Las funciones ζ y L en la teoría de los números primos

UNIVERSIDAD
COMPLUTENSE
MADRID

Antonio Pulido Iniesta
Tutores: Dr. Fernando Chamizo Lorente y Dra. María Jesús Carro Rossell
Facultad de Ciencias Matemáticas
Universidad Complutense de Madrid

Trabajo de Fin de Grado presentado para optar al Grado de
Grado en Matemáticas

Curso 2024-2025

Abstract

This work explores two central objects in analytic number theory: the Riemann zeta function and the Dirichlet L-functions, focusing on their connection with the distribution of prime numbers and the important role they play in nowadays research in this field. Starting from classical questions such as the infinitude of primes as well as in arithmetic progressions, we delve into complex analysis tools that lead to fundamental theorems like the Prime Number Theorem and Dirichlet's theorem which are discussed and outlined analytically. We examine key analytic properties of these functions, including their Euler products, meromorphic extensions, and functional equations. Special emphasis is placed on the non-vanishing of L-functions at $s = 1$. Furthermore, some applications of L-functions to the study of class numbers of quadratic forms are presented. The goal is to highlight the power of analytic techniques in solving deep arithmetic problems, to emphasize the mathematical richness underlying analytic number theory and how these functions offer a unified framework for understanding various classical problems in the theory of primes.

Índice general

1. Motivación: dos resultados aritméticos **5**

2. La extensión meromorfa de ζ **12**

3. La distribución de los números primos **19**

4. Las funciones L y el teorema de Dirichlet **24**

5. Ecuaciones funcionales y caracteres cuadráticos **31**

6. El número de clases **40**

Capítulo 1

Motivación: dos resultados aritméticos

En este capítulo probaremos dos resultados relacionados con los números primos que nos servirán para ver la necesidad de definir las funciones L de Dirichlet, así como de la función ζ de Riemann y estudiar sus propiedades en búsqueda de una mayor comodidad a la hora de resolver ciertos problemas de la teoría de números.

Resultado 1: La suma de los inversos de los primos diverge.

Teorema 1.1. *[14]*

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

Demostración. Sea p primo, se tiene que:

$$(1 - p^{-s})^{-1} = \frac{1}{1 - p^{-s}} = \sum_{n=0}^{\infty} p^{-sn}, \text{ pues } |p^{-s}| < 1, \ \forall \ \Re(s) > 1, \ p \text{ primo.}$$

Luego,

$$\prod_p (1 - p^{-s})^{-1} = \prod_p \sum_{n=0}^{\infty} p^{-sn};$$

Sea $\varepsilon > 0, \ \exists N$ tal que:

$$|\zeta(s) - \prod_{p \leq N} (1 - p^{-s})^{-1}| \leq |\sum_{n \geq N} \frac{1}{n^s}| \leq \sum_{n \geq N} \frac{1}{n^{\Re(s)}} \leq \varepsilon.$$

Puesto que N es arbitrario, la función ζ de Riemann es absolutamente convergente para $\Re(s) > 1$ y, por el teorema fundamental de la Aritmética, desaparecen los números de la serie que se pueden poner como producto de los primos $p \leq N$. □

Teorema 1.2. *[14] Para $\Re(s) > 1$, $\log(\zeta(s)) = s \int_2^{\infty} \frac{\pi(x)}{x(x^s - 1)} dx$, donde $\pi(x)$ denota la función contadora de primos, es decir, el número de primos menores o iguales que x.*

Demostración. Por el teorema 1.1, ζ no tiene ceros en $\Re(s) > 1$. Por tanto, $\log(\zeta(s))$ está bien definida en dicho dominio y se tiene que

$$\log(\zeta(s)) = -\sum_p \log(1-p^{-s}) = -\sum_{n=2}^{\infty}(\pi(n)-\pi(n-1))\log(1-n^{-s}) =$$

$$= -\sum_{n=2}^{\infty}\pi(n)(\log(1-n^{-s}) - \log(1-(n+1)^{-s}) = \sum_{n=2}^{\infty}\pi(n)\int_n^{n+1}\frac{s}{x(x^s+1)}dx = s\int_2^{\infty}\frac{\pi(x)}{x(x^s+1)}dx.$$

□

Teorema 1.3.

$$\lim_{s\to 1^+}\zeta(s) = \infty.$$

***Nota**: Aquí $s \to 1^+$ indica $s > 1, s$ real, $s \to 1$.*

Demostración. Observemos que para todo $N \geq 1$, $\liminf_{s\to 1^+}\zeta(s) \geq \liminf \sum_{n=1}^{N}\frac{1}{n^s} = \sum_{n=1}^{N}\frac{1}{n}$. Por tanto, $\liminf_{s\to 1^+}\zeta(s) \geq \sum_{n=1}^{\infty}\frac{1}{n} = \infty$. □

Corolario 1.4. *Existen infinitos números primos.*

Teorema 1.5. *$\zeta(s)$ es holomorfa en el semiplano $\Re(s) > 1$.*

Demostración. Sean $f(s) = \zeta(s)$, $f_k(s) = \sum_{n=1}^{k}\frac{1}{n^s}$ y $A = \{\Re(s) > 1\}$. Observemos que la serie converge absolutamente para $\Re(s) > 1$ pues:

$$\sum_{n=1}^{\infty}\Big|\frac{1}{n^s}\Big| = \sum_{n=1}^{\infty}\frac{1}{n^{\Re(s)}} < \infty.$$

Veamos que $(f_k)_k \to f$ uniformemente en cualquier semiplano $\Re(s) \geq t$ con $t > 1$, en particular, en cualquier compacto $K \subset A$. Dado $\varepsilon > 0$,

$$|f(s) - f_k(s)| = \Big|\sum_{n=k+1}^{\infty}\frac{1}{n^s}\Big| \leq \sum_{n=k+1}^{\infty}\frac{1}{n^{\Re(s)}}.$$

Como $\zeta(s)$ es absolutamente convergente en dicho semiplano, existe un $N \in \mathbb{N}$ tal que para todo $k \geq N$, se tiene que $|f(s) - f_k(s)| \leq \varepsilon$, en $\Re(s) \geq t$. Además, cada f_k es holomorfa en A y $(f_k) \to f$ uniformemente en todo compacto de A, luego por el criterio de Weierstrass, f también es holomorfa en A. □

Proposición 1.6. *Existe una constante C tal que para cualquier $s \geq \frac{1}{2}$ y cualquier p primo se verifica que:*

$$|p^{-s} + \log(1-p^{-s})| \leq C \cdot p^{-2s}.$$

Demostración. Sea $f(x) = \log(1-x)$. Por el teorema de Taylor aplicado a $f(x)$ se tiene que: $\log(1-p^{-s}) = -p^{-s} - \sum_{k=2}^{\infty}\frac{p^{-sk}}{k}$. Por tanto, tomando $C = \frac{1}{1-\frac{1}{\sqrt{2}}}$ se verifica lo siguiente:

$$|p^{-s} + \log(1-p^{-s})| \leq \sum_{k=2}^{\infty}\frac{p^{-sk}}{k} \leq \sum_{k=2}^{\infty}p^{-sk} = (\sum_{k=0}^{\infty}p^{-sk})p^{-2s} \leq Cp^{-2s}.$$

□

Teorema 1.7. $\sum_p (p^{-s} + \log(1-p^{-s}))$ *converge para cualquier* $s > \frac{1}{2}$.

Demostración. Por la proposición 1.6 se tiene que:

$$\sum_p p^{-s} + \log(1-p^{-s}) \leq \sum_p C \cdot p^{-2s} \leq C \cdot \sum_{n=1}^{\infty} \left(\frac{1}{n^2}\right)^s < \infty \iff s > \frac{1}{2}.$$

□

Corolario 1.8.

$$\lim_{N\to\infty} \sum_{p\leq N} \frac{1}{p} = \infty.$$

Demostración. Por el teorema 1.7, tenemos que $\exists\, C(s)$ tal que:

$$\sum_p (p^{-s} + \log(1-p^{-s})) = C(s).$$

Se verifica que $\lim_{s\to 1^+} C(s) = K$ para cierta constante K, pues la serie converge uniformemente para $s > \frac{1}{2}$, en particular para $s \to 1^+$, luego la función $C(s)$ es continua para $s > \frac{1}{2}$ y, por tanto, debe existir $\lim_{s\to 1^+} C(s)$. Además, se tiene que, $\forall s > 1$, la serie se puede separar en dos series convergentes, que se pueden manipular en la ecuación:

$$\sum_p p^{-s} + \sum_p \log(1-p^{-s}) = C(s),$$

$$\sum_p p^{-s} = \log(\prod_p (1-p^{-s})^{-1}) + C(s).$$

Tomando límites a ambos lados cuando $s \to 1^+$, se obtiene que:

$$\lim_{s\to 1^+} \sum_p \frac{1}{p^s} = \lim_{s\to 1^+} (\log(\zeta(s)) + C(s)).$$

Usando el Teorema 1.3, que $\log x$ es continua y lo dicho anteriormente sobre $C(s)$, se tiene que $\lim_{s\to 1^+} \sum_p \frac{1}{p^s} = \infty$. Por último, notemos que para cada $s > 1$ y $N \in \mathbb{N}$, se cumple que $\sum_{p\leq N} \frac{1}{p^s} \leq \sum_{p\leq N} \frac{1}{p}$. Por tanto, $\liminf_{N\to\infty} \sum_{p\leq N} \frac{1}{p} \geq \sum_p \frac{1}{p^s}$ para todo $s > 1$. Finalmente, haciendo tender $s \to 1^+$ se obtiene el resultado. □

Vamos a definir ahora 4 caracteres y sus respectivas funciones L de Dirichlet asociadas.

Definición 1.9. Definimos los caracteres módulo 10 como las funciones $\chi_j : \mathbb{Z} \to \mathbb{C}$, $j \in \{0,1,2,3\}$ tales que:

$$\chi_j(n) = \begin{cases} i^{jk} & \text{con } 3^k \equiv n \pmod{10} \text{ si } \operatorname{mcd}(n,10) = 1, \\ 0 & \text{si } \operatorname{mcd}(n,10) \neq 1. \end{cases}$$

Y sus respectivas funciones L de Dirichlet, que las denotaremos como $L_j(s)$,

$$L_j(s,\chi_j) = \sum_{n=1}^{\infty} \frac{\chi_j(n)}{n^s} \quad \textit{para } \Re(s) > 1.$$

Lo primero que cabe preguntarse es si estos caracteres están bien definidos, es decir, si $\forall\ n,\ \exists\ k$ tal que $3^k \equiv n \pmod{10}$ y si da igual el k que elijamos. Eso es lo que probamos en la siguiente proposición.

Proposición 1.10. *Los caracteres χ_j están bien definidos.*

Demostración. Sin pérdida de generalidad se puede trabajar solo con los n tales que $\mcd(n,10)=1$, pues de lo contrario, la función es idénticamente nula. Sea n tal que $\mcd(n,10)=1$, podemos suponer que $n \in \{1,3,7,9\}$. Luego, tomando $k=0,1,3,2$, respectivamente, se obtiene la existencia. Supongamos ahora que dado n tal que $\mcd(n,10)=1$, existen k,l distintos, verificando que $3^k \equiv n \equiv 3^l \pmod{10}$. Queremos que $i^{jk}=i^{jl}$ lo cual es equivalente a que $k \equiv l \pmod 4$.
Existen t,s,r,r' tales que $k=4t+r,\ l=4s+r'$ con $r,r' \in \{0,1,2,3\}$. Luego se tiene que:

$$3^k = 3^{4t}\cdot 3^r = 81^t \cdot 3^r \equiv 3^r \pmod{10}.$$

Y lo mismo sucede para 3^l, por tanto:

$$3^r \equiv 3^{r'} \pmod{10} \implies r=r',$$

pues si $r \neq r'$, entonces $3^r \not\equiv 3^{r'} \pmod{10}$. Concluimos así que $k \equiv l \pmod 4 \implies i^{jk}=i^{jl}$ como queríamos. □

Proposición 1.11. *Los χ_j son funciones totalmente multiplicativas, $\chi_j(n)\cdot\chi_j(m)=\chi_j(nm)$, $\forall n,m \in \mathbb{Z}, \forall j$ y*

$$\frac{1}{4}\cdot\sum_{j=0}^{3}\chi_j(n) = \begin{cases} 1 & \text{si } n \equiv 1 \pmod{10}, \\ 0 & \text{en otro caso.} \end{cases}$$

Demostración. Si $\mcd(n,10)\neq 1$ o $\mcd(m,10)\neq 1$ la primera afirmación es trivial. Luego nos restringimos al caso en que $\mcd(n,10)=1=\mcd(m,10)$:

$$\chi_j(n)\cdot\chi_j(m) = i^{jk}\cdot i^{jl},$$

donde $3^k \equiv n \pmod{10}$ y $3^l \equiv n \pmod{10}$. Por tanto, se tiene que:

$$\chi_j(n)\cdot\chi_j(m) = i^{jk}\cdot i^{jl} = i^{j(k+l)} = \chi_j(nm).$$

pues $3^{k+l} \equiv nm \pmod{10}$ multiplicando las congruencias anteriores.
Ahora sea $n \equiv 1 \pmod{10} \implies \mcd(n,10)=1 \implies \chi_j(n)=i^{jk}$ con $k=0$, pues $3^k \equiv n \equiv 1 \pmod{10} \implies \chi_j(n)=1\ \forall j \implies \frac{1}{4}\cdot\sum_{j=0}^{3}\chi_j(n)=1$.
Si ahora $n \not\equiv 1 \pmod{10}$, dos opciones:

- $\mcd(n,10)=1 \implies n=3,7,9 \pmod{10}$ y se tiene que $\chi_j(n)=-\chi_{j'}(n)$ para $j \equiv j' \pmod 2$, $j \neq j'$, luego $\sum_{j=0}^{3}\chi_j(n)=0$.

- $\text{mcd}(n, 10) \neq 1 \implies n = 2, 4, 5, 6, 8 \pmod{10} \implies \chi_j(n) = 0 \ \forall n, \forall j \implies \sum_{j=0}^{3} \chi_j(n) = 0.$

□

Una vez definido esto, lo usaremos para probar el siguiente resultado:

Resultado 2: Hay infinitos primos que terminan en 1.

Teorema 1.12. $\forall j \in \{0, 1, 2, 3\}, \forall\ \Re(s) > 1$, *se tiene que:*

$$L_j(s) = \prod_p (1 - \chi_j(p)p^{-s})^{-1}.$$

Demostración. Análogamente al Teorema 1.1: Sea p primo, se tiene que:

$$(1 - \chi_j(p) \cdot p^{-s})^{-1} = \sum_{n=0}^{\infty} (\chi_j(p) \cdot p)^{-sn}, \text{ pues } |\chi_j(p) \cdot p^{-s}| < 1, \ \forall\ \Re(s) > 1, p \textit{ primo.}$$

Luego:

$$\prod_p (1 - \chi_j(p) \cdot p^{-s})^{-1} = \prod_p \sum_{n=0}^{\infty} (\chi_j(p) \cdot p)^{-sn}.$$

Sea $\varepsilon > 0, \ \exists N$ tal que:

$$|L_j(s) - \prod_{p \leq N} (1 - \chi_j(p) \cdot p^{-s})^{-1}| \leq |\sum_{n \geq N} \frac{\chi_j(p)}{n^s}| \leq \sum_{n \geq N} \frac{1}{n^s} \leq \varepsilon.$$

Pues N es arbitrario, todas las funciones L_j son absolutamente convergentes para $\Re(s) > 1$ y, por el teorema fundamental de la Aritmética, desaparecen los números de la serie que se pueden poner como producto de los primos $p \leq N$. □

Observación 1.13. A diferencia de la prueba del Teorema 1.1, nótese que hemos usado el hecho de que $\chi_j(n) \cdot \chi_j(m) = \chi_j(nm)$, $\forall n, m \in \mathbb{Z}, \forall j$, en los numeradores de cada producto.
Ahí es donde radica la importancia de la definición de las funciones L de Dirichlet, pues al ser los caracteres funciones totalmente multiplicativas, dichas series siempre pueden ponerse como producto de Euler sobre los primos.

Corolario 1.14. *Sea* $F(s) = \prod_{j=0}^{3} L_j(s)$, *se tiene que:*

$$F(s) = \prod_p f_s(p), \ \textit{donde } f_s(n) = \prod_{j=0}^{3} (1 - \chi_j(n) \cdot n^{-s})^{-1}.$$

Nota: $f_s(n)$ es real para s real porque $\chi_0(n)$ y $\chi_2(n)$ son reales y $\chi_1(n)$ y $\chi_3(n)$ son conjugados.

Proposición 1.15. *Existe una constante* C *tal que para cualquier* $s \geq \frac{1}{2}$ *y* p *primo se cumple que:*

$$|c(p) \cdot p^{-s} - \log(f_s(p))| \leq C \cdot p^{-2s} \ \textit{donde } c(n) = \begin{cases} 4 & \textit{si} \quad n \equiv 1 \pmod{10}, \\ 0 & \textit{en otro caso.} \end{cases}$$

Demostración. Sea $p \equiv 1 \pmod{10}$, entonces $\chi_j(p) = 1, \forall j \in \{0,1,2,3\}$, luego $f_s(p) = (1-p^{-s})^{-4} \implies \log(f_s(p)) = -4\log(1-p^{-s})$ y se tiene que:

$$|c(p)\cdot p^{-s} - \log(f_s(p))| = |4p^{-s} + 4\log(1-p^{-s})| \leq 4Cp^{-2s},$$

si $s \geq \frac{1}{2}$, donde $C = \frac{1}{1-\frac{1}{\sqrt{2}}}$ por la proposición 1.6. Renombrando C se tiene el resultado.
Sea ahora $p \not\equiv 1 \pmod{10} \implies p \equiv 3,7,9 \pmod{10}$ y, por conjugación, se tiene que:

$$f_s(p) = (1-p^{-4s})^{-1}.$$

Luego $|c(p)\cdot p^{-s} - \log(f_s(p))| = |\log(1-p^{-4s})| \leq \sum_{k=1}^{\infty} \frac{1}{k}\cdot p^{-4ks} \leq \sum_{k=1}^{\infty} p^{-4ks} = Kp^{-2s}$, donde $K = \sum_{k=0}^{\infty} p^{-2s(2k+1)} \leq \sum_{k=0}^{\infty} p^{-(2k+1)} \leq \sum_{k=0}^{\infty} 2^{-(2k+1)} = \frac{2}{3} = C$. Pues, por el Teorema de Taylor, $\log(1-p^{-4s}) = \sum_{k=1}^{\infty} \frac{-1}{k}\cdot p^{-4ks}$. □

Teorema 1.16.

$$\lim_{s\to 1^+} L_0(s) = \infty.$$

Demostración. La función $L_0(s)$ es igual que la función $\zeta(s)$ pero sin los términos pares y múltiplos de 5 pues, en ese caso, $\chi_0(n) = 0$. Por tanto:

$$L_0(s) = \zeta(s)\cdot(1-2^{-s})\cdot(1-5^{-s}).$$

Como $\lim_{s\to 1^+}\zeta(s) = \infty$ por el Teorema 1.3, se tiene que $\lim_{s\to 1^+} L_0(s) = \infty$. □

Teorema 1.17. *$\Re(L_1(s))$ y $L_2(s)$ convergen a un número positivo cuando $s \to 1^+$.*

Demostración.

$$\Re(L_1(s)) = \sum_{n\equiv 1 \pmod{10}}^{\infty} \frac{1}{n^s} - \sum_{n\equiv 9 \pmod{10}}^{\infty} \frac{1}{n^s} = \sum_{n=1}^{\infty} \Big(\frac{1}{(10n+1)^s} - \frac{1}{(10n+9)^s}\Big) := l(s).$$

Sea S_N la N-ésima suma parcial, $\Re(L_1(s))$ verifica el criterio de Leibniz, luego $\forall N \in \mathbb{N}$:

$$0 < l(s) - S_{2N}(s) \leq \frac{1}{(10(2N+1)+9)^s},$$

$$0 < \liminf_{s\to 1^+} l(s) - S_{2N}(1) \leq \limsup_{s\to 1^+} l(s) - S_{2N}(1) \leq \frac{1}{(10(2N+1)+9)},$$

$$0 < S_{2N}(1) < \liminf_{s\to 1^+} l(s) \leq \limsup_{s\to 1^+} l(s) \leq S_{2N}(1) + \frac{1}{(10(2N+1)+9)}.$$

Como N es arbitrario, tomando límites cuando $N \to \infty$, se obtiene el resultado, pues $\lim_{N\to\infty} S_{2N}(1) > 0$.

Análogamente, considerando:

$$L_2(s) = \sum_{n\equiv 1 \pmod{10}}^{\infty} \frac{1}{n^s} + \sum_{n\equiv 9 \pmod{10}}^{\infty} \frac{1}{n^s} - \sum_{n\equiv 3 \pmod{10}}^{\infty} \frac{1}{n^s} - \sum_{n\equiv 7 \pmod{10}}^{\infty} \frac{1}{n^s}.$$

Para $s > 1, L_2(s)$ es absolutamente convergente, luego reordenando los términos, se tiene que la serie verifica el criterio de Leibniz, transformándola en una serie alternada:

$$L_2(s) = \sum_{k=1}^{\infty} \Big(\frac{1}{(10k+1)^s} - \frac{1}{(10k+3)^s} \Big) - \sum_{k=1}^{\infty} \Big(\frac{1}{(10k+7)^s} - \frac{1}{(10k+7)^s} \Big).$$

Por tanto, se puede trabajar con las mismas desigualdades (aplicadas a $L_2(s)$) para la suma parcial $2N$-ésima que hemos usado para $\Re(L_1(s))$ y se tiene lo mismo que para $\Re(L_1(s))$, pues $S_{2N}(1) > 0$ también. □

Teorema 1.18.

$$\lim_{s \to 1^+} F(s) = \infty.$$

Demostración. Como $L_1(s)$ y $L_3(s)$ son conjugadas, por los teoremas 1.16 y 1.17, se tiene que:

$$\lim_{s \to 1^+} F(s) = \lim_{s \to 1^+} \prod_{j=0}^{3} L_j(s) = \infty.$$

□

Corolario 1.19.

$$\lim_{N \to \infty} \sum_{\substack{p \equiv 1 \pmod{10} \\ p \leq N}} \frac{1}{p} = \infty.$$

Demostración. Por la proposición 1.15, la serie $\sum_p \big(c(p)p^{-s} - \log(f_s(p)) \big)$ converge a un cierto número $K(s), \forall s > \frac{1}{2}$. Además, se verifica que $\lim_{s \to 1^+} K(s) = K$ para cierta constante K, pues la serie converge uniformemente para $s > \frac{1}{2}$, en particular para $s \to 1^+$, luego la función $K(s)$ es continua para $s > \frac{1}{2}$ y, por tanto, debe existir $\lim_{s \to 1^+} K(s)$. Por consiguiente:

$$\sum_p \big(c(p)p^{-s} - \log(f_s(p)) \big) = K(s).$$

Para $s > 1$, ambas series convergen, luego se pueden separar y queda:

$$\sum_{p \equiv 1 \pmod{10}} 4p^{-s} = \log(F(s)) + K(s).$$

Tomando límites cuando $s \to 1^+$ y usando el Teorema 1.18 con un razonamiento análogo al del corolario 1.8, se obtiene el resultado. □

Observación 1.20. Nótese que el resultado implica que hay infinitos primos cuya última cifra es 1. Adaptando ligeramente la demostración se prueba que hay infinitos primos cuya última cifra es $3, 7$ y 9, aunque los resultados expuestos previamente dicen más pues dan la divergencia de ciertas series en los primos.

Capítulo 2

La extensión meromorfa de ζ

En este capítulo, vamos a probar ciertas propiedades de la función ζ de Riemann que nos permitirán extenderla a una función meromorfa en $\mathbb{C}$, así como obtener su famosa ecuación funcional que nos ayudará a calcular ciertos valores concretos como son los llamados ceros triviales de ζ.

Teorema 2.1. *Para $\Re(s) > 1$, se tienen las siguientes igualdades:*

$$\zeta(s) = s\int_1^\infty \frac{\lfloor x\rfloor}{x^{s+1}}dx = \frac{s}{s-1} - \frac{1}{2} - s\int_1^\infty \frac{x - \lfloor x\rfloor - \frac{1}{2}}{x^{s+1}}dx,$$

donde $\lfloor x\rfloor$ denota la parte entera de x.

Demostración. Usando la identidad de Abel, [2], Th.4.2, probaremos la primera igualdad. Sean $a(n) \equiv 1, f_s(x) = \frac{1}{x^s}$, cuya derivada es $f'(x) = \frac{-s}{x^{s+1}}$ y $A(x) = \sum_{n\leq x} a(n) = \lfloor x\rfloor$. La identidad de Abel nos dice que, como f_s' es continua en $[1, x]$ para todo $x \in \mathbb{R}$, $\Re(s) > 1$, se tiene que:

$$\sum_{1<n\leq x} a(n)f_s(n) = A(x)f_s(x) - A(1)f_s(1) - \int_1^x \lfloor t\rfloor f_s'(t)dt, \tag{2.1}$$

$$\sum_{1<n\leq x} \frac{1}{n^s} = \frac{\lfloor x\rfloor}{x^s} - 1 + s\int_1^x \frac{\lfloor t\rfloor}{t^{s+1}}dt, \tag{2.2}$$

pasando el 1 al otro lado y tomando límites cuando $x \to \infty$ se obtiene el resultado. Para ver la otra igualdad vamos a combinar (2.1) con la fórmula de integración por partes de $\int_1^x tf_s'(t)dt$ para obtener la fórmula de sumación de Euler-Maclaurin, [8], para nuestro caso particular:

$$\int_1^x tf_s'(t)dt = xf_s(x) - f_s(1) - \int_1^x f_s(t)dt,$$

$$\sum_{1<n\leq x} a(n)f_s(n) = \lfloor x\rfloor f_s(x) - f_s(1) - \int_1^x \lfloor t\rfloor f_s'(t)dt - xf_s(x) + f_s(1) + \int_1^x f_s(t)dt + \int_1^x tf_s'(t)dt,$$

$$\sum_{1<n\leq x} f_s(n) = \int_1^x f_s(t)dt + \int_1^x (t - \lfloor t\rfloor)f_s'(t)dt + f_s(x)(\lfloor x\rfloor - x), \tag{2.3}$$

$$\sum_{1<n\leq x} f_s(n) = \int_1^x \frac{1}{t^s}dt - s\int_1^x \frac{t - \lfloor t\rfloor}{t^{s+1}}dt + \frac{\lfloor x\rfloor - x}{x^s}, \tag{2.4}$$

Sumando 1 a cada lado y tomando límites cuando $x \to \infty$, se obtiene:

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

$$\zeta(s) = \frac{s}{s-1} - \frac{1}{2} - s\int_1^\infty \frac{t - \lfloor t \rfloor - \frac{1}{2}}{t^{s+1}} dt. \tag{2.5}$$

□

Teorema 2.2. *$\zeta(s)$ se puede extender a una función meromorfa en $\Re(s) > 0$, con un único polo en $s = 1$ con residuo 1.*

Demostración. Sea $A = \{s \in \mathbb{C} : \Re(s) > 0\}$. La última integral del Teorema 2.1 converge en A, pues:

$$\Big| \int_1^\infty \frac{x - \lfloor x \rfloor - \frac{1}{2}}{x^{s+1}} dx \Big| \leq \int_1^\infty \frac{1}{|x^{s+1}|} dx = \int_1^\infty x^{-\Re(s)-1} dx = \frac{1}{\Re(s)}.$$

Luego la segunda igualdad del Teorema 2.1 define una extensión meromorfa de $\zeta(s)$ en A, pues es una función holomorfa en cualquier abierto de A que no contenga a $s = 1$, donde tiene un polo simple de residuo 1. Veamos esto último, sea $f(s) = \frac{s}{s-1} - \frac{1}{2} - s\int_1^\infty \frac{x - \lfloor x \rfloor - \frac{1}{2}}{x^{s+1}} dx$, se tiene que $\lim_{s\to 1}(s-1)f(s) = 1$, lo cual prueba el resultado. □

Observación 2.3. Por el principio de unicidad, a lo sumo hay una posible extensión meromorfa de una función compleja en una región dada. Por tanto, para $\zeta(s)$ en $\Re(s) > 0$ esa es la única extensión meromorfa posible. [12]

A continuación, vamos a probar algunas propiedades de la función Γ de Euler que usaremos para obtener la ecuación funcional de ζ.

Definición 2.4. Definimos la función Γ en $\Re(s) > 0$ como $\Gamma(s) = \int_0^\infty x^{s-1} e^{-x} dx$.

Teorema 2.5. *Se verifica que $\Gamma(s+1) = s\Gamma(s)$, luego Γ tiene una extensión meromorfa a $A = \{\Re(s) > -1\}$, con un único polo en $s = 0$ con residuo igual a 1.*

Demostración.

$$\Gamma(s+1) = \int_0^\infty x^s e^{-x} dx = \big[-x^s e^{-x} \big]_0^\infty + s\int_0^\infty x^{s-1} e^{-x} dx = s\Gamma(s).$$

Luego si definimos $\Gamma(s) := \frac{\Gamma(s+1)}{s}$ para $-1 < \Re(s) < 0$, está bien definida al estarlo $\Gamma(s+1)$, pues $\Re(s+1) > 0$, y es una extensión meromorfa de Γ a A.
Asimismo, se verifica que $\Gamma(s)$ tiene un polo simple en $s = 0$ con residuo 1, pues $\lim_{s\to 0} s\Gamma(s) = \lim_{s\to 0} \Gamma(s+1) = \Gamma(1) = 1$, donde hemos tomado el límite dentro de la función pues $\Gamma(s+1)$ es continua en $s = 0$. □

Teorema 2.6. *Γ admite una extensión meromorfa a $\mathbb{C}$ tal que los polos están en $\mathbb{Z}_{\leq 0}$ y todos son simples.*

Demostración. Sean $A_n = \{\Re(s) > -n\}$, probaré por inducción en n que Γ admite una extensión meromorfa a A_n, $\forall n \in \mathbb{N}$ y que dicha extensión tiene un polo simple en $s = -n$.

Para $n = 0$, se tiene por el teorema anterior. Supongamos ahora que se tiene para n y veamos para $n+1$. Definimos $\Gamma(s) := \frac{\Gamma(s+1)}{s}$ para $-n-1 < \Re(s) < -n$, que está bien definida por estarlo $\Gamma(s+1)$, pues $\Re(s+1) > -n$. Ahora, como la extensión a A_n tiene un polo simple en $s = -n$, se tiene que $\lim_{s\to -n}(s+n)\Gamma(s) = L < \infty$, luego $\lim_{s\to -n-1}(s+n+1)\Gamma(s) = \lim_{s\to -n-1}\frac{(s+n+1)\Gamma(s+1)}{s} = \lim_{t\to -n}\frac{(t+n)\Gamma(t)}{t-1} = \frac{-L}{n+1} < \infty$. Luego $\Gamma(s)$ tiene una extensión meromorfa a A_{n+1} con un polo simple en $s = -n-1$. □

Proposición 2.7. *$\forall n \in \mathbb{N}$, $\Gamma(n) = (n-1)!$ y $\Gamma(\frac{1}{2}) = \sqrt{\pi}$.*

Demostración. La primera parte la probaremos por inducción en n. Para $n = 1$ es trivial pues $\Gamma(1) = 1 = 0!$ Supongamos el resultado cierto para n y veamos para $n+1$. Aplicando el Teorema 2.5 y la hipótesis de inducción, se tiene: $\Gamma(n+1) = n\Gamma(n) = n(n-1)! = n!$ Por otra parte, $\Gamma(\frac{1}{2}) = \int_0^\infty \frac{e^{-x}}{\sqrt{x}}dx$, haciendo el cambio de variable $u = \sqrt{x}$, se tiene que:

$$\Gamma\Big(\frac{1}{2}\Big) = 2\int_0^\infty e^{-u^2}du = \int_{-\infty}^\infty e^{-u^2}du = \sqrt{\pi}.$$

Pues se obtiene una integral Gaussiana. □

Teorema 2.8. *Γ no se anula nunca y, por tanto, $\frac{1}{\Gamma}$ es entera.*

Demostración. Para demostrarlo vamos a introducir una relación que cumple la función Γ, esta es:

$$\Gamma(s)\int_0^\infty x^{w-1}(1+x)^{-s}dx = \Gamma(s-w)\Gamma(w),$$

donde $\Re(s) > 0, \Re(w-s) < 0$ para que esté bien definida. Esto se da pues:

$$\Gamma(s)\int_0^\infty x^{w-1}(1+x)^{-s}dx = \int_0^\infty\int_0^\infty x^{w-1}(1+x)^{-s}y^{s-1}e^{-y}dxdy.$$

Haciendo el cambio de variable $x = \frac{u}{v}, y = u+v$, cuyo jacobiano tiene determinante $\frac{u+v}{v^2}$ obtenemos:

$$\int_0^\infty\int_0^\infty u^{w-1}v^{1-w}(u+v)^{-s}v^s(u+v)^{s-1}e^{-u-v}\frac{u+v}{v^2}dudv =$$

$$= \int_0^\infty\int_0^\infty u^{w-1}e^{-u}v^{s-w-1}e^{-v} = \Gamma(s-w)\Gamma(w).$$

Supongamos ahora que existe un s tal que $\Re(s) > 0$ y $\Gamma(s) = 0$. Tomando $w = \frac{1}{n}$ para n suficientemente grande, se tiene que $\Re(w) > 0, \Re(w-s) < 0$, luego podemos aplicar la fórmula anterior y se tiene que $\Gamma(s-\frac{1}{n})\Gamma(\frac{1}{n}) = 0$. Por consiguiente, hay una cantidad infinita de n para los cuales $\Gamma(s-\frac{1}{n}) = 0$ o eso sucede para $\Gamma(\frac{1}{n})$. En el primer caso, dado $\varepsilon > 0$, Γ es holomorfa en $D(s,\varepsilon)$, luego $\Gamma(z) = 0, \forall z \in D(s,\varepsilon)$ y, por tanto, idénticamente nula en $\{\Re(s) > 0\}$. En el segundo caso, como Γ tiene un polo en $s = 0$, $\lim_{s\to 0^+}|\Gamma(s)| = \infty$ luego no puede darse este caso.

En conclusión, Γ no se anula nunca y, por tanto, $\frac{1}{\Gamma}$ es una función entera cuyos ceros están en $\mathbb{Z}_{\leq 0}$ pues los polos de Γ están en $\mathbb{Z}_{\leq 0}$. □

Vamos a probar ahora dos proposiciones que nos serán de mucha utilidad para probar de forma elegante la ecuación funcional de $\zeta(s)$.

Proposición 2.9.

$$\sum_{n\in\mathbb{Z}} e^{-\pi n^2 t} = \frac{1}{\sqrt{t}} \sum_{n\in\mathbb{Z}} e^{-\pi n^2/t} \text{ para } t \in \mathbb{R}^+. \tag{2.6}$$

Demostración. Sea $t \in \mathbb{R}^+$, consideremos $F(x) = \sum_{m\in\mathbb{Z}} e^{-\pi(m+x)^2 t}$. Esta función es 1-periódica y regular para todo t, luego coincide con su desarrollo de Fourier:

$$F(x) = \sum_{n\in\mathbb{Z}} a_n e^{2\pi i n x} \quad \text{con } a_n = \int_{-1/2}^{1/2} F(x) e^{-2\pi i n x} dx.$$

Veamos que los coeficientes a_n son de la forma $a_n = \int_{-\infty}^{\infty} e^{-\pi t x^2 - 2\pi i n x} dx$, pero antes veamos que $\sum_{m\in\mathbb{Z}} e^{-\pi(m+x)^2 t}$ converge uniformemente en x en el intervalo $[-1/2, 1/2]$. Dado $\varepsilon > 0$, sean N, M arbitrarios, se verifica que:

$$0 < F(x) - \sum_{m=M}^{N} e^{-\pi(m+x)^2 t} = \sum_{m=-\infty}^{M-1} e^{-\pi(m+x)^2 t} + \sum_{m=N+1}^{\infty} e^{-\pi(m+x)^2 t}.$$

Como $e^{-\pi(m+x)^2 t} = e^{-\pi m^2 t} e^{-\pi(x^2 - 2xm)t} \leq e^{-\pi m^2 t} e^{2\pi x m t} \leq e^{-\pi(m^2 - m)t}$, sustituyendo x por $1/2$ en la última estimación. Luego se tiene que:

$$\sum_{m=-\infty}^{M-1} e^{-\pi(m+x)^2 t} + \sum_{m=N+1}^{\infty} e^{-\pi(m+x)^2 t} \leq \sum_{m=-\infty}^{M-1} e^{-\pi(m^2 - m)t} + \sum_{m=N+1}^{\infty} e^{-\pi(m^2 - m)t}.$$

Además, $m^2 - m > 0$ para m^2 suficientemente grande y $e^{-\pi t} < 1, \forall t \in \mathbb{R}^+$. Por tanto, haciendo tender $N, M \to \infty$ se tiene que todo es menor que ε. Sea ahora $f(x) = e^{-\pi t x^2}$, como $F(x)$ converge uniformemente en el rango de integración, se pueden intercambiar integral y sumatorio, luego se tiene que:

$$a_n = \int_{-1/2}^{1/2} F(x) e^{-2\pi i n x} dx = \sum_{m\in\mathbb{Z}} \int_{-1/2}^{1/2} f(x+m) e^{-2\pi i n x} dx, \text{ cambiando ahora } x = y - m,$$

$$\sum_{m\in\mathbb{Z}} \int_{m-1/2}^{m+1/2} f(y) e^{-2\pi i n y} dy = \int_{-\infty}^{\infty} f(y) e^{-2\pi i n y} dy = \frac{1}{\sqrt{t}} \int_{-\infty}^{\infty} e^{-\pi u^2 - 2\pi i \frac{n}{\sqrt{t}} u} du = \frac{1}{\sqrt{t}} e^{-\pi \frac{n^2}{t}}.$$

Donde se ha hecho el cambio de variable $x = \frac{u}{\sqrt{t}}$ en la penúltima igualdad y en la última se ha aplicado la fórmula para una integral de una función Gaussiana. Nótese ahora que el sumatorio que tenemos en la parte izquierda de (2.6) es $F(0)$, pero $F(0) = \sum_{n\in\mathbb{Z}} a_n = \frac{1}{\sqrt{t}} \sum_{n\in\mathbb{Z}} e^{-\pi n^2/t}$. □

Proposición 2.10. *Consideremos la función $w : \mathbb{R}^+ \to \mathbb{R}$ de decaimiento rápido, definida por $w(x) = \sum_{n=1}^{\infty} e^{-\pi n^2 x}$. Satisface que:*

$$w(x^{-1}) = \frac{\sqrt{x} - 1}{2} + \sqrt{x} w(x), \text{ para cualquier } x > 0.$$

Demostración. Por la proposición anterior, considerando $t = x$ y que $f(n) = e^{-\pi n^2 x}$ es par, se tiene que:

$$2w(x) + 1 = \frac{1}{\sqrt{x}}(2w(x^{-1}) + 1),$$
$$w(x^{-1}) = \frac{\sqrt{x} - 1}{2} + \sqrt{x}w(x).$$

□

Teorema 2.11. *Sea $\xi(s) = s(1-s)\pi^{-s/2}\Gamma(s/2)\zeta(s)$. Para $\Re(s) > 1$ se tiene que:*

$$\xi(s) = 1 + s(1-s)\int_1^\infty (x^{\frac{s}{2}-1} + x^{\frac{1-s}{2}-1})w(x)dx. \tag{2.7}$$

Demostración. Consideramos $\Gamma(s/2)$ y hacemos el cambio de variable $t = \pi n^2 x$:

$$\Gamma(s/2) = \int_0^\infty t^{\frac{s}{2}-1}e^{-t}dt = \pi^{s/2}n^s \int_0^\infty x^{\frac{s}{2}-1}e^{-\pi n^2 x}dx, \text{ por tanto, se tiene que:}$$

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \int_0^\infty x^{\frac{s}{2}-1}w(x)dx.$$

A continuación multiplicamos a ambos lados por $s(1-s)$ y hacemos el cambio de variable $x \to 1/x$ en el intervalo $(0, 1]$ del rango de integración en la integral anterior y usamos la proposición 2.10:

$$s(1-s)\Big(\int_1^\infty x^{-\frac{s}{2}-1}w(x^{-1})dx + \int_1^\infty x^{\frac{s}{2}-1}w(x)dx\Big),$$
$$s(1-s)\int_1^\infty x^{-\frac{s}{2}-1}\frac{\sqrt{x}-1}{2}dx + s(1-s)\int_1^\infty (x^{\frac{s}{2}-1} + x^{\frac{1-s}{2}-1})w(x)dx,$$
$$s(1-s)\frac{1}{s(1-s)} + s(1-s)\int_1^\infty (x^{\frac{s}{2}-1} + x^{\frac{1-s}{2}-1})w(x)dx.$$

□

Teorema 2.12. *Se tiene que:*

1. *$\xi(s)$ se extiende a una función entera.*
2. *Se cumple que $\xi(s) = \xi(1-s)$ para todo $s \in \mathbb{C}$.*
3. *$\zeta(s) - 1/(s-1)$ se extiende a una función entera.*

Demostración. 1. La integral del lado derecho de (2.7) converge absolutamente para todo s y converge uniformemente respecto a s en cualquier región acotada de $\mathbb{C}$, pues $w(x)$ verifica que existe un M tal que:

$$\int_1^\infty |x^{\frac{s}{2}-1}|w(x)dx, \int_1^\infty |x^{\frac{1-s}{2}-1}|w(x)dx \leq M.$$

Al cumplir que $\lim_{x\to\infty} |x^{\frac{s}{2}-1}|w(x) = \lim_{x\to\infty} |x^{\frac{1-s}{2}-1}|w(x) = 0, \forall s$ (por ser de decaimiento rápido). Luego $f(s) := \int_1^\infty (x^{\frac{s}{2}-1} + x^{\frac{1-s}{2}-1})w(x)dx$ es entera y, por consiguiente, $\xi(s)$ también lo es.

2. Se verifica la igualdad pues $s(s-1)$ no cambia al cambiar s por $s-1$ y lo mismo ocurre para $x^{\frac{s}{2}-1}+x^{\frac{1-s}{2}-1}$ en (2.7).

3. ζ se extiende de manera holomorfa y única a todo $\mathbb{C}-\{1\}$. En efecto, la igualdad (2.7) da lugar a $\pi^{-s/2}\Gamma(s/2)\zeta(s)=\frac{1}{s(s-1)}+\int_1^\infty(x^{\frac{s}{2}-1}+x^{\frac{1-s}{2}-1})w(x)dx$, en $\Re(s)>1$. Como ya hemos visto, la integral del lado derecho define una función entera, luego despejando $\zeta(s)$ se obtiene una expresión válida en $\Re(s)>1$ y cuyo lado derecho es una función holomorfa en $\mathbb{C}-\{1\}$, pues $s\Gamma(s/2)$ no tiene ceros. Por tanto, define la extensión de $\zeta(s)$ a $\mathbb{C}-\{1\}$. Así, como $\zeta(s)$ tiene un polo en $s=1$ de residuo 1 se obtiene lo que queremos.

□

Corolario 2.13. *Se verifica lo que se conoce como la ecuación funcional de $\zeta(s)$:*

$$\pi^{-s/2}\Gamma(s/2)\zeta(s)=\pi^{-(1-s)/2}\Gamma\Big(\frac{1-s}{2}\Big)\zeta(1-s),\quad \forall s\in\mathbb{C}.$$

Demostración. Se deduce del hecho de que $\xi(s)=\xi(1-s)$. □

Vamos a usar ahora la ecuación funcional para calcular algunos valores de $\zeta(s)$. Por ejemplo, para $s=-2k, k\in\{1,2,3...\}$, como $\Gamma(s/2)$ tiene polos simples en dichos valores de s, $\zeta(s)=0$, pues $\xi(s)$ es entera y de no ser así, tendría polos en cada $s=-2k$. Estos se llaman los ceros triviales de $\zeta(s)$ y son los únicos ceros de la función con parte real negativa. Otro ejemplo fácil de deducir es $\zeta(-1)$, pues verifica:

$$\pi^{-1}\Gamma(1)\zeta(2)=\sqrt{\pi}\Gamma(-1/2)\zeta(-1).$$

Y usando que $\zeta(2)=\frac{\pi^2}{6}, \Gamma(1)=1, \Gamma(-1/2)=-2\sqrt{\pi}$, se tiene que $\zeta(-1)=\frac{-1}{12}$. Finalmente, $\zeta(0)$ se puede obtener haciendo tender $s\to 0$ en la fórmula obtenida en (2.5). Esto se debe a que la integral $\int_1^\infty\frac{x-\lfloor x\rfloor-\frac{1}{2}}{x^{s+1}}dx$ no puede tender a infinito cuando tomamos el límite. Veámoslo: Sean $\sigma=\Re(s)$ y consideremos $x>1$:

$$\Big|\frac{x-\lfloor x\rfloor-\frac{1}{2}}{x^{s+1}}\Big|\le x^{-\sigma}+\Big|\frac{\lfloor x\rfloor+\frac{1}{2}}{x^{s+1}}\Big|\le x^{-\sigma}+\frac{2}{x^\sigma},\quad \text{pues } x^\sigma\le x^{\sigma+1}.$$

Así, se tiene que $\frac{x-\lfloor x\rfloor-\frac{1}{2}}{x^{s+1}}=O(x^{-s})$, luego $\int_1^\infty\frac{x-\lfloor x\rfloor-\frac{1}{2}}{x^{s+1}}dx=\int_1^\infty O(x^{-s})dx=O\Big(\int_1^\infty x^{-s}\Big)=O(\frac{1}{1-s})$ y, por tanto, al tomar el límite cuando $s\to 0$ está acotado. En conclusión, el valor de $\zeta(0)=-\frac{1}{2}$.

Teorema 2.14. *Sea $\mathscr{Z}=\{s\in\mathbb{C}:\zeta(s)=0\}$. Entonces $-\zeta'(s)/\zeta(s)-(s-1)^{-1}$ es holomorfa en el abierto $\mathscr{U}=\mathbb{C}-\mathscr{Z}$ y tiene polos simples en los elementos de $\mathscr{Z}$.*

Demostración. Lo haremos en genérico y luego particularizaremos para el caso de $\zeta(s)$. Sea $f(s)$ una función meromorfa en $\mathbb{C}$, entonces $f'(s)/f(s)$ es holomorfa en $\mathbb{C}$ salvo quizás en los polos o ceros de f. Lo haremos para los polos y se demuestra análogamente para los ceros. Sea s_0 un polo de $f(s)$ de orden k, entonces $\exists r>0$ tal que $f(s)$ tiene desarrollo en serie de Laurent en el disco perforado

de centro s_0 y radio r: $f(s) = (s-s_0)^{-k}g(s)$ con $g(s)$ holomorfa en $D(s_0,r)$ y $g(s_0) \neq 0$ (pues el $(-k)$-ésimo coeficiente de su desarrollo debe ser distinto de 0 pues el polo tiene orden k). Se tiene por tanto que:

$$\frac{f'(s)}{f(s)} = \frac{-k(s-s_0)^{-k-1}g(s) + (s-s_0)^{-k}g'(s)}{(s-s_0)^{-k}g(s)} = \frac{-k}{s-s_0} + \frac{g'(s)}{g(s)},$$

y como $\frac{g'(s)}{g(s)}$ es holomorfa en $D(s_0,r)$, se concluye que $\frac{f'(s)}{f(s)}$ tiene un polo simple en $s = s_0$ de residuo $-k$. Lo mismo sucede para los ceros de orden k de $f(s)$ que dan lugar a polos simples de $\frac{f'(s)}{f(s)}$ de residuo k.

Por tanto, en el caso de $-\zeta'(s)/\zeta(s)$, se deduce que tiene polos simples en $s = 1$, por tener un polo simple $\zeta(s)$, y en los $s \in \mathscr{Z}$, por ser los ceros de $\zeta(s)$. Luego al restarle el término $(s-1)^{-1}$, desaparece el polo en $s = 1$, lo que nos da una función holomorfa en $\mathscr{U}$ con polos simples en los elementos de $\mathscr{Z}$. □

Teorema 2.15. $-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$ *para* $\Re(s) > 1$ *donde* $\Lambda(n) = \begin{cases} \log p & \text{si } n = p^k \text{ con } k \in \mathbb{Z}^+, \\ 0 & \text{en otro caso.} \end{cases}$
A la función aritmética $\Lambda(n)$ *se la conoce como función de Von Mangoldt.*

Demostración. Dada una función $f(x)$, $\log(f(x))' = \frac{f'(x)}{f(x)}$. Como $\zeta(s) = \prod_p (1-p^{-s})^{-1}$, se tiene que:

$$-\frac{\zeta'(s)}{\zeta(s)} = -(\log(\zeta(s)))' = \sum_p \frac{\log p}{p^s - 1} = \sum_p \frac{\log p}{p^s}\frac{1}{1-p^{-s}} = \sum_p \sum_{k=0}^{\infty} \frac{\log p}{p^s} p^{-sk}.$$

Esas sumas se recorren sobre los $n = p^t$ para cierto $t \in \mathbb{N}$ y p primo, además $\Lambda(n) = \log p$. Luego se tiene que $\sum_p \sum_{k=0}^{\infty} \frac{\log p}{p^s} p^{-sk} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$. □

Observación 2.16. Si bien es cierto que el logaritmo complejo es una correspondencia multivaluada, siempre se puede restringir a un cierto dominio para convertirlo en una función bien definida. Además, en este caso, al restringirnos a $\Re(s) > 1$, la función ζ nunca se anula por lo que no hay problemas al evaluar el logaritmo y tampoco los hay para calcular su derivada, pues es una función holomorfa al ser el conjunto en el que trabajamos un abierto convexo de $\mathbb{C}$.

Teorema 2.17. *Sea* $F(s) = \sum_p \frac{\log p}{p^s}$. *Entonces se cumple que* $\frac{\zeta'(s)}{\zeta(s)} + F(s)$ *admite una extensión holomorfa en* $\Re(s) > \frac{1}{2}$.

Demostración.

$$\Big|\frac{\zeta'(s)}{\zeta(s)} + F(s)\Big| = \Big|\sum_p \Big(\frac{-\log p}{p^s - 1} + \frac{\log p}{p^s}\Big)\Big| \leq \sum_p \frac{\log p}{p^{\Re(s)}(p^{\Re(s)} - 1)} \leq \sum_{n=2}^{\infty} \frac{\log n}{n^{\Re(s)}(n^{\Re(s)} - 1)}.$$

Esa serie del final tiene el mismo tipo de convergencia que $\sum_{n=1}^{\infty} n^{-2\Re(s)}$, pues $n^{2\Re(s)}$ domina a $\log n$ y a $n^{\Re(s)}$ para n suficientemente grande. Por tanto, dicha serie converge si y sólo si $\Re(s) > \frac{1}{2}$. Concluimos así que $\frac{\zeta'(s)}{\zeta(s)} + F(s)$ admite una extensión holomorfa en $\Re(s) > \frac{1}{2}$. □

Capítulo 3

La distribución de los números primos

En este capítulo vamos a demostrar el teorema de los números primos, siguiendo a [11], un resultado que describe el comportamiento asintótico de la distribución de los números primos. Fue probado en 1896, de manera independiente, por Jacques Hadamard y Charles Jean de la Vallée Poussin y dice que $\pi(x) \sim \frac{x}{\log x}$, lo cual significa que:

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1. \tag{3.1}$$

donde $\pi(x)$ describe el número de primos menores o iguales a x. Intuitivamente, este resultado dice que dado un número natural N suficientemente grande, la probabilidad de que un entero cualquiera menor o igual que N sea primo es de aproximadamente $1/\log(N)$, lo cual refleja el hecho de que a medida que los números se hacen más grandes, los primos se hacen 'menos comunes'. Una formulación equivalente es la siguiente $\lim_{x\to\infty} \frac{\theta(x)}{x} = 1$, donde $\theta(x) = \sum_{p\leq x} \log p$.
Esta convergencia es mucho más rápida, lo cual hace pensar que una mejor aproximación para $\pi(x)$ es el logaritmo integral: $\mathrm{Li}(x) = \int_2^\infty \frac{dt}{\log t}$, como ya observó experimentalmente Gauss.
Por ejemplo, para $x = 10^6$ el porcentaje de error de $x/\log x$ es del 8.11 %, mientras que el de $Li(x)$ es del 0.164 %. Si aumentamos hasta 10^{29}, el error de $x/\log x$ es del 1.53 %, todavía notable frente al despreciable $2.99 \cdot 10^{-13}$ % de $Li(x)$.
Comenzaremos probando un resultado analítico fundamental para probar el teorema de los números primos, y es el hecho de que ζ no tiene ceros en $\Re(s) = 1$.

Teorema 3.1. *ζ no tiene ceros en $\Re(s) = 1$.*

Demostración. Veamos que para $\sigma > 1$ y $t_0 \in \mathbb{R} - \{0\}$ se tiene que:

$$(1-\sigma)\sum_{k=-2}^{2} \binom{4}{2+k} \frac{\zeta'(\sigma + ikt_0)}{\zeta(\sigma + ikt_0)} = (\sigma-1)\sum_n \frac{\Lambda(n)}{n^\sigma}(n^{it_0/2} - n^{-it_0/2})^4 \geq 0.$$

Por el teorema 2.15 se tiene que $\frac{\zeta'(\sigma+ikt_0)}{\zeta(\sigma+ikt_0)} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^{\sigma+ikt_0}}$, luego:

$$(1-\sigma)\sum_{k=-2}^{2}\binom{4}{2+k}\frac{\zeta'(\sigma+ikt_0)}{\zeta(\sigma+ikt_0)} = (\sigma-1)\sum_{n}\frac{\Lambda(n)}{n^{\sigma}}\Big(\sum_{k=-2}^{2}\binom{4}{2+k}n^{-ikt_0}\Big).$$

Y como $\sum_{k=-2}^{2}\binom{4}{2+k}n^{-ikt_0} = (n^{it_0/2} - n^{-it_0/2})^4$ se obtiene el resultado.

Supongamos ahora que existe un $t_0 \in \mathbb{R} - \{0\}$ tal que ζ tiene un cero de orden m en $s_0 = 1 + it_0$. Por lo probado en el teorema 2.14, $-\zeta'/\zeta$ tiene un polo simple en s_0 de residuo $-m$. Por tanto, se verifica que $\lim_{s\to s_0}(s-s_0)\frac{-\zeta'(s)}{\zeta(s)} = -m$. Además, como ζ es holomorfa en cualquier disco que no contenga a $s = 1$, por el teorema de Taylor, se puede escribir como serie de potencias en un disco centrado en $\overline{s_0}$ y sigue anulándose en $\overline{s_0}$ por anularse en s_0, luego también este es un cero de orden m de ζ y tiene residuo m, así que se tienen las mismas propiedades del límite que para s_0. Finalmente, como $-\zeta'/\zeta$ tiene un polo simple en $s = 1$ de residuo 1, $\lim_{s\to 1}(s-1)\frac{-\zeta'(s)}{\zeta(s)} = 1$. Juntando todo esto y que $-\zeta'/\zeta$ es holomorfa en cualquier otro punto de la recta $\Re(s) = 1$, se tiene que tomando límites cuando $\sigma \to 1^+$ en la parte de la izquierda de la desigualdad se cumple que: $\binom{4}{2} - m\binom{4}{3} - m\binom{4}{1} \geq 0$, lo cual es imposible para $m \geq 1$. □

Teorema 3.2. *La función $F(s)$ del teorema 2.17 cumple que:*

$$F(s) = s\int_1^{\infty}\frac{\theta(x)}{x^{s+1}}dx \quad \textit{para } \Re(s) > 1,$$

donde $\theta(x)$ es la función definida en la introducción de este capítulo.

Demostración. Vamos a aplicar la identidad de Abel, [2], Th.4.2. Sean $b(n) = \begin{cases} 1 & \text{si } n \text{ es primo,} \\ 0 & \text{en otro caso.} \end{cases}$, $f(x) = 1/x^s$ y $f'(x) = -s/x^{s+1}$. Denotamos por $a(n) = b(n)\log(n)$ y sea $A(x) = \sum_{n\leq x} a(n)$ (nótese que, en este caso $A(x) = \theta(x)$). Tomando el intervalo $[1, x]$ con $x \in \mathbb{R}$, f' es continua en dicho intervalo y, por la identidad de Abel se verifica que:

$$\sum_{n\leq x} a(n)f(n) = \frac{\theta(x)}{x^s} + s\int_1^x \frac{\theta(t)}{t^{s+1}}dt.$$

Teniendo en cuenta que $a(1) = 0$. Ahora tomando límites cuando $x \to \infty$ y considerando que $\Re(s) > 1$, se tiene el resultado. Comprobemos que dicha integral converge para $\Re(s) > 1$:

$$\Big|\int_1^{\infty}\frac{\theta(x)}{x^{s+1}}dx\Big| \leq \int_1^{\infty}\frac{\theta(x)}{x^{\Re(s)+1}}dx \leq \int_1^{\infty}\frac{x\log x}{x^{\Re(s)+1}}dx < \infty.$$

□

Teorema 3.3. *Existe un abierto $\mathscr{U}$ que contiene a $\{\Re(s) \geq 1\}$ tal que $G(s) = \int_1^{\infty}(\theta(x) - x)\frac{dx}{x^{s+1}}$ admite una extensión holomorfa a $\mathscr{U}$.*

Demostración. Si $\Re(s) > 1$, por el teorema previo y el hecho de que $\int_1^\infty x^{-s}dx = \frac{1}{s-1}$, se tiene que:

$$G(s) = \frac{1}{s}\Big(F(s) - \frac{1}{1-s}\Big) = \frac{1}{s}\Big(F(s) + \frac{\zeta'(s)}{\zeta(s)} - \frac{\zeta'(s)}{\zeta(s)} - \frac{1}{1-s}\Big).$$

Por el teorema 3.1 sabemos que ζ no tiene ceros en $\{\Re(s) \geq 1\}$, luego por los teoremas 2.15 y 2.17 sabemos que $G(s)$ admite una extensión holomorfa a un abierto $\mathscr{U}$ que contiene a $\{\Re(s) \geq 1\}$ pero que no puede contener a ningún s tal que $\Re(s) < \frac{1}{2}$. □

A continuación vamos a ver que la siguiente afirmación implica el teorema de los números primos:

$$\mathcal{I}(a,b) = \int_a^b (\theta(x) - x)\frac{dx}{x^2} \to 0, \quad \text{cuando } b > a \to \infty. \tag{3.2}$$

Esto es equivalente a decir que la integral impropia $\mathcal{I}(1,\infty)$ converge. Luego vamos a probar la implicación contradiciendo el teorema de los números primos y llegando a que dicha integral impropia diverge.

Si el teorema de los números primos fuese falso entonces $\limsup > 1$ o $\liminf < 1$, lo haré primero para el caso del límite superior y luego comentaré el caso del límite inferior.

Si el límite superior fuese estrictamente mayor que 1, por definición, existe una constante $L > 1$ y una sucesión positiva $x_n \to \infty$ tal que $\pi(x_n)\log(x_n) > Lx_n$. Veremos que esto lleva a contradicción en los dos siguientes resultados.

Proposición 3.4. *Sea $\beta = \frac{L+1}{L}$. Entonces, para $x \geq x_n$ se verifican las siguientes desigualdades:*

$$\theta(x) \geq \beta(\pi(x_n) - \pi(x_n^\beta)\log(x_n)) \geq \frac{L+1}{2}x_n - \beta x_n^\beta \log(x_n).$$

Demostración. Como $f(x) = \frac{x+1}{2x}$ es estrictamente decreciente para todo x, en particular se tiene que $\beta < f(1) = 1$. Luego $x_n^\beta < x_n$.

$$\theta(x) \geq \theta(x_n) \geq \sum_{x_n^\beta < p \leq x_n} \log p \geq (\pi(x_n) - \pi(x_n^\beta))\log(x_n^\beta).$$

Por otro lado se tiene:

$$\beta(\pi(x_n) - \pi(x_n^\beta))\log(x_n) = \frac{\pi(x_n)\log(x_n)}{2} + \frac{\pi(x_n)\log(x_n)}{2L} - \beta\pi(x_n^\beta)\log(x_n) \geq \frac{L+1}{2}x_n - \beta x_n^\beta\log(x_n).$$

Donde hemos usado que $\pi(x_n^\beta) \leq x_n^\beta$ y que $\pi(x_n)\log(x_n) > Lx_n$. □

Teorema 3.5. $\mathcal{I}(x_n, Lx_n) \geq \frac{L^2-1}{2L} - \log L + c_n$, *donde* $c_n \to 0$ *y* $\frac{L^2-1}{2L} - \log L > 0$.

Demostración. Por la proposición 3.4, se tiene que:

$$\mathcal{I}(x_n, Lx_n) \geq \int_{x_n}^{Lx_n} \Big(\frac{L+1}{2}x_n - \beta x_n^\beta\log(x_n) - x\Big)\frac{dx}{x^2} = \Big(\frac{L+1}{2}x_n - \beta x_n^\beta\log(x_n)\Big)\Big(\frac{-1}{Lx_n} + \frac{1}{x_n}\Big) - \log L,$$

$$\mathcal{I}(x_n, Lx_n) \geq \frac{L^2-1}{2L} - \log L + c_n, \quad \text{donde } c_n = \frac{x_n^\beta\log(x_n^\beta)}{Lx_n}(1-L) \to 0 \text{ cuando } n \to \infty,$$

pues $x_n > x_n^\beta$. Para la última parte, sea $f(x) = \frac{x^2-1}{2x} - \log x$, se puede comprobar que $f(x)$ es estrictamente creciente en $[1,\infty)$ y, por lo tanto, $f(L) > f(1) = 0$. □

Observación 3.6. Para el caso del límite inferior se sigue un razonamiento análogo. Si existe una constante $l < 1$ y una sucesión positiva $x_n \to \infty$ tal que $\pi(x_n)\log(x_n) < lx_n$, entonces se verifica que $\theta(x) \leq \pi(x_n)\log(x_n)$ para $x \leq x_n$ y se obtiene que $\mathcal{I}(lx_n, x_n) \leq 1 - l - \log l$, que es una constante estrictamente negativa pues $f(x) = 1 - x + \log x$ es estrictamente creciente en $(0, 1]$.

La idea para demostrar el teorema de los números primos es demostrar que el teorema 3.3 implica (3.2) y, como acabamos de comprobar, de esta afirmación se deriva (3.1).
A continuación, probaremos una acotación para la función θ que nos será de utilidad para probar lo que queremos.

Proposición 3.7. *Veamos que para $x > 1$ y escogiendo k tal que $x \in (2^{k-1}, 2^k]$, se tiene que $\theta(x)/x \leq 4\log 2$.*

Demostración. $\theta(x) \leq \theta(2^k) = \sum_{j=1}^{k}(\theta(2^j) - \theta(2^{j-1}))$. Además,

$$\theta(2^j) - \theta(2^{j-1}) = \sum_{2^{j-1}<p\leq 2^j} \log p = \log\Big(\prod_{2^{j-1}<p\leq 2^j} p\Big).$$

A su vez, $\binom{2^j}{2^{j-1}} = \frac{\prod_{2^{j-1}<n\leq 2^j} n}{(2^{j-1})!} = k\prod_{2^{j-1}<p\leq 2^j} p$ con $k \geq 1$ y entero. Por tanto, $\theta(2^j) - \theta(2^{j-1}) \leq \log\binom{2^j}{2^{j-1}}$. Por último, por el binomio de Newton se tiene que $(1+1)^{2^j} \geq \binom{2^j}{2^{j-1}}$ y tomando logaritmos se tiene que $\log\binom{2^j}{2^{j-1}} \leq 2^j\log(2)$. Concatenando todas las estimaciones se llega a que $\theta(x) \leq \sum_{j=1}^{k} 2^j\log(2) = 2(2^k - 1)\log(2) \leq 4x\log 2$, pues $2^k \leq 2x$. □

Definimos ahora unas funciones que nos servirán para probar que el teorema 3.3 implica que se tiene (3.2). Sea $c > 1$, definimos $G_c(s) = \int_1^c(\theta(x)-x)\frac{dx}{x^{s+1}}$, $h_c(s) = c^s(1+\frac{s^2}{R^2})$, $B_c(s) = G_c(s+1)h_c(s)$ y $A_c(s) = B_c(s) - G(s+1)h_c(s)$. Sea la región $D = \{s \in \mathbb{C} : |s| \leq R, \Re(s) > -\delta\}$ con $R > 1 > \delta > 0$. Es sencillo comprobar que para cualquier R, existe un $\delta > 0$ tal que $\{s + 1 : s \in D\} \subset \mathscr{U}$, donde $\mathscr{U}$ es el abierto donde $G(s)$ es holomorfa. Por tanto, las funciones antes definidas y G son holomorfas en un abierto que contiene a D. De hecho, G_c, h_c y B_c son enteras.

Teorema 3.8.

$$\mathcal{I}(a, b) = \frac{1}{2\pi i}\int_{\partial D}(A_b(s) - A_a(s))\frac{ds}{s}.$$

Demostración. La función $f(s) = A_b(s) - A_a(s)$ es holomorfa en un abierto que contiene a D y, por tanto, contiene al camino que forma su frontera ∂D. Luego, como $s = 0$ está en el interior de D, por la fórmula integral de Cauchy se tiene que:

$$\frac{1}{2\pi i}\int_{\partial D}(A_b(s) - A_a(s))\frac{ds}{s} = f(0) = h_a(0)(G(1) - G_a(1)) - h_b(0)(G(1) - G_b(1)) =$$

$$= \int_a^\infty(\theta(x) - x)\frac{dx}{x^2} - \int_b^\infty(\theta(x) - x)\frac{dx}{x^2} = \mathcal{I}(a, b).$$

□

Consideremos ahora $\partial D = C_1 \sqcup C_2$, donde C_1 es la semicircunferencia derecha, $C_1 = \{|s| = R, \Re(s) \geq 0\}$, y C_2 el resto. Veamos que se tiene (3.2) si dado $\varepsilon > 0$, existe un $R > 1$ tal que $J_1 := \left| \int_{C_1} (A_b(s) - A_a(s)) \frac{ds}{s} \right| < \varepsilon/2$ y $J_2 := \left| \int_{C_2} (B_b(s) - B_a(s)) \frac{ds}{s} \right| < \varepsilon/2$. Se verifica que:

$$|\mathcal{I}(a,b)| \leq \left| \int_{\partial D} (A_b(s) - A_a(s)) \frac{ds}{s} \right| \leq J_1 + \left| \int_{C_2} (A_b(s) - A_a(s)) \frac{ds}{s} \right| \leq$$

$$\leq J_1 + J_2 + \left| \int_{C_2} G(s+1)(h_a(s) - h_b(s)) \frac{ds}{s} \right|.$$

Ahora bien, cuando $b > a \to \infty$, entonces $h_a(s), h_b(s) \to 0, \forall s \in C_2$, luego la última integral tiende a 0. Por tanto, si se da lo dicho anteriormente, se tendría (3.2). Veamos que, efectivamente, se da eso en el siguiente teorema.

Teorema 3.9. *Para $s \in C_1$, con $\Re(s) = \sigma$, se tiene que $|h_c(s)| = 2R^{-1}\sigma c^\sigma$ y $|G_c(s+1) - G(s+1)| \leq K\sigma^{-1}c^{-\sigma}$ para cierta constante K.*

Demostración. Sea $s = \sigma + iy$. Se verifica que: $|h_c(s)| = c^\sigma \frac{|R^2+s^2|}{R^2}$. Teniendo en cuenta que $s \in C_1$, se cumple que $R^2 = \sigma^2 + y^2$. Así, $|R^2 + s^2| = 2R\sigma$ y se tiene el resultado.
Para la segunda parte, vamos a usar la proposición 3.7 para estimar $|G_c(s+1) - G(s+1)|$. Sea $M = 4\log 2$:

$$|G_c(s+1) - G(s+1)| = \left| \int_c^\infty (\theta(x) - x) \frac{dx}{x^{s+2}} \right| \leq \int_c^\infty (M-1) \frac{dx}{x^{\sigma+1}} = K\sigma^{-1}c^{-\sigma}.$$

Donde $K = M - 1$. □

Sea ahora C_3 la semicircunferencia izquierda simétrica a C_1, es decir, $C_3 = \{|s| = R, \Re(s) < 0\}$, consideramos el camino cerrado γ que se obtiene al recorrer C_2 en sentido positivo y luego C_3 en sentido negativo. Como $g(s) = \frac{B_b(s) - B_a(s)}{s}$ es holomorfa en el interior de γ, se tiene que $\int_\gamma g(s)ds = 0$, lo que implica que $J_2 = \left| \int_{C_3} (B_b(s) - B_a(s)) \frac{ds}{s} \right|$.

Teorema 3.10. *Dado $\varepsilon > 0$, existe un $R > 1$ tal que $J_1 < \varepsilon/2$ y $J_2 < \varepsilon/2$.*

Demostración. Aplicando el teorema 3.9 y teniendo en cuenta que $|s| = R$, se tiene que:

$$J_1 = \left| \int_{C_1} ((G_b(s+1) - G(s+1))h_b(s) - (G_a(s+1) - G(s+1))h_a(s)) \frac{ds}{s} \right| \leq$$

$$\leq \int_{C_1} (K\sigma^{-1}b^{-\sigma}) \frac{2R^{-1}\sigma b^\sigma}{R} ds + \int_{C_1} (K\sigma^{-1}a^{-\sigma}) \frac{2R^{-1}\sigma a^\sigma}{R} ds = \int_{C_1} \frac{4K}{R^2} ds \to 0$$

cuando $R \to \infty$. Luego dado $\varepsilon > 0$, existe un $R > 1$ tal que $J_1 \leq \varepsilon/2$. Ahora para J_2 se tiene que:

$$J_2 = \left| \int_{C_3} (G_b(s+1)h_b(s) - G_a(s+1)h_a(s)) \frac{ds}{s} \right| \leq \int_{C_3} (|G_b(s+1)||h_b(s)| + |G_a(s+1)||h_a(s)|) \frac{ds}{R}.$$

Para $s \in C_3$, se tiene que $|h_c(s)| = 2R^{-1}|\sigma|c^\sigma$ y $|G_c(s+1)| \leq \int_1^c Kx^{-\sigma-1}dx = K|\sigma|^{-1}(c^{-\sigma} - 1)$. Entonces se verifica que $J_2 \leq \frac{2K}{R}(2 - b^\sigma - a^\sigma) \to 0$ cuando $R \to \infty$, pues $b^\sigma, a^\sigma \to 0$ cuando $b > a \to \infty$ por ser $\sigma < 0$. □

Capítulo 4

Las funciones L y el teorema de Dirichlet

El objetivo de este capítulo será probar el siguiente teorema:

Teorema 4.1. ***Teorema de Dirichlet:*** *Para $q \in \mathbb{Z}_{>1}$ y $a \in \mathbb{Z}$ con $mcd(q,a) = 1$, la sucesión $\{qn+a\}_{n=0}^{\infty}$ contiene infinitos números primos.*

Comenzaremos el capítulo introduciendo la noción de carácter de Dirichlet.

Definición 4.2. Sea G un grupo abeliano finito. Se denota por $\hat{G}$ al conjunto de los caracteres de G y se le llama grupo dual de G. Estos son los homomorfismos $\chi : G \to \{z \in \mathbb{C} : |z| = 1\}$. Se verifica que $|G| = |\hat{G}|$.

Observación 4.3. Dado G un grupo abeliano finito, se cumple que:

$$\sum_{x \in G} \chi(x) = \begin{cases} |G| & \text{si } \chi = \chi_0, \\ 0 & \text{si } \chi \neq \chi_0. \end{cases} \quad \text{y} \quad \sum_{\chi \in \hat{G}} \chi(g) = \begin{cases} |\hat{G}| & \text{si } g = e, \\ 0 & \text{si } g \neq e. \end{cases}$$

Definición 4.4. Consideremos el grupo $(\mathbb{Z}/q\mathbb{Z})^*$ de los elementos de $q\mathbb{Z}$ con inverso multiplicativo, es decir, los que no tienen factores comunes con q. Se llaman caracteres de Dirichlet módulo q a las extensiones a $\mathbb{Z}$ de los caracteres de este grupo asignando a n el valor $\chi(n \pmod q)$ si n y q son coprimos y cero en otro caso. Se denota por $\chi_0 : \mathbb{Z} \to \mathbb{C}$ a $\chi_0(n) = 1$ si $\text{mcd}(n,q) = 1$, $\chi_0(n) = 0$ en otro caso.

Observación 4.5. Nótese que los caracteres son funciones multiplicativas y q-periódicas.

Teorema 4.6. ***Relaciones de ortogonalidad:*** *Análogamente a la observación 4.3, se verifica:*

$$\sum_{a=1}^{q} \chi(a) = \begin{cases} \varphi(q) & si\ \chi = \chi_0, \\ 0 & si\ \chi \neq \chi_0. \end{cases} \quad y \quad \sum_{\chi} \chi(a) = \begin{cases} \varphi(q) & si\ a \equiv 1\ (q), \\ 0 & si\ a \not\equiv 1\ (q). \end{cases}$$

Demostración. En primer lugar, si $\chi = \chi_0$ el primer resultado es inmediato. Por otra parte, observemos que si $\chi \neq \chi_0$, entonces existe un x tal que $\chi(x) \neq 1$. Por tanto, $\chi(x) \sum_{a=1}^{q} \chi(a) = \sum_{a=1}^{q} \chi(xa) =$

$\sum_{a=1}^{q}\chi(a)$ y pasando al otro lado se tiene que $\sum_{a=1}^{q}\chi(a)=0$. Para el segundo resultado, nótese que si $a\equiv 1\ (q)$, entonces $\chi(a)=\chi(1)=1$ para todo carácter χ, luego $\sum_{\chi}\chi(a)=|\hat{G}|=\varphi(q)$. Si $a\not\equiv 1\ (q)$ y $\text{mcd}(a,q)=1$ (si $\text{mcd}(a,q)>1$ es trivial), entonces existe un carácter χ' tal que $\chi'(a)\neq 1$. Por tanto, $\chi'(a)\sum_{\chi}\chi(a)=\sum_{\chi}\chi'(a)\chi(a)=\sum_{\chi}\chi(a)$ y se tiene el resultado. □

Cuando q es impar, los caracteres de Dirichlet restringidos a $(\mathbb{Z}/q\mathbb{Z})^*$ conforman un grupo isomorfo a $C_{\varphi(p_1^{\alpha_1})}\times ...\times C_{\varphi(p_k^{\alpha_k})}$ donde $q=p_1^{\alpha_1}...p_k^{\alpha_k}$ y los caracteres se escriben de manera explícita en términos de las raíces primitivas. Si q es par, esto no es cierto y lo podemos ver con un contraejemplo. Los caracteres de Dirichlet reales son los que toman valores en $\{-1,0,1\}$ y, por tanto, verifican que $\chi^2=\chi_0$ (es por ello que a veces se les llama caracteres cuadráticos). Consideremos el grupo $(\mathbb{Z}/8\mathbb{Z})^*=\{1,3,5,7\}$. Los caracteres de Dirichlet de este grupo son: $\chi_0=1,\chi_1=\{1,1,-1,-1\},\chi_2=\{1,-1,1,-1\}$ y $\chi_3=\{1,-1,-1,1\}$ (usando dicha notación para especificar las imágenes de $1,3,5$ y 7 respectivamente. El resto se siguen por extensión). Es evidente que estos caracteres son reales, luego su orden como elementos del grupo dual, $\hat{G}$, es 2. Por tanto, $\hat{G}\cong\mathbb{Z}_2\times\mathbb{Z}_2$ en lugar de ser isomorfo a $\mathbb{Z}_{\varphi(2^3)}=\mathbb{Z}_4$.
Antes de definir las funciones L de Dirichlet, vamos a probar un par de resultados generales sobre un tipo especial de caracteres llamados primitivos. Su definición la dejaremos para el próximo capítulo donde jugarán un papel esencial.

Definición 4.7. Dado un carácter de Dirichlet χ mód q, definimos $e_q(m)=e^{2\pi im/q}$ y $\tau(\chi)=\sum_{m=1}^{q}\chi(m)e_q(m)$. Nótese que $e_q(m)$ denota una raíz q-ésima de la unidad y que $e_q(m)=e_q(n)$ si $m\equiv n\ (\text{mód } q)$ (q-periódica). Asimismo, $\tau(\chi)$ es lo que se conoce como suma de Gauss.

Proposición 4.8. *Si $mcd(n,q)=1$ y $\tau(\overline{\chi})\neq 0$, se tiene que $\chi(n)\tau(\overline{\chi})=\sum_{h=1}^{q}\overline{\chi}(h)e_q(nh)$.*

Demostración. $\chi(n)\tau(\overline{\chi})=\sum_{m=1}^{q}\overline{\chi}(m)\chi(n)e_q(m)=\sum_{m=1}^{q}\overline{\chi}(m\overline{n})e_q(m)=\sum_{h=1}^{q}\overline{\chi}(h)e_q(nh)$ con h tal que $m\equiv nh\ (\text{mód } q)$. □

Proposición 4.9. *Si χ es un carácter primitivo, entonces la igualdad de 4.8 se sostiene incluso si $mcd(n,q)>1$.*

Demostración. El lado de la derecha es 0, luego tenemos que ver que $\sum_{h=1}^{q}\overline{\chi}(h)e_q(nh)=0$. Como $\text{mcd}(n,q)>1$, se cumple que $\frac{n}{q}=\frac{n_1}{q_1}$ con $\text{mcd}(n_1,q_1)=1$ y $q_1|q, q_1<q$. Además, podemos suponer que $q_1>1$, pues en caso contrario, n sería múltiplo de q y la igualdad se cumple trivialmente por las relaciones de ortogonalidad. Por tanto, debemos probar que $\sum_{h=1}^{q}\overline{\chi}(h)\exp(2\pi in_1h/q_1)=0$. Sea $q=q_1q_2$ y pongamos $h=uq_1+v$, con $0\leq u<q_2$, $1\leq v\leq q_1$. La exponencial depende solo de v y, por tanto, basta probar que $\sum_{u=0}^{q_2-1}\overline{\chi}(uq_1+v)=0$ para cada v (se saca $\exp(2\pi in_1v/q_1)$ como factor común). Considerada como función de v, llamémosla $S(v)$, es una función q_1-periódica pues al cambiar v por $v+q_1$, u estaría entre 1 y q_2 y $u=q_2$ es equivalente a $u=0$. Supongamos ahora que c es un número que satisface $\text{mcd}(c,q)=1$ y $c\equiv 1\ (\text{mód } q_1)$. Entonces se verifica que

$\overline{\chi}(c)S(v) = \sum_{u=0}^{q_2-1} \overline{\chi}(cuq_1 + cv) = \sum_{u=0}^{q_2-1} \overline{\chi}(uq_1 + cv) = S(cv) = S(v)$, por ser S q_1-periódica. Por la definición de carácter primitivo, existen enteros c_1, c_2 tales que $(c_1, q) = (c_2, q) = 1$, $c_1 \equiv c_2$ (mód q_1) y $\chi(c_1) \neq \chi(c_2)$. Luego $c \equiv c_1 c_2^{-1}$ satisface lo anterior y $\chi(c) \neq 1$, por tanto, $\overline{\chi}(c) \neq 1$ y se deduce que $S(v) = 0$. □

Definición 4.10. Asociado a cada carácter de Dirichlet χ, se define la función L de Dirichlet:

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \quad \text{con } \Re(s) > 1.$$

Observación 4.11. Para $\chi \neq \chi_0$ esta definición es también válida para $s \in \mathbb{R}$, $s > 0$ y da lugar a una función regular gracias a que el criterio de Dirichlet asegura su convergencia y la de sus derivadas. Además, la serie converge y es holomorfa en $\Re(s) > 0$.

Teorema 4.12. *Para $\Re(s) > 1$, se tiene que:*

$$L(s, \chi) = \prod_p (1 - \chi(p)p^{-s})^{-1} \quad y \quad -\frac{L'(s, \chi)}{L(s, \chi)} = \sum_{n=1}^{\infty} \chi(n) \frac{\Lambda(n)}{n^s}.$$

En particular, $L(s, \chi_0) = \zeta(s) \prod_{p|q} (1 - p^{-s})$.

Demostración. En primer lugar, observemos que dado p primo, $|\chi(p)p^{-s}| \leq |p^{-s}| < 1$ para todo $\Re(s) > 1$. Por tanto, dado que χ es una función totalmente multiplicativa, se verifica que $(1 - \chi(p)p^{-s})^{-1} = \sum_{n=0}^{\infty} \chi(p^n)p^{-sn}$. Si consideramos un cierto $N \in \mathbb{N}$ se tiene que, en $L(s, \chi) - \prod_{p \leq N}(1 - \chi(p)p^{-s})^{-1}$, todos los términos cuyos factores primos sean menores o iguales que N desaparecen de la suma por el teorema fundamental de la aritmética y por ser χ totalmente multiplicativa. Así, sea $\varepsilon > 0$, existe un $N \in \mathbb{N}$ tal que: $|L(s, \chi) - \prod_{p \leq N}(1 - \chi(p)p^{-s})^{-1}| \leq \sum_{n \geq N} \frac{|\chi(n)|}{|n^s|} \leq \sum_{n \geq N} \frac{1}{n^{\Re(s)}} \leq \varepsilon$. Por tanto, se obtiene el primer resultado y para $\chi = \chi_0$, se tiene que $L(s, \chi_0) = \prod_{\text{mcd}(p,q)=1} (1 - p^{-s})^{-1}$. Usando el teorema 1.1, obtenemos el resultado, pues $\zeta(s) \prod_{p|q} (1 - p^{-s})$ solo deja los términos p tales que $\text{mcd}(p, q) = 1$ en el producto de Euler de ζ. De esta forma, observamos que $(s-1)L(s, \chi_0)$ admite una extensión entera.

Para la segunda igualdad, observemos que $L(s, \chi)$ es una función holomorfa en un convexo de $\mathbb{C}$ en el que dicha función nunca se anula (observando su expresión como producto de Euler es claro que no se anula en $\Re(s) > 1$), luego $\log(L(s, \chi))$ está bien definido y es una función holomorfa en dicha región. Por tanto, usando la primera fórmula se obtiene que: $-\frac{L'(s,\chi)}{L(s,\chi)} = (-\log(L(s, \chi)))' = (\sum_p \log(1 - \chi(p)p^{-s}))' = \sum_p \chi(p) \frac{\log p}{p^s} \frac{1}{1 - \chi(p)p^{-s}} = \sum_p \sum_{k=0}^{\infty} \chi(p) \frac{\log p}{p^s} p^{-sk}$. Como dichas sumas se recorren en los $n = p^t, t \in \mathbb{N}$ y p primo, y $\Lambda(n) = \log(p)$, se tiene el resultado. □

Teorema 4.13. *Sean q y a coprimos, la siguiente expresión está acotada para $s > 1$:*

$$\varphi(q) \sum_{\substack{n=1 \\ n \equiv a(q)}} \frac{\Lambda(n)}{n^s} - \frac{1}{s-1} + \sum_{\chi \neq \chi_0} \overline{\chi}(a) \frac{L'(s, \chi)}{L(s, \chi)}. \tag{4.1}$$

donde los caracteres son módulo q. Además, si suponemos que $L(1, \chi) \neq 0$ si $\chi \neq \chi_0$, entonces se deduce el teorema 4.1.

Demostración. Dado que $s > 1$, estamos en las condiciones del teorema 4.12 que nos dice que $\sum_\chi \overline{\chi}(a)\frac{L'(s,\chi)}{L(s,\chi)} = -\sum_{n=1}^\infty \frac{\Lambda(n)}{n^s}\sum_\chi \overline{\chi}(a)\chi(n)$. Denotando por $\overline{a}$ el inverso multiplicativo de a en $(\mathbb{Z}/q\mathbb{Z})^*$, se tiene que $\chi(\overline{a}) = 1/\chi(a) = \overline{\chi(a)} = \overline{\chi}(a)$. Luego, $\sum_\chi \overline{\chi}(a)\chi(n) = \sum_\chi \chi(\overline{a}n) = \varphi(q)$ si $n \equiv a(q)$, usando el teorema 4.6. De esta manera, se obtiene que (4.1) es igual a $\frac{-1}{s-1} - \frac{L'(s,\chi_0)}{L(s,\chi_0)}$. Denotando por $k(s) = \prod_{p|q}(1-p^{-s})$, es una función no singular en $s \geq 1$, nunca nula y verifica que $L(s,\chi_0) = \zeta(s)k(s)$ por el teorema 4.12. Por tanto, se tiene que $-\frac{L'(s,\chi_0)}{L(s,\chi_0)} = -\frac{k'(s)}{k(s)} - \frac{\zeta'(s)}{\zeta(s)}$. Por todo ello, se tiene que (4.1) es igual a $\frac{-1}{s-1} - \frac{k'(s)}{k(s)} - \frac{\zeta'(s)}{\zeta(s)}$ y esta última expresión está acotada para $s > 1$ pues es una función holomorfa en $s \geq 1$ dado que $\frac{-1}{s-1}$ se cancela con el término $\frac{1}{s-1}$ de la expansión en serie de Laurent de $-\frac{\zeta'(s)}{\zeta(s)}$. Para la última afirmación, observemos que el último término de (4.1) está acotado cuando $s \to 1^+$ pues $L(1,\chi) \neq 0$ para $\chi \neq \chi_0$ por hipótesis y la suma es finita. Luego para que todo esté acotado cuando tomamos $s \to 1^+$ en la expresión (4.1), debe darse que $\lim_{s\to 1^+} \sum_{\substack{n=1 \\ n\equiv a(q)}} \frac{\Lambda(n)}{n^s} = \infty$. Para concluir el teorema 4.1 solo nos falta ver que $F(s) = \sum_{m=2}^\infty \sum_{p^m \equiv a(q)} \frac{\log p}{p^{ms}} < \infty$ para $s = 1$, pues $\sum_{\substack{n=1 \\ n\equiv a(q)}} \frac{\Lambda(n)}{n^s} = \sum_{p\equiv a(q)} \frac{\log p}{p^s} + F(s)$ y $F(s) \leq F(1) < \infty$ para todo $s > 1$, si $F(1)$ converge. Se tiene que:

$$F(1) \leq \sum_p \sum_{m=2}^\infty \frac{\log p}{p^m} = \sum_p \frac{\log p}{p(p-1)} \leq \sum_{n=2}^\infty \frac{\log n}{n(n-1)}.$$

Y dicha serie converge pues $\lim_{n\to\infty} \frac{n^{\frac{3}{2}}\log n}{n(n-1)} = 0$ y $\sum_{n=1}^\infty n^{-\frac{3}{2}}$ converge. □

Teorema 4.14. *Para $s > 1$, se tiene que:*

$$L(s,\chi_0)\prod_{\chi\neq\chi_0} L(s,\chi) = \exp\Big(\varphi(q)\sum_{\substack{n=2 \\ n\equiv 1(q)}}^\infty \frac{\Lambda(n)}{n^s \log n}\Big) \geq 1.$$

Demostración. Por el teorema 4.12, tenemos que:

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

pues $\sum_{n=1}^\infty n^{-1}x^n = \log(\frac{1}{1-x})$ si $|x| < 1$. Por tanto,

$$\log(\prod_\chi L(s,\chi)) = \sum_{n=1}^\infty \sum_\chi \frac{\chi(n)\Lambda(n)}{n^s \log n} = \varphi(q)\sum_{\substack{n=2 \\ n\equiv 1(q)}}^\infty \frac{\Lambda(n)}{n^s \log n}$$

por el teorema 4.6. La última desigualdad se sigue del hecho de que lo que hay dentro de la exponencial es positivo. □

Corolario 4.15. *$L(1,\chi) \neq 0$ si χ es un carácter no real.*

Demostración. Si $L(1,\chi) = 0$ con χ no real, entonces $L(1,\overline{\chi}) = 0$ y $\prod_{\chi\neq\chi_0} L(s,\chi)$ tendría un cero doble en $s = 1$, luego el producto de la izquierda en el teorema 4.14 tendría un cero en $s = 1$ pues $L(s,\chi_0)$ tiene un polo simple en $s = 1$ al igual que la función $\zeta(s)$. Así, tomando $s \to 1^+$ se llegaría a contradicción. □

Con estos últimos resultados, lo único que nos falta para probar el teorema 4.1 es demostrar que si $\chi \neq \chi_0$ es un carácter real, entonces $L(1,\chi) \neq 0$.

Para probar esta afirmación usaremos una función aritmética y su suma, más concretamente, $c(n) = \sum_{d|n} \chi(d)$ y $f(x) = \sum_{1 \leq n \leq x} c(n)$. Es claro que c es una función multiplicativa, esto es, para $m, n \in \mathbb{Z}^+$ coprimos, se cumple que $c(mn) = c(m)c(n)$. Esto se debe al famoso lema de Euclides, pues sea $d|mn$ y $\prod_{i=1}^{k} p_i^{\alpha_i}$ la descomposición en factores primos de d, cada uno de los p_i divide a m o n, luego dado un divisor de mn tenemos dicho divisor como producto de dos divisores de m y n respectivamente. Recíprocamente, dados dos divisores $d_1|m$ y $d_2|n$, $d = d_1 d_2$ divide a mn. Así, puesto que χ es multiplicativa, se tiene que $c(mn) = \sum_{d|mn} \chi(d) = \sum_{k|m} \chi(k) \sum_{l|n} \chi(l) = c(m)c(n)$. A continuación, vamos a enunciar el llamado Lema de Landau, cuya prueba haremos en dos pasos y que nos será de gran utilidad para probar lo que queremos. En lo que resta de capítulo, salvo en el Lema de Landau, c y f denotan las funciones que acabamos de definir.

Teorema 4.16. ***Lema de Landau:*** *Sea $f : [1, \infty) \to \mathbb{R}$ localmente integrable y no negativa tal que $\lim_{x\to\infty} f(x)x^{-1-\varepsilon} = 0$ para cualquier $\varepsilon > 0$. Si la transformada integral:*

$$L_f(s) = \int_1^\infty \frac{f(x)}{x^{s+1}} dx$$

se extiende a una función holomorfa en algún abierto que contiene a un intervalo $(\sigma, 1]$ con $0 < \sigma < 1$, entonces la integral converge para $\Re(s) > \sigma$ y es holomorfa allí.

Nótese que la hipótesis sobre el límite asegura que la integral converge en $\Re(s) > 1$. Definimos $\sigma' = \text{ínf}\{\delta > \sigma : L_f(s) \text{ converge para } \Re(s) > \delta\}$. El teorema se sigue si $\sigma' > \sigma$ lleva a una contradicción. La holomorfía se puede obtener como consecuencia del teorema de Morera, pero no vamos a usarla. Las siguientes dos proposiciones demuestran el teorema:

Proposición 4.17.

$$\lim_{N\to\infty} \int_1^N x^{-1-\delta} f(x)dx = \infty \text{ para todo } 0 < \delta < \sigma'.$$

Demostración. Sean $N, M \in \mathbb{N}$. Si fuese cierto que la integral para δ converge, entonces $\lim_{N,M\to\infty} \int_N^M x^{-1-\delta} f(x)dx = 0$. Como $\delta < \sigma'$, existe algún $s \in \mathbb{C}$ tal que $\Re(s) > \delta$ y $L_f(s)$ no converge, pero entonces $L_f(\Re(s))$ no converge. En efecto, si convergiese, entonces $\lim_{N,M\to\infty} \int_N^M x^{-1-\Re(s)} f(x)dx = 0$, luego $0 \leq |\int_N^M x^{-1-s} f(x)dx| \leq \int_N^M x^{-1-\Re(s)} f(x)dx$ y $L_f(s)$ convergería. Por tanto, podemos suponer que s es real y cumple que $0 < \delta < s < \sigma'$ y $L_f(s)$ no converge. Sin embargo, en $[1, \infty)$, $x^{-1-\delta} \geq x^{-1-s}$, luego $\int_N^M x^{-1-\delta} f(x)dx \geq \int_N^M x^{-1-s} f(x)dx \geq 0$ pues $f \geq 0$. Así, para N, M suficientemente grandes se debería tener la convergencia a 0 de $\int_N^M x^{-1-s} f(x)dx$, lo que no es posible. Además, se tiene que $\int_1^N x^{-1-\delta} f(x)dx = \sum_{n=1}^{N-1} a(n)$ donde $a(n) = \int_n^{n+1} f(x)x^{-1-\delta}dx \geq 0$, pues $f \geq 0$. Por tanto, sabiendo que dicha integral no converge, su límite cuando $N \to \infty$ debe ser ∞ pues es una serie de términos positivos que no converge. □

Proposición 4.18. *Sean σ_+ y σ_- con $\sigma < \sigma_- < \sigma' < \sigma_+$ suficientemente cercanos para que σ_- pertenezca a un disco centrado en σ_+ en el que $L_f(s)$ tiene extensión holomorfa, llamémosla F. Se cumple que:*

$$F(\sigma_-) = \sum_{n=0}^{\infty} \frac{L_f^{(n)}(\sigma_+)}{n!}(\sigma_- - \sigma_+)^n = \sum_{n=0}^{\infty} \frac{(\sigma_+ - \sigma_-)^n}{n!} \int_1^{\infty} \frac{f(x)(\log x)^n}{x^{1+\sigma_+}} dx. \tag{4.2}$$

Por tanto, restringiendo la integral a $[1, N]$ se tiene que $\int_1^N f(x)x^{-1-\sigma_-}$ está uniformemente acotada por $F(\sigma_-)$.

Demostración. La primera igualdad de (4.2) se deduce del teorema de Taylor aplicado a F en el disco mencionado centrado en σ_+, pues en dicho punto, $L_f(s)$ converge y es holomorfa, luego coincide con F al igual que todas sus derivadas. La segunda igualdad se deduce por la derivación bajo el signo integral de $L_f(s)$, pues $L_f^{(n)}(\sigma_+) = (-1)^n \int_1^{\infty} \frac{f(x)(\log x)^n}{x^{1+\sigma_+}} dx$. Por otro lado, se verifica que $\int_1^N f(x)x^{-1-\sigma_-}dx = \int_1^N f(x)x^{-1-\sigma_+}x^{\sigma_+-\sigma_-}dx$ y sea $k = \sigma_+ - \sigma_-$, tenemos que $x^k = \sum_{n=0}^{\infty} \frac{k^n(\log x)^n}{n!}$. Por tanto, $\int_1^N f(x)x^{-1-\sigma_-}dx = \sum_{n=0}^{\infty} \frac{k^n}{n!} \int_1^N \frac{f(x)(\log x)^n}{x^{1+\sigma_+}} dx$. Nótese que la no negatividad de f nos permite intercambiar integral y sumatorio usando el teorema de la convergencia monótona de Lebesgue (pues las $g_n = \frac{k^n}{n!} \frac{f(x)(\log x)^n}{x^{1+\sigma_+}}$ son positivas). Además, la convergencia de $L_f(\sigma_+)$ nos asegura que $\int_1^N \frac{f(x)(\log x)^n}{x^{1+\sigma_+}} dx \leq \int_1^{\infty} \frac{f(x)(\log x)^n}{x^{1+\sigma_+}} dx$. Por tanto, $\int_1^N f(x)x^{-1-\sigma_-}dx \leq F(\sigma_-)$, lo que supone una contradicción con la proposición 4.17. □

Ahora vamos a enunciar una observación y un teorema que prueban que f verifica la condición del límite del teorema 4.17.

Lema 4.19. ***Truco de Rankin:*** *Sea $g(n)$ una función multiplicativa no negativa y $\sigma > 0$ tal que $G(\sigma) = \sum_{n=1}^{\infty} g(n)n^{-\sigma}$ converge, entonces $\sum_{n \leq x} g(n) \leq x^{\sigma}G(\sigma) = x^{\sigma} \prod_p (\sum_{n=0}^{\infty} g(p^n)p^{-n\sigma})$.*

Demostración. Dado que $g(n) \geq 0$, es claro que $\sum_{n \leq x} g(n)n^{-\sigma} \leq G(\sigma)$. Por tanto, se verifica que:

$$\sum_{n \leq x} g(n) \leq \sum_{n \leq x} g(n)\Big(\frac{x}{n}\Big)^{\sigma} \leq x^{\sigma}G(\sigma) = x^{\sigma} \prod_p (1 + g(p)p^{-\sigma} + g(p^2)p^{-2\sigma} + ...).$$

□

Teorema 4.20. *Para $\varepsilon > 0$ y $N \in \mathbb{Z}_{>1}$ se verifica:*

$$\frac{1}{N} \sum_{n=1}^{N} \sum_{d|n} 1 \leq N^{\varepsilon/2} \prod_{p \leq N} (1 - p^{-1-\varepsilon/2})^{-2}.$$

Demostración. Vamos a usar el lema 4.19. Con la misma notación que en dicha observación, tomando $\sigma = 1 + \varepsilon/2 > 0$ y $g(p^k) = d(p^k)$ si $p^k \leq x$ y $g(p^k) = 0$ si $p^k > x$ (conviniendo que $d(0) = 0$), obtenemos que $G(\sigma)$ converge y $\sum_{n \leq x} d(n) \leq x^{\sigma} \sum_{n \leq x} d(n)n^{-\sigma}$.
Por tanto, como $d(n)n^{-\sigma}$ es multiplicativa, se tiene que $\sum_{n \leq x} d(n)n^{-\sigma} \leq \prod_{p \leq x} \sum_{k=0}^{\infty} (k+1)p^{-\sigma k} = \prod_{p \leq x} (1 - p^{-\sigma})^{-2}$ pues $\sum_{n=0}^{\infty} (n+1)x^n = (1-x)^{-2}$ y $\sum_{d|p^k} 1 = k+1$. Así, tomando $x = N$ se tiene el resultado. □

Gracias al teorema 4.20 se tiene que $f(N) \leq \sum_{n=1}^{N} \sum_{d|n} 1 \leq N^{\sigma} \prod_{p \leq N} (1 - p^{-\sigma})^{-2}$ por ser χ carácter real. A su vez, $\lim_{N \to \infty} \prod_{p \leq N} (1-p^{-\sigma})^{-2} = \zeta(\sigma)^2 < \infty$. Por tanto, $N^{\sigma} \prod_{p \leq N} (1-p^{-\sigma})^{-2}$ se comporta como N^{σ} para N suficientemente grande. Así pues, $\lim_{x \to \infty} f(x) x^{-1-\varepsilon} = \lim_{x \to \infty} x^{-\varepsilon/2} = 0$ para cualquier $\varepsilon > 0$.

Teorema 4.21. *Con la notación del teorema 4.16, se tiene que $sL_f(s) = \zeta(s)L(s,\chi)$. Además, suponiendo $f \geq 0$, se tiene que $L_f(1/2)$ converge si $L(1,\chi) = 0$.*

Demostración. Para $\Re(s) > 1$ se tiene que $\zeta(s)L(s,\chi) = \sum_{m=1,k=1}^{\infty} \frac{\chi(k)}{(mk)^s} = \sum_{n=1}^{\infty} \sum_{d|n} \frac{\chi(d)}{n^s}$. Por otro lado, dado que f es constante e igual a $f(n)$ en cada intervalo $[n, n+1)$, se verifica que $sL_f(s) = \sum_{n=1}^{\infty} \int_n^{n+1} \frac{sf(x)}{x^{s+1}} = \sum_{n=1}^{\infty} f(n)(n^{-s} - (n+1)^{-s}) = 1 + \sum_{n=2}^{\infty} \frac{f(n)-f(n-1)}{n^s}$. Además, se cumple que $f(n)-f(n-1) = \sum_{n-1<k\leq n} \sum_{d|k} \chi(d) = \sum_{d|n} \chi(d)$. Por tanto, $sL_f(s) = \sum_{n=1}^{\infty} \sum_{d|n} \frac{\chi(d)}{n^s}$ y se tiene la igualdad deseada. Por el teorema de unicidad la igualdad se extendería a $\Re(s) > 0$ suponiendo que $L(1,\chi) = 0$, pues $\zeta(s)L(s,\chi)$ sería holomorfa allí. Por tanto, si suponemos que $f \geq 0$ y aplicamos el teorema 4.16, obtenemos que $L_f(s)$ converge para $\Re(s) > 0$ (en particular para $s = 1/2$). □

Teorema 4.22. *Se verifica que $c(n) \geq 0$, $c(n^2) \geq 1$, $f(n^2) \geq n$ y $L_f(1/2)$ no converge.*

Demostración. Sea $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, como c es multiplicativa, basta probar que $c(p^m) \geq 0$ con p primo y $m \in \mathbb{N}$ (nótese que $c(n) = \prod_{i=1}^{k} c(p_i^{\alpha_i})$). Asimismo, $c(p^m) = \sum_{i=0}^{m} \chi(p^i)$. Si $\chi(p)$ es 0 o 1 es trivial. Si $\chi(p) = -1$, se tiene que $c(p^m) = 1 - 1 + 1 - 1...$ y esta suma siempre es positiva, tanto si termina en -1, en cuyo caso $c(p^m) = 0$, como si termina en 1, donde se tiene que $c(p^m) = 1$. Para ver que $c(n^2) \geq 1$ aplicamos nuevamente que c es multiplicativa, por lo que basta probarlo para el caso de un primo p elevado a un m par, como es el caso para los factores primos de n^2. Si $\chi(p) = 0$, entonces $c(p^m) = 1$ y si $\chi(p) = \pm 1$ entonces $\chi(p^m) = 1$, luego $c(p^m) \geq 1$ (de hecho es exactamente 1 en el caso de que $\chi(p) = -1$ por el razonamiento anterior y es igual a $m+1$ si $\chi(p) = 1$).
Sea $A = \{k : k^2 \leq n^2\}$, se verifica que $c(k^2) \geq 1$ y $|A| = n$. Además, para el resto de $k \leq n^2$, $c(k) \geq 0$. Por tanto, $f(n^2) = \sum_{1 \leq k \leq n^2} c(k) \geq n$. Por último, nótese que $f(x) = f(\lfloor x \rfloor)$ para todo $x \in [1, \infty)$ y que f es creciente, luego dado $n \in \mathbb{N}$, sea k^2 el mayor cuadrado menor que n, se verifica que $f(n) \geq f(k^2) \geq k = \lfloor \sqrt{n} \rfloor$. Por tanto, tenemos que $L_f(1/2) = \int_1^{\infty} \frac{f(x)}{x^{3/2}} = \sum_{n=1}^{\infty} \int_n^{n+1} \frac{f(n)}{x^{3/2}} dx \geq \sum_{n=1}^{\infty} f(n)(n+1)^{-3/2} \geq \sum_{n=1}^{\infty} \lfloor \sqrt{n} \rfloor (n+1)^{-3/2}$ que tiene el mismo tipo de convergencia que la serie $\sum_{n=1}^{\infty} \sqrt{n} n^{-3/2} = \sum_{n=1}^{\infty} \frac{1}{n}$. Es decir, $L_f(1/2)$ diverge. □

En consecuencia, el teorema 4.22 supone una contradicción con el teorema 4.21 salvo si $L(1,\chi) \neq 0$ y tenemos lo que queríamos.

Capítulo 5

Ecuaciones funcionales y caracteres cuadráticos

Definición 5.1. Módulo inducido: Sea χ un carácter de Dirichlet módulo q y sea d un divisor positivo de q. El número d se llama módulo inducido de χ si $\chi(a) = 1$ siempre que $mcd(a, q) = 1$ y $a \equiv 1 \pmod{d}$. Es decir, d es un módulo inducido si el carácter χ mód q actúa como un carácter mód d en los representantes de la clase $\overline{1}$ mód d que son coprimos con q.

Definición 5.2. Carácter primitivo: Un carácter de Dirichlet mód q se dice primitivo si no tiene módulos inducidos $d < q$. Es decir, χ es primitivo mód q si y sólo si para cada divisor de q, $0 < d < q$, existe un entero $a \equiv 1 \pmod{d}$, $mcd(a, q) = 1$ tal que $\chi(a) \neq 1$.

Proposición 5.3. *Sea χ un carácter de Dirichlet mód q, entonces:*

I) *1 es un módulo inducido de χ si y sólo si $\chi = \chi_0$.*

II) *Sea $d|q, d > 0$, entonces d es módulo inducido de χ si y sólo si $\chi(a) = \chi(b)$ siempre que $(a, q) = (b, q) = 1$ y $a \equiv b \pmod{d}$.*

Demostración. Para la primera, si $\chi = \chi_0$ entonces $\chi(a) = 1$ si $(a, q) = 1$ y como todo a satisface que $a \equiv 1 \pmod{1}$ entonces 1 es módulo inducido. Recíprocamente, si 1 es módulo inducido entonces $\chi(a) = 1$ siempre que $(a, q) = 1$, luego $\chi = \chi_0$ pues χ se anula en los números que no son coprimos con q. Veamos ahora la segunda. Si se da la condición de la derecha, entonces d es módulo inducido pues podemos elegir $b = 1$ y usar la definición 5.1. Recíprocamente, elijamos a y b que verifiquen dicha condición y veamos que $\chi(a) = \chi(b)$. Sea a' el inverso de a mód q, $aa' \equiv 1 \pmod{q}$, que existe porque $(a, q) = 1$. Por tanto, $aa' \equiv 1 \pmod{d}$ pues $d|q$. Así, $\chi(aa') = 1$ porque d es módulo inducido. Sin embargo, $aa' \equiv ba' \pmod{d}$ porque $a \equiv b \pmod{d}$, luego $\chi(a)\chi(a') = \chi(b)\chi(a')$. Como $\chi(a)\chi(a') = 1$, entonces $\chi(a') \neq 0$ y se tiene el resultado. □

Proposición 5.4. *Si χ es un carácter primitivo mód q, entonces se verifica que $|\tau(\chi)| = \sqrt{q}$.*

Demostración. Por las proposiciones 4.8 y 4.9 tenemos que $\chi(n)\overline{\tau(\chi)} = \sum_{h_1=1}^{q} \overline{\chi}(h_1)e_q(-nh_1)$ y $\overline{\chi}(n)\tau(\chi) = \sum_{h_2=1}^{q} \chi(h_2)e_q(nh_2)$. Por tanto:

$$|\chi(n)|^2|\tau(\chi)|^2 = \sum_{h_1}^{q}\sum_{h_2}^{q} \overline{\chi}(h_1)\chi(h_2)e_q(n(h_2-h_1)).$$

Ahora, sumando en n para un conjunto completo de residuos modulo q, se tiene que la suma de los $|\chi(n)|^2$ es $\varphi(q)$ puesto que $|\chi(n)| = 1$ si $\text{mcd}(n,q) = 1$ y $|\chi(n)| = 0$ en otro caso. Asimismo, la suma de las exponenciales es 0 salvo si $h_1 \equiv h_2$. En efecto, si $h_1 \equiv h_2$, entonces $e_q(n(h_2-h_1)) = e_q(0) = 1$ y la suma es q. En caso contrario, sea $d = h_2 - h_1$. Se tiene que $\sum_{n=1}^{q} e_q(nd)$ es una serie geométrica de razón $z = e^{2\pi id/q}$. Así, dicha suma es $\frac{z(1-z^q)}{1-z}$ bien definida pues $z \neq 1$. Además, como z es una raíz q-ésima de la unidad, se tiene que esa suma es 0. Por último, nótese que si $h_1 \equiv h_2$, entonces $\overline{\chi}(h_1)\chi(h_2) = |\chi(h_2)|^2$ pues $\chi(h_1) = \chi(h_2)$. Por todo ello, se cumple que: $\varphi(q)|\tau(\chi)|^2 = q\sum_h |\chi(h)|^2 = q\varphi(q)$ y se tiene el resultado. □

Nuestro primer objetivo es demostrar la ecuación funcional de las funciones L para caracteres primitivos, siguiendo la línea del teorema 2.11 y el corolario 2.13 para ζ. Esta dependerá del valor que χ asigne a -1 [6]. Supongamos que $\chi(-1) = 1$. En la demostración del teorema 2.11 obtuvimos que $\Gamma(\frac{s}{2}) = \pi^{\frac{s}{2}} n^s \int_0^\infty x^{\frac{s}{2}-1}e^{-\pi n^2 x}dx$. Haciendo el cambio de variable $x = \frac{y}{q}$ y cambiando después y por x, tenemos que $\pi^{-\frac{s}{2}} q^{\frac{s}{2}}\Gamma(\frac{s}{2})n^{-s} = \int_0^\infty x^{\frac{s}{2}-1}e^{-n^2\pi x/q}dx$. Multiplicando por $\chi(n)$ y sumando en n, obtenemos:

$$\pi^{-\frac{s}{2}} q^{\frac{s}{2}}\Gamma\Big(\frac{s}{2}\Big)L(s,\chi) = \int_0^\infty x^{\frac{s}{2}-1}\sum_{n=1}^{\infty}\chi(n)e^{-n^2\pi x/q}dx, \quad \text{para } \Re(s) > 1.$$

Donde el intercambio de suma e integral está justificado por el teorema de convergencia de Levi, [1], Th.10.26. Como $\chi(-1) = 1$ y $\chi(0) = 0$, se tiene que $\chi(n) = \chi(-n)$ y podemos poner la parte derecha de la igualdad como sigue:

$$\frac{1}{2}\int_0^\infty x^{\frac{s}{2}-1}F(x,\chi)dx, \quad \text{donde } F(x,\chi) = \sum_{-\infty}^{\infty}\chi(n)e^{-n^2\pi x/q}. \tag{5.1}$$

La tarea entonces consiste en encontrar una ecuación funcional para $F(x,\chi)$. Para ello necesitamos un lema previo que nos será de gran utilidad.

Lema 5.5. *Sea $x > 0$ y $\alpha \in \mathbb{R}$ arbitrario, se verifica que:*

$$\sum_{-\infty}^{\infty} e^{-(n+\alpha)^2\pi/x} = \sqrt{x}\sum_{-\infty}^{\infty} e^{-n^2\pi x + 2\pi i n\alpha}. \tag{5.2}$$

Demostración. Consideramos la función $F(x) = \sum_{n\in\mathbb{Z}} e^{-\pi(n+x)^2 t}$ usada en la proposición 2.9. Con la notación de dicha proposición, vimos que si $t > 0$ y $x \in \mathbb{R}$, entonces $F(x) = \frac{1}{\sqrt{t}}\sum_{n=-\infty}^{\infty} e^{-\pi\frac{n^2}{t}+2\pi i n x}$. Cambiando ahora x por α y t por x^{-1} en la notación anterior, se tiene el resultado. □

Teorema 5.6. *Sea $x > 0$, se verifica que:*

$$\tau(\overline{\chi})F(x,\chi) = (q/x)^{\frac{1}{2}}F(x^{-1},\overline{\chi}).$$

Demostración.

$$\tau(\overline{\chi})F(x,\chi) = \sum_{m=1}^{q}\overline{\chi}(m)\sum_{n=-\infty}^{\infty}e^{-n^2\pi x/q+2\pi imn/q} = \sum_{m=1}^{q}\overline{\chi}(m)(q/x)^{\frac{1}{2}}\sum_{n=-\infty}^{\infty}e^{-(n+m/q)^2\pi q/x} =$$

$$(q/x)^{\frac{1}{2}}\sum_{m=1}^{q}\overline{\chi}(m)\sum_{n=-\infty}^{\infty}e^{-(nq+m)^2\pi/xq} = (q/x)^{\frac{1}{2}}\sum_{l=-\infty}^{\infty}\overline{\chi}(l)e^{-l^2\pi/xq} = (q/x)^{\frac{1}{2}}F(x^{-1},\overline{\chi}).$$

Donde en la segunda igualdad hemos usado el lema 5.5 y en la cuarta que $\overline{\chi}(m) = \overline{\chi}(l)$ con $l = nq + m$. □

Ahora dividimos la integral de (5.1) en dos partes y usamos el teorema 5.6:

$$\pi^{-\frac{s}{2}}q^{\frac{s}{2}}\Gamma\Big(\frac{s}{2}\Big)L(s,\chi) = \frac{1}{2}\int_1^\infty x^{\frac{s}{2}-1}F(x,\chi)dx + \frac{1}{2}\int_1^\infty x^{-\frac{s}{2}-1}F(x^{-1},\chi)dx =$$

$$= \frac{1}{2}\int_1^\infty x^{\frac{s}{2}-1}F(x,\chi)dx + \frac{1}{2}\frac{\sqrt{q}}{\tau(\overline{\chi})}\int_1^\infty x^{-\frac{s}{2}-\frac{1}{2}}F(x,\overline{\chi})dx. \tag{5.3}$$

Donde hemos usado que $\int_0^1 x^{\frac{s}{2}-1}F(x,\chi)dx = \int_1^\infty x^{-\frac{s}{2}-1}F(x^{-1},\chi)dx$ haciendo el cambio de variable $x \to x^{-1}$. Posteriormente hemos aplicado el teorema 5.6 y hemos obtenido la segunda integral en (5.3). Esta expresión representa una función de s holomorfa en todo el plano complejo (la demostración es análoga a la realizada para la ecuación funcional de ζ pues $F(x,\chi)$ también es una función de decaimiento rápido como lo era $w(x)$) y, por tanto, nos da la extensión analítica de $L(s,\chi)$ sobre $\mathbb{C}$, holomorfa en todo el plano pues $\Gamma(\frac{s}{2}) \neq 0$. Además, si reemplazamos s por $1-s$ y χ por $\overline{\chi}$, la expresión anterior se convierte en:

$$\frac{1}{2}\frac{\sqrt{q}}{\tau(\chi)}\int_1^\infty x^{\frac{s}{2}-1}F(x,\chi)dx + \frac{1}{2}\int_1^\infty x^{-\frac{s}{2}-\frac{1}{2}}F(x,\overline{\chi})dx,$$

que es igual a (5.3) multiplicada por $\frac{\sqrt{q}}{\tau(\chi)}$ pues $\tau(\chi)\tau(\overline{\chi}) = q$. Esto último se debe a que, como $\chi(n) = \chi(-n)$, entonces $\tau(\overline{\chi}) = \overline{\tau(\chi)}$ y la igualdad se sigue de la proposición 5.4. Así, hemos obtenido la ecuación funcional de $L(s,\chi)$:

$$\pi^{-\frac{1-s}{2}}q^{\frac{1-s}{2}}\Gamma\Big(\frac{1-s}{2}\Big)L(1-s,\overline{\chi}) = \frac{\sqrt{q}}{\tau(\chi)}\pi^{-\frac{s}{2}}q^{\frac{s}{2}}\Gamma\Big(\frac{s}{2}\Big)L(s,\chi). \tag{5.4}$$

Esta ecuación es válida para todo carácter primitivo módulo q tal que $\chi(-1) = 1$. Sea $\sigma = \Re(s)$, como $L(1-s,\overline{\chi})$ no tiene ceros para $1-\sigma > 1$, es decir, para $\sigma < 0$ y $\Gamma(\frac{1-s}{2})$ no tiene ceros, se deduce que los únicos ceros de $L(s,\chi)$ para $\sigma < 0$ están en $s = -2, -4, -6, ...$, que corresponden a los polos de $\Gamma(\frac{s}{2})$.

Supongamos ahora que $\chi(-1) = -1$. El argumento anterior falla pues la función $F(x,\chi)$ es idénticamente cero. Modificamos por tanto el argumento cambiando $\frac{1}{2}(s+1)$ en lugar de $\frac{s}{2}$ en la fórmula original. Con este ligero ajuste, la fórmula ahora es:

$$\pi^{-\frac{1}{2}(s+1)} q^{\frac{1}{2}(s+1)} \Gamma\Big(\frac{1}{2}(s+1)\Big) n^{-s} = \int_0^\infty n e^{-n^2\pi x/q} x^{\frac{s}{2}-\frac{1}{2}} dx,$$

y obtenemos que:

$$\pi^{-\frac{1}{2}(s+1)} q^{\frac{1}{2}(s+1)} \Gamma\Big(\frac{1}{2}(s+1)\Big) L(s,\chi) = \frac{1}{2}\int_0^\infty G(x,\chi) x^{\frac{s}{2}-\frac{1}{2}} dx,$$

donde $G(x,\chi) = \sum_{-\infty}^{\infty} n\chi(n) e^{-n^2\pi x/q}$ pues $n\chi(n) = -n\chi(-n), \forall n \in \mathbb{N}$.

Lema 5.7.

$$\sum_{-\infty}^{\infty} n e^{-n^2\pi x/q + 2\pi i m n/q} = i(q/x)^{\frac{3}{2}} \sum_{-\infty}^{\infty} (n+m/q) e^{-\pi(n+m/q)^2 q/x}.$$

Demostración. Usando el lema 5.5, podemos derivar con respecto de α a ambos lados de la expresión (5.2), pues las series obtenidas de derivar término a término convergen uniformemente. Esto da:

$$2\pi i \sum_{-\infty}^{\infty} n e^{-n^2\pi x + 2\pi i n\alpha} = -2\pi x^{-\frac{3}{2}} \sum_{-\infty}^{\infty} (n+\alpha) e^{-(n+\alpha)^2\pi/x}.$$

y se tiene el resultado cambiando x por x/q y α por m/q. □

La ecuación funcional que satisface $G(x,\chi)$, análogamente a la de $F(x,\chi)$, es la siguiente:

Teorema 5.8.

$$\tau(\overline{\chi}) G(x,\chi) = i q^{\frac{1}{2}} x^{-\frac{3}{2}} G(x^{-1}, \overline{\chi}).$$

Demostración. Aplicando el lema 5.7 tenemos que:

$$\tau(\overline{\chi}) G(x,\chi) = \sum_{m=1}^{q} \overline{\chi}(m) \sum_{n=-\infty}^{\infty} n e^{-n^2\pi x/q + 2\pi i m n/q} = i(q/x)^{\frac{3}{2}} \sum_{m=1}^{q} \overline{\chi}(m) \sum_{n=-\infty}^{\infty} (n+m/q) e^{-\pi(n+m/q)^2 q/x}$$

$$= i q^{\frac{1}{2}} x^{-\frac{3}{2}} \sum_{m=1}^{q} \overline{\chi}(m) \sum_{n=-\infty}^{\infty} (m+nq) e^{-\pi(m+nq)^2/xq} = i q^{\frac{1}{2}} x^{-\frac{3}{2}} \sum_{l=-\infty}^{\infty} \overline{\chi}(l) e^{-\pi l^2/xq} = i q^{\frac{1}{2}} x^{-\frac{3}{2}} G(x^{-1}, \overline{\chi}).$$

□

Usando el teorema 5.8 se obtiene que:

$$\pi^{-\frac{1}{2}(s+1)} q^{\frac{1}{2}(s+1)} \Gamma\Big(\frac{1}{2}(s+1)\Big) L(s,\chi) = \frac{1}{2}\int_1^\infty G(x,\chi) x^{\frac{s}{2}-\frac{1}{2}} dx + \frac{1}{2}\int_1^\infty G(x^{-1},\chi) x^{-\frac{s}{2}-\frac{3}{2}} dx =$$

$$= \frac{1}{2}\int_1^\infty G(x,\chi) x^{\frac{s}{2}-\frac{1}{2}} dx + \frac{1}{2}\frac{i q^{\frac{1}{2}}}{\tau(\overline{\chi})} \int_1^\infty G(x,\overline{\chi}) x^{-\frac{s}{2}} dx. \tag{5.5}$$

Esto se debe a que $\int_0^1 G(x,\chi) x^{\frac{s}{2}-\frac{1}{2}} dx = \int_1^\infty G(x^{-1},\chi) x^{-\frac{s}{2}-\frac{3}{2}} dx$ haciendo el cambio de variable $x \to x^{-1}$. Nuevamente esta expresión nos da una continuación analítica de $L(s,\chi)$ como función holomorfa en todo $\mathbb{C}$ pues $G(x,\chi)$ es una función de decaimiento rápido. Si reemplazamos s por

$1-s$ y χ por $\overline{\chi}$, dicha expresión es igual que (5.5) pero multiplicada por $\frac{iq^{\frac{1}{2}}}{\tau(\chi)}$ dado que ahora $\tau(\chi)\tau(\overline{\chi}) = -q$ pues $\chi(-n) = -\chi(n)$ y $\overline{\tau(\chi)} = -\tau(\overline{\chi})$. Por tanto, la ecuación funcional en este caso queda como sigue:

$$\pi^{-\frac{1}{2}(2-s)}q^{\frac{1}{2}(2-s)}\Gamma\Big(\frac{1}{2}(2-s)\Big)L(1-s,\overline{\chi}) = \pi^{-\frac{1}{2}(s+1)}q^{\frac{1}{2}(s+1)}\Gamma\Big(\frac{1}{2}(s+1)\Big)L(s,\chi). \tag{5.6}$$

Análogamente, se obtiene que los ceros de $L(s,\chi)$ para $\sigma < 0$ son los polos de $\Gamma\Big(\frac{1}{2}(s+1)\Big)$, es decir, $s = -1, -3, -5, ...$

Ejemplo 1: Si χ no es primitivo, entonces no tenemos la proposición 5.4 y todo el argumento anterior se desmorona. Ahí es donde se puede apreciar la importancia de tratar con caracteres primitivos. Sin embargo, aún podemos conseguir una ecuación funcional. Sea el carácter módulo 1575, $\chi(n) = \left(\frac{n}{1575}\right)$ donde los paréntesis indican el símbolo de Jacobi. Entonces 7 es un módulo inducido de χ pues si $a \equiv 1 \pmod 7$ y $(a, 1575) = 1$, $\left(\frac{a}{7}\right) = 1$. Por tanto, $\chi(a) = \left(\frac{a}{3}\right)^2\left(\frac{a}{5}\right)^2 = 1$. Además, 3 y 5 no son módulos inducidos por los contraejemplos respectivos 19 y 31. Luego $\chi(n) = \psi(n)\chi_0(n)$, donde $\psi(n) = \left(\frac{n}{7}\right)$ carácter módulo 7 y χ_0 es el carácter trivial módulo 1575. Por tanto, $L(s,\chi) = L(s,\psi)\prod_{p|1575}(1 - \frac{\psi(p)}{p^s}) = L(s,\psi)(1+3^{-s})(1+5^{-s})$. Como ψ es un carácter primitivo tal que $\psi(-1) = 1$, obtenemos la ecuación funcional para $L(s,\chi)$ usando (5.4). Este ejemplo motiva los siguientes resultados:

Definición 5.9. Sea χ un carácter de Dirichlet mód q, se llama conductor de χ al menor d que es módulo inducido de χ. Si el carácter es primitivo, su conductor es q.

Teorema 5.10. *Sea χ carácter de Dirichlet mód q y sea $d|q, d > 0$. Entonces son equivalentes:*

a) d es un módulo inducido de χ.

b) Existe un carácter ψ mód d tal que $\chi(n) = \psi(n)\chi_0(n)$ con χ_0 el carácter principal mód q.

De ello se deduce que todo carácter de Dirichlet mód q se puede expresar como un producto $\chi(n) = \psi(n)\chi_0(n)$ con χ_0 el carácter principal mód q y ψ un carácter primitivo módulo el conductor de χ.

Demostración. b) implica a) es obvio. Para ver la otra implicación vamos a construir el carácter ψ: Si $(n,d) > 1$, entonces $\psi(n) = 0$. En este caso también tenemos que $(n,q) > 1$, luego la igualdad se sostiene. Sea ahora $(n,d) = 1$, entonces existe un entero m tal que $m \equiv n \pmod d$ y $(m,q) = 1$ por el teorema de Dirichlet. Dicho m es único mód d, luego definiendo $\psi(n) = \chi(m)$ se tiene que ψ está bien definida porque χ toma los mismos valores en números que sean congruentes mód d y coprimos con q (proposición 5.3). Veamos que se tiene lo que queremos: si $(n,q) = 1$, entonces $(n,d) = 1$, luego $\psi(n) = \chi(m)$ para cierto $m \equiv n \pmod d, (m,q) = 1$. Por la proposición 5.3, $\chi(n) = \chi(m) = \psi(n) = \psi(n)\chi_0(n)$, pues $\chi_0(n) = 1$. Si $(n,q) > 1$, entonces $\chi(n) = \chi_0(n) = 0$ y ambos miembros son 0. Para la segunda parte, sea d el conductor de χ. Sabemos que χ se puede expresar de esa forma con ψ carácter mód d. Veamos que ψ es primitivo. Supongamos que no lo es,

entonces existe un divisor k de d, $k < d$, que es módulo inducido de ψ. Sea $n \equiv 1 \pmod{k}, (n,q) = 1$, entonces $(n,d) = 1$ y $\chi(n) = \psi(n) = \psi(1) = 1$. Luego k es módulo inducido de χ y llegamos a contradicción. □

Observación 5.11. Sea χ carácter de Dirichlet mód q y sea d un módulo inducido. Entonces, escribiendo $\chi(n) = \psi(n)\chi_0(n)$ como en el teorema 5.10, se tiene que $L(s,\chi) = L(s,\psi)\prod_{p|q}(1 - \psi(p)p^{-s})$ sin más que comparando productos de Euler. Por tanto, toda función $L(s,\chi)$ asociada a un carácter de Dirichlet no primitivo, tiene una ecuación funcional obtenida alterando ligeramente la ecuación funcional de $L(s,\psi)$ con ψ el carácter primitivo módulo su conductor, como vimos en el ejemplo 1.

A continuación, vamos a particularizar la ecuación funcional de las funciones L al caso de caracteres cuadráticos/reales, que vienen dados en general por símbolos de Jacobi (o Kronecker).

Teorema 5.12. *Sea $n \in \mathbb{Z}^+$ impar, definimos $\chi_n(m)$ como 0 si m es par y como $\left(\frac{2n}{|m|}\right)$ si m es impar. Se tiene que χ_n es un carácter de Dirichlet módulo $8n$ y es primitivo si y sólo si n es libre de cuadrados.*

Demostración. Sea $m > 0$ impar tal que $(m,n) = (m+8n,n) = 1$ (nótese que $m+8n$ es impar, pues de lo contrario $\chi_n(m+8n) = 0 \neq \chi_n(m)$). Aplicando primero que el símbolo de Jacobi es totalmente multiplicativo y luego la ley de reciprocidad cuadrática para este símbolo, se tiene que $\chi_n(m) = \chi_n(m+8n)$ pues $\left(\frac{m}{n}\right) = \left(\frac{m+8n}{n}\right)(-1)^{(8n)^2/8}(-1)^{8nm/4}(-1)^{8n(n-1)/4}$. Además, si m es par, $\chi_n(m) = 0 = \chi_n(m+8n)$ y si m es impar con $(m,n) > 1$, entonces $(m+8n,n) > 1$ y se tiene de nuevo la igualdad. Ahora veamos que ocurre con los negativos. Si $m > 8n$ impar con $(m,n) = 1$, $\chi_n(-m) = \chi(m) = \chi(m-8n) = \chi(-m+8n)$. Si $0 < m < 8n$ impar con $(m,n) = 1$. Veamos que $\chi_n(-m) = \chi_n(m) = \chi_n(-m+8n)$. Esto sucederá si $(-1)^{(m-1)(n-1)/4} = \left(\frac{-1}{n}\right)(-1)^{(-m+8n-1)(n-1)/4}$ lo cual se verifica sea cual sea n. Por consiguiente, χ_n es un carácter de Dirichlet mód $8n$. Para la segunda parte, consideremos los caracteres: χ, definido como $\left(\frac{2}{m}\right)$ si $4|n-1$ y como $\left(\frac{-2}{m}\right)$ si $4|n-3$ y $\psi_n(m) = \left(\frac{m}{n}\right)$. χ es un carácter de Dirichlet módulo 8 y primitivo: $\chi(m) = \chi(m+8)$ y $\chi(5) = -1$ independientemente de n, luego 2 y 4 no son módulos inducidos. Además, $\chi_n(m) = \chi(m)\psi_n(m)$. Por otro lado, ψ_n es un carácter de Dirichlet mód n. Como $(n,8) = 1$, $\chi_n = \chi\psi_n$ es primitivo si y sólo si lo son χ y ψ_n ([10], Lem.9.3). Veamos cuándo es primitivo ψ_n. Al igual que en el ejemplo 1, si $n = \prod_{j=1}^{n} p_j^{\alpha_j}$, tomando $n = kt$ con t el subproducto resultante de agrupar los cuadrados y k el resto, se tiene que $\psi_n(m) = \left(\frac{m}{k}\right)\chi_0(m)$ con χ_0 el carácter trivial mód n. Por tanto, para que ψ_n sea primitivo, n debe ser libre de cuadrados. Recíprocamente, usando de nuevo [10], Lem.9.3, se tiene que, si n es libre de cuadrados, entonces ψ_n es primitivo por serlo cada carácter $\left(\frac{m}{p_j}\right)$ con p_j primo y se tiene el resultado. □

Lema 5.13. *Sea $p > 2$ primo, entonces* $\frac{1}{\sqrt{p}}\sum_{n=1}^{p}\left(\frac{n}{p}\right)e^{2\pi in/p} = \begin{cases} 1, & si\ 4|p-1 \\ i, & si\ 4 \nmid p-1. \end{cases}$

Demostración. Por [10], Cor.9.16, sabemos que $\hat{S} = \sum_{n=1}^{p} e^{2\pi i n^2/p} = \frac{1+i^{-p}}{1-i}\sqrt{p}$ (una fórmula debida a Gauss que, de hecho, implica la ley de reciprocidad cuadrática). Sean $0 < x \neq y < p$ tales que $x^2 \equiv y^2 \pmod{p}$, entonces $(x-y)(x+y) \equiv 0 \pmod{p}$, luego $x + y = p$. Como p es primo, hay exactamente $\frac{p-1}{2}$ residuos cuadráticos, y, por lo anterior, exactamente 2 clases cuyos cuadrados son el mismo. Así, $S = \sum_{n=1}^{p} \left(\frac{n}{p}\right) e^{2\pi i n/p} = \sum_{n=1,\left(\frac{n}{p}\right)=1}^{p} e^{2\pi i n/p} - \sum_{n=1,\left(\frac{n}{p}\right)=-1}^{p} e^{2\pi i n/p}$. Además, se tiene que $\sum_{n=1}^{p} e^{2\pi i n/p} = \frac{e^{2\pi i}-1}{e^{2\pi i/p}-1} = 0$, luego $-\sum_{n=1,\left(\frac{n}{p}\right)=-1}^{p} e^{2\pi i n/p} = \sum_{n=1,\left(\frac{n}{p}\right)=1}^{p} e^{2\pi i n/p} + 1$. Por tanto, $S = 1 + 2\sum_{n=1,\left(\frac{n}{p}\right)=1}^{p} e^{2\pi i n/p} = \hat{S}$, donde la última igualdad se deduce de lo comentado previo a los cálculos. Finalmente, nótese que $\frac{1}{\sqrt{p}}\hat{S}$ es lo dicho en el enunciado. □

Proposición 5.14. *Si χ_n es primitivo, entonces $\tau(\chi_n) = \sqrt{8n}$.*

Demostración. Con la notación usada en la demostración de 5.12 se tiene que, por [10], Th. 9.7, $\tau(\chi_n) = \tau(\chi)\tau(\psi_n)\chi(n)\psi_n(8)$. Por un lado, si $4|n-1$, entonces $\chi(n)\psi_n(8) = 1$ y $\tau(\chi) = e^{\pi i/4} - e^{3\pi i/4} - e^{5\pi i/4} + e^{7\pi i/4} = \sqrt{8}$. Por otro lado, si $4|n-3$, $\chi(n)\psi_n(8) = -1$ y $\tau(\chi) = e^{\pi i/4} + e^{3\pi i/4} - e^{5\pi i/4} - e^{7\pi i/4} = \sqrt{8}i$. Para calcular $\tau(\psi_n)$ recordemos que χ_n es primitivo si y sólo si n es libre de cuadrados. Así, si $n = \prod_{j=1}^{k} p_j$, se tiene que $\tau(\psi_n) = \prod_{j=1}^{k} \tau(\psi_{p_j}) \prod_{i\neq j} \psi_{p_i}(p_j)$ usando de nuevo [10], Th. 9.7. Por el lema 5.13, $\tau(\psi_{p_j}) = \begin{cases} \sqrt{p_j}, \text{ si } 4|p_j - 1 \\ i\sqrt{p_j}, \text{ si } 4 \nmid p_j - 1 \end{cases}$. Por la ley de reciprocidad cuadrática, $\psi_{p_i}(p_j)\psi_{p_j}(p_i) = \begin{cases} 1, \text{ si } 4|p_j - 1 \text{ o } 4|p_i - 1 \\ -1, \text{ si } 4 \nmid p_j - 1, p_i - 1 \end{cases}$. Además, el número de factores primos de n congruentes con 3 mód 4 es una cantidad par si $4|n-1$ e impar si $4|n-3$. Por tanto, si $4|n-1$ y p_i, p_j son congruentes con 3 mód 4, entonces $\tau(\psi_{p_j})\tau(\psi_{p_i})\psi_{p_i}(p_j)\psi_{p_j}(p_i) = \sqrt{p_j p_i}$. En definitiva, $\tau(\psi_n) = \sqrt{n}$. En cambio, si $4|n-3$, al agrupar en pares los factores primos de n congruentes con 3 mód 4, sobra uno. El primo p_k que falta cumple que $\tau(\psi_{p_k}) = i\sqrt{p_k}$. Por el mismo razonamiento que antes $\tau(\psi_n) = i\sqrt{n}$, luego $\tau(\chi_n) = \sqrt{8n}$. □

Lema 5.15. *Sea $s \in \mathbb{C} - \mathbb{Z}$, entonces $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\operatorname{sen}(\pi s)}$. Además, si $s \in \mathbb{C}$, se tiene la fórmula de duplicación $\Gamma(s)\Gamma(s+1/2) = 2^{1-2s}\sqrt{\pi}\Gamma(2s)$.*

Demostración. Por el teorema de convergencia monótona, $\Gamma(s) = \lim_{n\to\infty} \int_0^n (1 - x/n)^n x^{s-1} dx = \lim_{n\to\infty} \frac{n^s n!}{s(s+1)\ldots(s+n)}$ aplicando integración por partes sucesivamente. Sea $H_n = 1 + 1/2 + \ldots + 1/n$, sabemos que $H_n - \log n \to \gamma$ cuando $n \to \infty$, donde γ denota la constante de Euler-Mascheroni. Podemos escribir $n^s = e^{s(\log n - H_n)} e^{sH_n}$ y deducimos la fórmula de Weierstrass:

$$\frac{1}{s\Gamma(s)} = e^{\gamma s} \prod_{n=1}^{\infty} \left(1 + \frac{s}{n}\right) e^{-s/n}. \tag{5.7}$$

Como $\operatorname{sen}(\pi s) = \pi s \prod_{n=1}^{\infty}(1 - \frac{s^2}{n^2})$ [12] y $\Gamma(1-s) = -s\Gamma(-s)$, se tiene el primer resultado. Para obtener la fórmula de duplicación, aplicamos 2.8 y se tiene que $\sqrt{\pi}\Gamma(s) = \Gamma(s+1/2)\int_0^\infty x^{-1/2}(1+x)^{-s-1/2}dx$. Denotando a esta integral por I, se tiene que $I = 2^{2s-1}\int_0^\infty y^{s-1}(1+y)^{-2s}dy =$

$2^{2s-1}\frac{\Gamma(s)^2}{\Gamma(2s)}$ pues $\Gamma(s)^2 = \Gamma(2s)\int_0^\infty x^{s-1}(1+x)^{-2s}dx$, por la fórmula del teorema 2.8 y se tiene el segundo resultado. □

Teorema 5.16. *Si χ_n es primitivo, entonces $\chi_n(-1) = 1$ y se tiene que*

$$L(s,\chi_n) = 2^{3/2-2s}n^{1/2-s}\pi^{s-1}\Gamma(1-s)\operatorname{sen}\Big(\frac{\pi s}{2}\Big)L(1-s,\chi_n).$$

Demostración. Sabemos que $\chi_n(-1) = \chi_n(8n-1)$. Además, $\chi_n(8n-1) = \left(\frac{2^2 2n}{8n-1}\right) = \left(\frac{8n-(8n-1)}{8n-1}\right) = 1$. Por tanto, la ecuación funcional de $L(s,\chi_n)$ viene dada por la fórmula (5.4). Aplicando la proposición 5.14, que χ_n es un carácter real (coincide con su conjugado) y despejando $L(s,\chi_n)$ se obtiene:

$$L(s,\chi_n) = \pi^{s-1/2}(8n)^{1/2-s}\Gamma\Big(\frac{s}{2}\Big)^{-1}\Gamma\Big(\frac{1-s}{2}\Big)L(1-s,\chi_n).$$

Por el lema 5.15, $\Gamma(\frac{s}{2})\Gamma(1-s/2) = \frac{\pi}{\operatorname{sen}(\frac{\pi s}{2})}$ y $\Gamma(1-s/2)\Gamma(\frac{1-s}{2}) = 2^s\sqrt{\pi}\Gamma(1-s)$, luego $\Gamma(\frac{s}{2})^{-1}\Gamma(\frac{1-s}{2}) = \frac{\operatorname{sen}(\frac{\pi s}{2})}{\pi}2^s\sqrt{\pi}\Gamma(1-s)$ y se tiene el resultado. □

Observación 5.17. Aplicando el lema 5.15 se puede obtener de igual manera la ecuación funcional antisimétrica de $\zeta(s)$: $\zeta(s) = 2(2\pi)^{s-1}\operatorname{sen}(\frac{\pi s}{2})\Gamma(1-s)\zeta(1-s)$.

A finales de los años 90, algunos investigadores se percataron de que al combinar funciones L de caracteres cuadráticos tanto primitivos como no primitivos en una función L "múltiple", los problemas desaparecían y dicha función L múltiple adquiría una ecuación funcional sencilla además de buenas propiedades de extensión meromorfa. Esto es lo que vamos a tratar a continuación.

Definición 5.18. Definimos

$$L(s,w) = (2^{2s+2w-1}-1)\zeta(2s+2w-1)\sum_{\substack{n=1\\ 2\nmid n}}^{\infty}\frac{L(s,\chi_n)}{n^w}.$$

Nótese que la suma se podría escribir como una suma doble en $\chi_n(m)m^{-s}n^{-w}$. En ese sentido, dicha función es una función L doble. Es fácil ver que para $\Re(s), \Re(w) > 1$ hay convergencia.

Nuestro propósito es obtener una ecuación funcional sencilla para $L(s,w)$ lo cual es sorprendente ya que las $L(s,\chi_n)$ no la tienen en general pues hay una infinidad de χ_n que no son primitivos.

Teorema 5.19. *El sumatorio de la definición 5.18 se puede escribir como:*

$$\sum_{q=1}^{\infty}\frac{\mu^2(2q)}{q^w}L(s,\chi_q)\sum_{2\nmid l}l^{-2w}\prod_{p\mid l}(1-\chi_q(p)p^{-s}).$$

donde μ denota la función de Möbius.

Demostración. Sea $n \in \mathbb{Z}^+$, se puede descomponer como $n = ql^2$ donde q es libre de cuadrados. Se tiene que $2 \nmid n$ si y sólo si $2 \nmid q, 2 \nmid l$. En ese caso $\mu^2(2q) = 1$, en los demás casos se anula. Por tanto:

$$\sum_{\substack{n=1 \\ 2\nmid n}}^{\infty} \frac{1}{n^w} = \sum_{q=1}^{\infty} \frac{\mu^2(2q)}{q^w} \sum_{2\nmid l} l^{-2w}.$$

Por último, notemos que $\chi_n(m) = \chi_q(m)\left(\frac{l}{m}\right)^2$, es decir, $\chi_n(p) = \chi_q(p)$ si y sólo si $p \nmid l$. En cambio, si $p|l$, $\chi_n(p) = 0$. En definitiva, usando el teorema 4.12, $L(s, \chi_n) = \prod_{p\nmid l}(1 - \chi_q(p)p^{-s})^{-1} = L(s, \chi_q)\prod_{p|l}(1 - \chi_q(p)p^{-s})$ y se tiene el resultado. □

Teorema 5.20. *Si $\Re(s), \Re(w) > 1$, la fórmula del teorema 5.19 es igual a:*

$$(1 - 2^{-2w})\zeta(2w)\sum_{n=1}^{\infty} \frac{\mu^2(2n)}{n^w} \frac{L(s, \chi_n)}{L(s + 2w, \chi_n)}.$$

Demostración. Por el teorema 5.19, basta probar que para cada $n \in \mathbb{N}$: $(1 - 2^{-2w})\zeta(2w)L(s + 2w, \chi_n)^{-1} = \sum_{2\nmid l} l^{-2w}\prod_{p|l}(1-\chi_n(p)p^{-s})$. Sabemos, por los teoremas 1.1 y 4.12, que $(1-2^{-2w})\zeta(2w)L(s+2w, \chi_n)^{-1} = \prod_{p>2}\frac{1-\chi_n(p)p^{-s}p^{-2w}}{1-p^{-2w}}$. Observemos que:

$$\sum_{2\nmid l} l^{-2w}\prod_{p|l}(1 - \chi_n(p)p^{-s}) = \prod_{p>2}(1 + \sum_{k=1}^{\infty}(p^{-2w})^k(1 - \chi_n(p)p^{-s})).$$

Esto es debido a que si consideramos el producto de la derecha hasta un cierto N y se lo restamos a la suma de la izquierda, se cancelan todos los términos l cuya factorización en primos contenga únicamente primos impares menores que N. Nótese que si, por ejemplo, $l = 15$, tomando los términos $k = 1$ de los respectivos sumatorios en $p = 3, 5$ su producto da el término que deseamos para l. Como la suma de la izquierda converge en $\Re(s), \Re(w) > 1$, se tiene lo deseado. Finalmente, el resultado se sigue de que $\frac{1-\chi_n(p)p^{-s}p^{-2w}}{1-p^{-2w}} = \sum_{k=0}^{\infty}(p^{-2w})^k(1-\chi_n(p)p^{-s}p^{-2w}) = 1+\sum_{k=1}^{\infty}(p^{-2w})^k(1-\chi_n(p)p^{-s})$. □

Teorema 5.21. *$L(s, w)$ satisface la siguiente ecuación funcional:*

$$L(s, w) = \sqrt{2}\pi^{s-1}\Gamma(1 - s)\operatorname{sen}\left(\frac{\pi s}{2}\right)L(1 - s, s + w - 1/2).$$

Demostración. Por el teorema 5.20,

$$L(s, w) = (2^{2s+2w-1} - 1)(1 - 2^{-2w})\zeta(2w)\zeta(2s + 2w - 1)\sum_{n=1}^{\infty} \frac{\mu^2(2n)}{n^w} \frac{L(s, \chi_n)}{L(s + 2w, \chi_n)}.$$

Aplicando el teorema 5.16, se tiene que:

$$L(s, w) = K(s, w)\zeta(2w)\zeta(2s + 2w - 1)\pi^{s-1}\Gamma(1 - s)\operatorname{sen}\left(\frac{\pi s}{2}\right)\sum_{n=1}^{\infty} \frac{\mu^2(2n)}{n^{s+w-1/2}} \frac{L(1 - s, \chi_n)}{L(s + 2w, \chi_n)}, \quad (5.8)$$

donde $K(s, w) = (2^{2s+2w-1} - 1)(1 - 2^{-2w})2^{3/2-2s}$. Finalmente, observemos que $K(s, w) = \sqrt{2}(2^{2w} - 1)(1 - 2^{-2s-2w+1})$ y que si hacemos el cambio $s \to 1 - s, w \to s + w - 1/2$, entonces $\zeta(2w), \zeta(2s + 2w - 1), L(s + 2w, \chi_n)$ se transforman en $\zeta(2s + 2w - 1), \zeta(2w)$ y $L(s + 2w, \chi_n)$ respectivamente. Luego (5.8) da lugar a la ecuación funcional del enunciado. □

Capítulo 6

El número de clases

Una de las motivaciones para preocuparse por la función L doble, $L(s,w)$, definida en el capítulo anterior es el tema central de este último capítulo, el número de clases de una forma cuadrática con discriminante fijo. Como veremos, este número está relacionado con el valor en $s=1$ de una función L de un carácter cuadrático. De esta forma, $L(1,w)$ puede servir para estudiar promedios del número de clases. Incluso sin particularizar en $s=1$, considerar las propiedades de promedios de funciones L es un problema natural. Por medio de diferentes herramientas analíticas, la variable w da mucha flexibilidad para controlar dichos promedios.

A lo largo de este capítulo usaremos la siguiente notación para denotar a las formas cuadráticas binarias: $ax^2+bxy+cy^2$, $a,b,c\in\mathbb{Z}$ o $\{a,b,c\}$. Llamaremos discriminante de la forma a $d=b^2-4ac$. Observemos que $d\equiv 0,1 \pmod 4$. Fijado un discriminante d, dos formas con dicho discriminante se dice que están relacionadas si existe una transformación lineal $x=\alpha x'+\beta y', y=\gamma x'+\delta y'$ con coeficientes enteros tales que $\alpha\delta-\beta\gamma=1$, es decir, si existe una matriz en $SL_2(\mathbb{Z})$ que transforma la matriz de una en la matriz de la otra. Las llamamos transformaciones unimodulares. Es fácil ver que si dos formas cuadráticas están relacionadas, entonces necesariamente tienen el mismo discriminante y representan los mismos enteros [4]. Usaremos la notación estándar $\sim$.

Observación 6.1. Si $d<0$ y $a>0$, por el criterio de Sylvester, la forma es definida positiva. Por tanto, si $d<0$ todas las formas son definidas sin más que considerar lo anterior y cambiar a,b,c por $-a,-b,-c$ (la mitad son definidas positivas y la otra mitad definidas negativas). Si $d>0$, las formas son indefinidas, luego serán equivalentes a alguna forma con $a>0$, de la cual podemos elegir un cierto número positivo representado propiamente (es decir, con x,y coprimos). Dicho número será el primer coeficiente de una forma equivalente. Por ello, sin pérdida de generalidad, consideraremos formas con $a>0$ como representantes y definidas positivas si $d<0$.

Observación 6.2. Si una forma $\{a,b,c\}$ verifica que $(a,b,c)=1$, entonces se dice que es primitiva. En caso contrario, se dice imprimitiva. Si $\{a,b,c\}\sim\{a',b',c'\}$ entonces ambas son o bien primitivas

o bien imprimitivas. De aquí en adelante, solo consideraremos las clases de formas primitivas y denotaremos por $h(d)$ al número de dichas clases (definidas positivas si $d < 0$).

Proposición 6.3. *Toda clase tiene una forma para la cual $|b| \leq |a| \leq |c|$. Se le llama representante reducido [7].*

Demostración. Sea a el entero con menor valor absoluto del conjunto no vacío de valores representables por alguna forma de la clase (por tanto, por todas). Sea $\{a', b', c'\}$ una forma en la clase. Existen enteros r, t tales que $a = a'r^2 + b'rt + c't^2$ con $(r, t) = 1$, de lo contrario, $a/(r, t)^2$ es representable y tiene menor valor absoluto que a. Por la identidad de Bézout, existen enteros s, u tales que $ru - st = 1$, luego $\{a', b', c'\}$ se transforma en $\{a, b_0, c_0\}$ vía $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$. Ahora, la transformación $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ convierte $\{a, b_0, c_0\}$ en $\{a, b, c\}$ con $b = 2ah + b_0$. Por tanto, elegimos h de manera que $|b| \leq |a|$. Como c es representable por $\{a, b, c\}$ y esta forma está en la misma clase que $\{a', b', c'\}$, se deduce de la definición que $|a| \leq |c|$. □

Corolario 6.4. *Fijado un discriminante d, $h(d)$ es finito [9].*

Demostración. Si $d > 0$, se sigue que $|ac| \geq b^2 = d + 4ac > 4ac$. Luego $ac < 0$ y $4a^2 \leq 4|ac| = -4ac = d - b^2 \leq d$. Así, $|b| \leq |a| \leq \frac{\sqrt{d}}{2}$. Por tanto, a y b solo tienen un conjunto finito de valores que pueden tomar y, por consiguiente, lo mismo ocurre para c. Sea ahora $d < 0$, por la observación 6.1, podemos suponer $a, c > 0$. Entonces $|b| \leq a \leq c, 4a^2 \leq 4ac = -d + b^2 \leq |d| + a^2$ y $|b| \leq a \leq \frac{\sqrt{|d|}}{3}$ y se tiene lo mismo que antes. □

Observación 6.5. Siempre hay al menos una forma de discriminante d, a saber, la llamada forma principal: $\begin{cases} x^2 - \frac{1}{4}dy^2, \text{ si } d \equiv 0 \pmod 4 \\ x^2 + xy - \frac{1}{4}(d-1)y^2, \text{ si } d \equiv 1 \pmod 4. \end{cases}$ Luego $h(d)$ es un entero positivo.

Observación 6.6. En la demostración de la relación entre $h(d)$ y $L(s, \chi)$ interviene un factor que depende del número de automorfismos de las formas con discriminante d. Esto es, el número de transformaciones unimodulares que convierten una en otra. Siempre hay dos triviales: $x = x', y = y'$ y $x = -x', y = -y'$. Si $d < 0$, en general, no hay más, pero hay dos excepciones: $d = -3, -4$. En ambos casos, como veremos, $h(d) = 1$. Si $d = -3$, la forma principal es $x^2 + xy + y^2$ y se tienen los automorfismos adicionales: $x = -y', y = x' + y'$ y $x = x' + y', y = -x'$ y sus negativos. Si $d = -4$, la forma principal es $x^2 + y^2$ y se tiene el automorfismo adicional $x = y', y = -x'$ y su negativo [13].

Definición 6.7. Gracias a la observación 6.6, si $d < 0$, se define $w = \begin{cases} 2 \text{ si } d < -4 \\ 4 \text{ si } d = -4 \\ 6 \text{ si } d = -3. \end{cases}$ Este número también se puede interpretar como el número de raíces de la unidad en el cuerpo cuadrático $\mathbb{Q}(\sqrt{d})$.

Observación 6.8. Si $d > 0$ entonces cada forma tiene infinitos automorfismos y estos están determinados por las soluciones de la ecuación de Pell (tiene infinitas soluciones): $t^2 - du^2 = 4$. Para

la forma con coeficientes a, b, c, los automorfismos vienen dados por: $\begin{cases}\alpha = \frac{1}{2}(t - bu),\ \beta = -cu,\\ \gamma = au,\ \delta = \frac{1}{2}(t + bu).\end{cases}$ Los automorfismos triviales corresponden a las soluciones triviales $t = \pm 2, u = 0$. Que todos ellos son automorfismos es fácil de ver factorizando: $ax^2 + bxy + cy^2 = a(x - \theta y)(x + \theta' y)$, donde $\theta = \frac{-b+\sqrt{d}}{2a}, \theta' = \frac{-b-\sqrt{d}}{2a}$. Por tanto, $x - \theta y = \frac{1}{2}(t - u\sqrt{d})(x' - \theta y'), x - \theta' y = \frac{1}{2}(t + u\sqrt{d})(x' - \theta' y')$. Así, $ax^2 + bxy + cy^2 = a\frac{1}{4}(t^2 - du^2)(x' - \theta y')(x' - \theta' y') = a(x')^2 + bx'y' + c(y')^2$.

Ahora, nos preguntamos sobre el número total de representaciones de un entero positivo n por un conjunto de representantes de las clases de formas de discriminante dado d. Esta cuestión fue respondida en la teoría clásica de formas cuadráticas, desarrollada por Lagrange y Gauss. Si $d < 0$, el número de representaciones de n por cualquier forma es finito, pues lo son los automorfismos. Denotamos por $R(n)$ a dicho número. Si $d > 0$, hay infinitas representaciones de n para cada forma, por haber infinitos automorfismos. En este caso, si x, y y X, Y son dos representaciones del mismo entero que están relacionadas por un automorfismo, entonces $\frac{x-\theta' y}{x-\theta y} = \frac{\frac{1}{2}(t+\sqrt{du})}{\frac{1}{2}(t-\sqrt{du})}\frac{X-\theta' Y}{X-\theta Y}$. Definimos $\varepsilon = \frac{1}{2}(t_0 + \sqrt{d}u_0)$, donde (t_0, u_0) es la solución de la ecuación de Pell con ambos positivos y u_0 el menor posible. A ε se le llama unidad fundamental. Nótese que $\varepsilon > 1$ pues, de lo contrario, se tendría que $4 = t_0^2 - du_0^2 = (t_0 + \sqrt{d}u_0)(t_0 - \sqrt{d}u_0) < 4$, esto será muy importante posteriormente. Siguiendo con lo anterior, se tiene que todas las soluciones de la ecuación de Pell vienen dadas por $\frac{1}{2}(t + \sqrt{d}u) = \pm\varepsilon^m, \frac{1}{2}(t - \sqrt{d}u) = \pm\varepsilon^{-m}$ para cierto entero m. Así, dados X, Y, hay solo una elección de m que asegura que $1 \leq \frac{x-\theta' y}{x-\theta y} < \varepsilon^2$ y, eligiendo el signo de ε, podemos asegurar que $x - \theta y > 0$. Una representación que cumpla estas dos condiciones se llamará primaria. El número de representaciones primarias de un entero n por una forma dada es finito, pues el producto $(x - \theta y)(x - \theta' y) = \frac{n}{a}$ y su cociente está acotado. Para $d > 0$, denotamos por $R(n)$ al número total de representaciones primarias de n por un conjunto de representantes de clases de formas con discriminante d.

Teorema 6.9. *Si $n > 0$ y $(n, d) = 1$, entonces:*

$$R(n) = w \sum_{m|n} \left(\frac{d}{m}\right),$$

donde w viene dado en 6.7 si $d < 0$ y $w = 1$ si $d > 0$.

Esta demostración es larga y necesita un resultado previo sobre cuántas soluciones hay de la ecuación $l^2 \equiv k \pmod{4n}$, por tanto, me remito a la demostración de [7] Th.3.4, Th.4.1.

Teorema 6.10.

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{n=1\\(n,d)=1}}^{N} R(n) = w\frac{\varphi(|d|)}{|d|} \sum_{m=1}^{\infty} \frac{1}{m}\left(\frac{d}{m}\right).$$

Demostración. Por el teorema 6.9:

$$w^{-1} \sum_{\substack{n=1\\(n,d)=1}}^{N} R(n) = \sum_{\substack{mk\leq N\\(mk,d)=1}} \left(\frac{d}{m}\right) = \sum_{m\leq\sqrt{N}} \left(\frac{d}{m}\right) \sum_{\substack{k\leq N/m\\(k,d)=1}} 1 + \sum_{\substack{k<\sqrt{N}\\(k,d)=1}} \sum_{\sqrt{N}<m<N/k} \left(\frac{d}{m}\right).$$

Se tiene que $\sum_{\substack{k\leq N/m\\(k,d)=1}} 1 = \frac{N}{m}\frac{\varphi(|d|)}{|d|}+O(\varphi(|d|))$, luego la primera suma doble es $N\frac{\varphi(|d|)}{|d|}\sum_{m\leq\sqrt{N}}\frac{1}{m}\left(\frac{d}{m}\right)+O(\sqrt{N})$ para un d fijado y N arbitrariamente grande. Como $\left(\frac{d}{m}\right)$ es un carácter no principal módulo $|d|$, la suma de sus valores cuando m varía sobre cualquier conjunto es acotada por el teorema 4.6. Por tanto,

$$w^{-1}\sum_{\substack{n=1\\(n,d)=1}}^{N} R(n) = N\frac{\varphi(|d|)}{|d|}\sum_{m\leq\sqrt{N}}\frac{1}{m}\left(\frac{d}{m}\right)+O(\sqrt{N}).$$

Finalmente, extendemos la suma $\sum_{m\leq\sqrt{N}}\frac{1}{m}\left(\frac{d}{m}\right)$ hasta infinito, lo cual aporta un error de $O(\sqrt{N})$, pues $\sum_{m>\sqrt{N}}\frac{1}{m}\left(\frac{d}{m}\right) = O(N^{-1/2})$. En efecto, dado $M\in\mathbb{N}$ arbitrario, aplicando sumación por partes [3], Lem.1.2.1, Cor.1.2.2, se tiene que $\left|\sum_{\sqrt{N}<m<M}\frac{1}{m}\left(\frac{d}{m}\right)\right| \leq N^{-1/2}\sup_{\sqrt{N}<n<M}|S_n|$, donde $S_n = \sum_{\sqrt{N}<m\leq n}\left(\frac{d}{m}\right)$. En particular, se concluye el resultado. □

Observación 6.11. Si consideramos el carácter $\chi(m) = \left(\frac{d}{m}\right)$, el símbolo de Kronecker, entonces $L(1,\chi) = \sum_{m=1}^{\infty}\frac{1}{m}\left(\frac{d}{m}\right)$, luego el teorema 6.10 se reescribe como:

$$\lim_{N\to\infty}\frac{1}{N}\sum_{\substack{n=1\\(n,d)=1}}^{N} R(n) = w\frac{\varphi(|d|)}{|d|}L(1,\chi).$$

El siguiente paso es evaluar el promedio de $R(n)$ dado antes por su definición original. Sea $R(n,f)$ denotando el número de representaciones de n (primarias si $d>0$) por la forma f de discriminante d. Entonces $R(n) = \sum_f R(n,f)$, donde f recorre un conjunto de representantes (con $a>0$). Por definición, el número de términos en la suma es $h(d)$. Queremos calcular $\lim_{N\to\infty}\frac{1}{N}\sum_{\substack{n=1\\(n,d)=1}}^{N} R(n,f)$.

Teorema 6.12. *Sean $d<0$ y $f=\{a,b,c\}$, se tiene que:*

$$\lim_{N\to\infty}\frac{1}{N}\sum_{\substack{n=1\\(n,d)=1}}^{N} R(n,f) = \frac{\varphi(|d|)}{|d|}\frac{2\pi}{|d|^{1/2}}.$$

Demostración. La suma $\sum_{\substack{n=1\\(n,d)=1}}^{N} R(n,f)$ es el número de pares (x,y) que satisfacen que $0<ax^2+bxy+cy^2\leq N, (ax^2+bxy+cy^2,d)=1$. La segunda condición limita x,y a ciertos pares de clases mód $|d|$. El número de estos pares es $|d|\varphi(|d|)$ ([9]). Por tanto, basta considerar el número de pares de enteros (x,y) tales que $0<ax^2+bxy+cy^2\leq N, x\equiv x_0, y\equiv y_0 \pmod{|d|}$, con (x_0,y_0) uno de los pares mencionados antes. La primera condición expresa que el punto (x,y) está en una elipse con centro el origen. El área de la elipse es $\frac{2\pi}{\sqrt{4ac-b^2}}N = \frac{2\pi}{|d|^{1/2}}N$. Dividiendo el plano en cuadrados de lado $|d|$, se prueba que el número de puntos en dicha elipse es asintótico a $\frac{1}{|d|^2}\frac{2\pi}{|d|^{1/2}}N$ cuando $N\to\infty$, [7] Th.8.1. Finalmente, multiplicando esta cantidad por $|d|\varphi(|d|)$ para admitir las distintas posibilidades de (x_0,y_0) que hay, se tiene el resultado. □

Teorema 6.13. *Sean $d>0$ y $f=\{a,b,c\}$, se tiene que:*

$$\lim_{N\to\infty}\frac{1}{N}\sum_{\substack{n=1\\(n,d)=1}}^{N} R(n,f) = \frac{\varphi(d)}{d}\frac{\log\varepsilon}{d^{1/2}},$$

donde ε es la unidad fundamental.

Demostración. Ahora, $\sum_{\substack{n=1\\(n,d)=1}}^{N} R(n,f)$, representa el número de pares de enteros (x,y) que verifican: $ax^2+bxy+cy^2 \leq N, x-\theta y > 0, 1 \leq \frac{x-\theta' y}{x-\theta y} < \varepsilon^2$ y $x \equiv x_0, y \equiv y_0 \pmod{d}$ como en el teorema 6.12. Las tres primeras condiciones representan un trozo de hipérbola acotado por dos semirrectas que pasan por el origen. Calculemos el área de este sector. Haciendo el cambio de variable x, y por $\xi = x-\theta y, \eta = x-\theta' y$, se tiene que el determinante jacobiano es $\theta - \theta' = \frac{\sqrt{d}}{a}$. En estas coordenadas, las 3 condiciones anteriores se reescriben como: $\xi\eta \leq N/a, \xi > 0, \xi \leq \eta < \varepsilon^2\xi$, que son equivalentes a: $0 < \xi \leq (N/a)^{\frac{1}{2}}, \xi \leq \eta < \text{mín}(\varepsilon^2\xi, N/a\xi)$. Por tanto, el área es $\int_0^{\xi_1}(\varepsilon^2\xi - \xi)d\xi + \int_{\xi_1}^{(N/a)^{1/2}}(\frac{N}{a\xi} - \xi)d\xi$, donde $\xi_1 = \varepsilon^{-1}(N/a)^{\frac{1}{2}}$. Esto es debido a que si $0 < \xi < \xi_1$, entonces $\varepsilon^2\xi \leq \varepsilon(N/a)^{1/2} < (N/a)^{1/2} \leq N/a\xi$, luego $\xi < \eta < \varepsilon^2\xi$. Por otra parte, si $\xi_1 < \xi \leq (N/a)^{1/2}$, entonces $\varepsilon\xi \geq (N/a)^{1/2}$, luego $\varepsilon^2\xi \geq \varepsilon(N/a)^{1/2} \geq (N/a\xi)$ y $\xi \leq \eta \leq (N/a\xi)$. La integral queda:

$$(\varepsilon^2-1)\frac{1}{2}\xi_1^2 + (N/2a)\log(N/a) - (N/a)\log\xi_1 - \frac{1}{2}(N/a) + \frac{1}{2}\xi_1^2,$$

que es simplemente $(N/a)\log\varepsilon$. Esta cantidad debe ser dividida entre el jacobiano del cambio, $\sqrt{d}a^{-1}$, después debemos dividir entre d^2 y multiplicar por $d\varphi(d)$ por las distintas elecciones de (x_0, y_0) posibles. Todo ello, nos da el resultado. □

Lo anterior nos lleva al resultado más importante de este capítulo:

Teorema 6.14. ***Fórmula del número de clases (Dirichlet, 1839)*** *Sean $\chi(m) = \left(\frac{d}{m}\right)$ y w como en la definición 6.7. Entonces:*

$$h(d) = \begin{cases} w\frac{|d|^{1/2}}{2\pi}L(1,\chi) \text{ si } d < 0, \\ \frac{d^{1/2}}{\log\varepsilon}L(1,\chi) \text{ si } d > 0. \end{cases}$$

Demostración. Notemos que la fórmula asintótica para $\frac{1}{N}\sum_{\substack{n=1\\(n,d)=1}}^{N} R(n,f)$ no depende de f tanto si $d > 0$ como si $d < 0$. Además, $R(n) = \sum_f R(n,f)$. Por ello, si $d < 0$, aplicando el teorema 6.12 y la observación 6.11 se obtiene que $w\frac{\varphi(|d|)}{|d|}L(1,\chi) = \frac{\varphi(|d|)}{|d|}\frac{2\pi}{|d|^{1/2}}h(d)$. Para $d > 0$, se obtiene que $w\frac{\varphi(|d|)}{|d|}L(1,\chi) = \frac{\varphi(d)}{d}\frac{\log\varepsilon}{d^{1/2}}h(d)$, usando el teorema 6.13 y la observación 6.11. □

Observación 6.15. Gracias al teorema 6.14, todo lo que se avance en el conocimiento de $L(1,\chi)$ se verá reflejado en $h(d)$ y viceversa. Por ejemplo, con la fórmula del número de clases, es claro que $L(1,\chi) > 0$ para todo carácter cuadrático/real. Recuérdese que su no anulación era esencial en el teorema de Dirichlet sobre progresiones aritméticas.

Observación 6.16. Los números d para los cuales $h(d) = 1$ son:

$$d = -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163.$$

Hay un teorema con una historia azarosa que prueba que no hay ningún caso más, pero es difícil de probar [4]. Sin embargo, recordemos que nos hemos restringido únicamente a las clases de formas primitivas. Si de los números anteriores consideramos solo los llamados discriminantes fundamentales, que son aquellos para los cuales todas las formas son primitivas, entonces verifican que solo hay una única forma, salvo transformación unimodular, con discriminante d. Por ejemplo, $d = -12$ no verifica esto pues $x^2 + 3y^2$ no puede transformarse en $2x^2 + 2xy + 2y^2$ pero $h(-12) = 1$ porque todas las formas primitivas están en la clase de $x^2 + 3y^2$. Los números que sí cumplen lo anterior son: [6]

$$d = -3, -4, -7, -8, -11, -19, -43, -67, -163.$$

Con este resultado en mente, podemos probar dos resultados clásicos cuyas demostraciones se simplifican enormemente con lo obtenido en este capítulo.

Corolario 6.17. ***Fermat:****[5] Sea p primo impar. Entonces $x^2 + y^2 = p$, tiene solución en $x, y \in \mathbb{Z}$ si y sólo si $p \equiv 1 \pmod 4$.*

Demostración. La implicación de izquierda a derecha es trivial. Para ver la otra implicación, observemos que $x^2 + y^2$ es la forma principal de $d = -4$. Como $p \equiv 1 \pmod 4$, la ley de reciprocidad cuadrática nos dice que existe un entero m tal que $p|m^2+1$. Consideremos ahora la forma cuadrática $Q(x, y) = px^2 + 2mxy + \frac{m^2+1}{p}y^2$. Esta forma verifica que $Q(1, 0) = p$ y tiene discriminante -4, luego como $h(-4) = 1$, se deduce que es equivalente a $x^2 + y^2$ y, por tanto, p es representable por dicha forma. □

Corolario 6.18. *[5] Sea $p \neq 2, 5$ primo. Entonces $x^2 + 5y^2 = p$ tiene solución en $x, y \in \mathbb{Z}$ si y sólo si $p \equiv 1, 9 \pmod{20}$.*

Demostración. Tomando representantes reducidos, tenemos que el conjunto de formas de discriminante -20 está compuesto por las clases de x^2+5y^2 y $2x^2+2xy+3y^2$ ([4]). Un cálculo sencillo muestra que $\{x^2 + 5y^2, x, y \in \mathbb{Z}/20\mathbb{Z}\} \cap (\mathbb{Z}/20\mathbb{Z})^* = \{1, 9\}$ y $\{2x^2 + 2xy + 3y^2, x, y \in \mathbb{Z}/20\mathbb{Z}\} \cap (\mathbb{Z}/20\mathbb{Z})^* = \{3, 7\}$. Por tanto, si $p \neq 2, 5$ es primo y es representable por x^2+5y^2 no puede serlo por $2x^2+2xy+3y^2$ pues representan distintas clases de congruencias. La fórmula de 6.9 muestra que con $d = -20$, $R(p) = 4$ para $p \equiv 1, 3, 7, 9 \pmod{20}$ y se tiene el resultado. □

Alentados por este último corolario, decimos que dos formas cuadráticas de discriminante d están en el mismo género si representan los mismos valores de $(\mathbb{Z}/|d|\mathbb{Z})^*$. Si dos formas están en la misma clase, representan los mismos valores, luego están en el mismo género. Por tanto, esta es una relación de equivalencia más débil. Siempre que cada género contenga una sola clase, podemos separar las representaciones en clases de congruencia y decidir la representabilidad de los primos. Para $4|d$, desde los tiempos de Euler se sabe que esto ocurre para 65 discriminantes, los llamados números idóneos/convenientes. Se ha probado que a lo sumo, hay otro ejemplo más [4].

Bibliografía

[1] Tom M. Apostol. *Mathematical Analysis.* Pearson, 1957.

[2] Tom M. Apostol. *Introduction to Analytic Number Theory.* Springer-Verlag, 1976.

[3] Fernando Chamizo. *Temas de Teoría de Números.* Universidad Autónoma de Madrid, 2006.

[4] Fernando Chamizo. *Ocho Lecciones de Teoría de Números.* Universidad Autónoma de Madrid, 2011.

[5] David A. Cox. *Primes of the Form $x^2 + ny^2$.* John Wiley and Sons, Inc, 1989.

[6] Harold Davenport. *Multiplicative Number Theory.* Springer-Verlag, 1980.

[7] L.K Hua. *Introduction to Number Theory.* Springer-Verlag, 1982.

[8] Henryk Iwaniec and Emmanuel Kowalski. *Analytic Number Theory.* American Mathematical Society, 2004.

[9] Edmund Landau. *Elementary Number Theory.* Chelsea Publishing Company, 1966.

[10] Hugh Montgomery and Robert C. Vaughan. *Multiplicative Number Theory I: Classical Theory.* Cambridge University Press, 2006.

[11] Donald J. Newman. *Analytic Number Theory.* Springer-Verlag, 1973.

[12] Walter Rudin. *Real and Complex Analysis.* McGraw-Hill Education, 1966.

[13] Jean-Pierre Serre. *A Course in Arithmetic.* Springer-Verlag, 1973.

[14] Edward C. Titchmarsh. *The Theory of the Riemann Zeta Function.* Oxford University Press, 1987.