos al revés, $f * (g * h)(n)$ llegaríamos a la misma expresión. □

Obseración: También se verifica la propiedad distributiva con respecto a la suma usual de funciones aritméticas

$$f * (g + h) = f * g + f * h$$

donde $g + h$ se define por:

$$(g + h)(n) = g(n) + h(n)$$

El hecho de que la convolución de Dirichlet verifique las propiedades usuales del producto, significa que el conjunto de las funciones aritméticas tiene estructura de **anillo conmutativo** con respecto a las operaciones de suma (usual) y convolución de Dirichlet.

Ejemplo: Introduzcamos una función aritmética u, llamada **función unidad** por

$$u(n) = 1 \; \forall \; n \in \mathbb{N}$$

Entonces la ecuación (5) se puede escribir

$$\mu * u = I$$

Como I es el neutro de la convolución de Dirichlet, esto significa que u y μ son elementos inversos para la convolución de Dirichlet. Podemos escribir esto simbólicamente como

$$\mu = u^{-1}$$

También notamos que la función d puede expresarse por

$$d = u * u$$

Ejemplo: Si introducimos una función aritmética N por

$$N(n) = n \; \forall \; n \in \mathbb{N}$$

la fórmula (5) establece que

$$\varphi * u = N$$

La definición de σ se puede escribir

$$\sigma = N * u$$

y la de σ_k

$$\sigma_k = N^k * u$$

donde

$$N^k(n) = n^k \; \forall \; n \in \mathbb{N}$$

Teorema 4.3 (Fórmula de Inversión de Möbius) *Sean $f, g : \mathbb{N} \to \mathbb{C}$ funciones aritméticas. Entonces:*

$$g(n) = \sum_{d|n} f(d) \; \forall \; n \in \mathbb{N} \tag{8}$$

y sólo si

$$f(n) = \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right) = \sum_{d|n} g\left(\frac{n}{d}\right)\mu(d) \; \forall \; n \in \mathbb{N} \tag{9}$$

Prueba: En términos de la convolución de Dirichlet, la ecuación (8) significa que

$$g = f * u$$

Convolucionando ambos miembros con μ, y utilizando la propiedad asociativa:

$$g * \mu = (f * u) * \mu = f * (u * \mu) = f * I = f$$

con lo que $f = g * \mu$ que es la afirmación (9).

Recíprocamente si vale (9), esto significa que $f = g * \mu$ y convolucionando con u,

$$f * u = (g * \mu) * u = g * (\mu * u) = g * I = g$$

que es la afirmación (8). □

Como ejemplo de aplicación, a partir de (5), tomando $f = \varphi, g = N$, podemos deducir una fórmula para la indicatriz de Euler φ:

Teorema 4.4 *Para todo $n \in \mathbb{N}$,*

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