Universidad Nacional Autónoma de México
Posgrado Conjunto en Ciencias Matemáticas
UMSNH-UNAM

El Problema Ternario de Goldbach

T E S I S

que para optar por el grado de

Maestro en Ciencias Matemáticas

presenta

Manuel Alejandro Espinosa García
esgama93@gmail.com

Asesor:
Dr. Moubariz Garaev Centro de Ciencias Matemáticas
garaev@matmor.unam.mx

Morelia, Michoacán, México
Enero 2019

Este trabajo se realizó gracias al apoyo del Programa de Becas Nacionales de CONACyT, el cual me apoyó para realizar mis estudios de maestría.

Índice general

Introducción

El Problema de Goldbach surge en el año de 1742, en una carta escrita por Christian Goldbach para Leonard Euler. En la carta, Goldbach conjeturaba que:

Todo número entero par mayor que 2 se puede escribir como la suma de dos números primos.

Este es uno de los problemas abiertos más famosos que existen en la teoría de los números y es conocido como la Conjetura de Goldbach. De manera posterior, durante el mismo año, Goldbach hizo otra conjetura, la cual era una versión más débil a la anterior. Ésta segunda conjetura decía que:

Todo número impar mayor que 5 se puede escribir como la suma de tres números primos.

Este segundo problema, conocido como el Problema débil de Goldbach o el Problema ternario de Goldbach, es el problema central de esta tesis, y fue un problema que tuvo avances importantes muy importantes a lo largo de la historia, hasta el año 2013 que fue totalmente demostrado.

El primer avance fuerte que se hizo al Problema débil de Goldbach fue a manos de G. H. Hardy y J. E. Littlewood [8], en 1923. Ellos demostraron, asumiendo la veracidad de la hipótesis de Riemann, que el Problema Débil de Goldbach se cumplía para cualquier entero impar suficientemente grande.

En 1930, Šnirel'man [9] demostró la existencia de un entero k tal que cualquier entero mayor que 1 se podía escribir como la suma de a lo más k números primos. Por este camino, el último avance que se realizó fue el 2012 en un trabajo de Terence Tao [10], el cual dice que cualquier entero impar mayor que 1 se puede escribir como la suma de a lo más 5 números primos.

En 1937, I. M. Vinogradov [11] demostró que el Problema débil de Goldbach se cumplía para cualquier entero impar suficientemente grande, sin depender de la hipótesis de Riemann. La parte fundamental en esta demostración es su teorema que establece la estimación

$$\sum_{n_1+n_2+n_3=N} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3) = \frac{N^2}{2}\prod_{p|N}\left(1-\frac{1}{(p-1)^2}\right)\prod_{p\nmid N}\left(1+\frac{1}{(p-1)^3}\right)+O\left(\frac{N^2}{(\log N)^A}\right)$$

para cualquier $A > 0$. Su demostración empleaba el Teorema de Siegel-Walfisz [12], el cual establece una estimación para el número de primos acotados por x en la progresión aritmética $a + nq$, dada por

$$\pi(x; q, a) = \frac{Li(x)}{\varphi(q)} + O(xe^{-c\sqrt{\log x}}),$$

donde $(a, q) = 1$, $q \leqslant (\log x)^M$ y $c = c_M$. Con esto, Vinogradov estableció que existe una constante absoluta C tal que cualquier entero impar mayor que C se puede escribir como la suma de tres números primos, sin embargo, no especificó el valor de dicha constante. El primero en establecer un valor explícito para la constante de Vinogradov fue K. Borozdin [13] en 1956, quien determinó que $C = 3^{3^{15}}$ era una cota válida, es decir, cualquier entero impar mayor que $3^{3^{15}}$ se puede escribir como suma de tres números primos. Con el paso del tiempo, esta constante se fue mejorando, por mencionar algún ejemplo, en el 2002, M. C. Liu y T. Wang [14] demostraron que e^{3100} era una cota válida.

En 1997 Deshouiller, Effinger, Te Riele y Zinoviev [15] demostraron que, asumiendo nuevamente la veracidad de la hipótesis de Riemann, cualquier entero impar mayor que 5 se podía escribir como suma de tres números primos.

Finalmente, H. Helfgott en el año 2013, con una serie de artículos, afirmó que cualquier entero impar mayor que 5 se podía escribir como suma de tres números primos. Con tres artículos, subidos a arXiv ([16],[17],[18]), Helfgott afirma que cualquier entero impar mayor que 10^{27} se puede escribir como suma de tres números primos. En un cuarto artículo, H. Helfgott y D. Platt [19] afirman haber demostrado computacionalmente que cualquier entero impar menor que $8.875 \cdot 10^{30}$ se puede escribir como suma de tres números primos. Aunque la demostración de Helfgott es aceptada por la comunidad matemática, hasta el momento no ha sido publicada en ninguna revista de arbitraje.

La meta de esta tesis es concluir el resultado que Vinogradov presentó en 1937 acerca del Problema ternario de Goldbach, y en el proceso serán demostrados muchos otros resultados importantes de la Teoría de Números, relacionados con la función ζ de Riemann y las funciones L de Dirichlet.

En el Capítulo 1 se presentarán algunos resultados clásicos de la Teoría de los Números, que serán necesarios en demostraciones posteriores, como la Fórmula de Sumación de Abel y el Teorema de Aproximación de Dirichlet. Además se dará una muy breve introducción a métodos trigonométricos que son muy usados en la Teoría de los Números y que serán el punto de partida para la demostración de Vinogradov del Problema Ternario de Goldbach. Finalmente, se dedica una amplia sección a resultados relacionados con Caracteres de Dirichlet.

En el Capítulo 2 se estudiarán las funciones ζ de Riemann y las funciones L de Dirichlet. Los resultados que se presentarán son aportaciones de Riemann, Dirichlet, von Mangoldt, Hadamard, Vallée Poussin y Hurwitz. Así mismo, se presenta la Identidad de Vaughan de 1977, la cual es útil para hacer buenas estimaciones para sumas de la forma $\sum_{n \leqslant N} f(n)\Lambda(n)$. En este capítulo también se demuestra la Fórmula del Número de Clase de Dirichlet, conjeturada en 1932 por Jacobi, y demostrada en 1939. Aunque estos últimos dos resultados no fueron usados en la demostración original de Vinogradov al Problema Ternario de Goldbach, serán aplicados en la demostración que se presenta en esta tesis.

En el Capítulo 3 se estudian los ceros no triviales de la función ζ de Riemann y de las funciones L de Dirichlet, así como regiones donde estas funciones son libres de ceros. Los resultados relacionados con los ceros de la función ζ de Riemann son aportaciones de Vallée Poussin y

Hadamard, pero la demostración que se expondrá en esta tesis es de Mertens. Para los ceros de las funciones L de Dirichlet, se sigue la misma línea de razonamiento que con la función ζ de Riemann, pero se añaden conclusiones importantes de Gronwall, Titchmarsh, Landau y Page. Este capítulo también contiene trabajo de von Mangoldt acerca del número de ceros no triviales con parte imaginaria acotada. Finalmente, se presentan algunas estimaciones para las funciones $\Psi(x)$ y $\Psi(x, \chi)$, dadas por von Mangoldt, y los Teoremas de Siegel y Siegel-Walfisz.

En el Capítulo 4, se demuestra el Teorema de Vinogradov para el Problema ternario de Goldbach, partiendo de la identidad trivial

$$J(N) = \int_0^1 \left(\sum_{p_i \text{ primo}} e^{2\pi i\alpha(p_1+p_2+p_3-N)} \right) d\alpha,$$

donde $J(N)$ representa la cantidad de maneras de escribir a N como suma de tres números primos.

Capítulo 1

Preliminares

1.1. Sumas trigonométricas

Una suma trigonométrica es una suma de la forma

$$\sum_{x=1}^{M} e^{2\pi i F(x)}.$$

Un resultado que ha sido primordial en el desarrollo de la teoría de los números es la aplicación de sumas trigonométricas en congruencias aditivas. El punto de partida es la identidad

$$\frac{1}{q}\sum_{n=0}^{q-1} e^{2\pi i n x/q} = \begin{cases} 1 & \text{si } x \equiv 0 (\text{mod } q), \\ 0 & \text{si } x \not\equiv 0 (\text{mod } q), \end{cases} \tag{1.1}$$

la cual se cumple para cualquier $q \in \mathbb{N}$.

Existe una identidad muy similar a la ecuación (1.1), que en vez de caracterizar una congruencia, caracteriza una igualdad. Dicha identidad es

$$\int_0^1 e^{2\pi i \alpha x} dx = \begin{cases} 1 & \text{si } \alpha = 0, \\ 0 & \text{si } \alpha \in \mathbb{Z}\backslash\{0\}. \end{cases} \tag{1.2}$$

Teorema 1.1. *Para cualquier $n \in \mathbb{N}$ y a entero primo relativo a n se cumple la igualdad*

$$\sum_{\substack{l=1 \\ (l,n)=1}}^{n} e^{2\pi i \frac{al}{n}} = \mu(n).$$

Demostración. Veamos primero que es cierto cuando n es potencia de primo. Si n es primo, se sigue de la ecuación (1.1). Para $n = p^\alpha$ con p primo y $\alpha \geqslant 2$ se sigue de que

$$\sum_{\substack{l=1 \\ (l,p^\alpha)=1}}^{p^\alpha} e^{2\pi i \frac{al}{p^\alpha}} = \sum_{\substack{l=1 \\ (l,p^\alpha)=1}}^{p^{\alpha-1}} e^{2\pi i \frac{al}{p^\alpha}} \sum_{k=0}^{p-1} e^{2\pi i \frac{akp^{\alpha-1}}{p^\alpha}} = 0.$$

La demostración se sigue de lo anterior, ya que ambos lados de la ecuación a demostrar son multiplicativos. ■

1.2. Teorema de aproximación de Dirichlet

Teorema 1.2 (Teorema de aproximación de Dirichlet)**.** *Sea $\alpha \in \mathbb{R}$ y $1 \leqslant Q$, entonces existen a, q enteros, con $1 \leqslant q \leqslant Q$ y $(a, q) = 1$, tales que*

$$\left|\alpha - \frac{a}{q}\right| \leqslant \frac{1}{qQ}.$$

Demostración. Para cada $0 \leqslant j < Q$, considérese el intervalo

$$I_j = \left[\frac{j}{\lfloor Q\rfloor + 1}, \frac{j+1}{\lfloor Q\rfloor + 1}\right).$$

Consideremos los números $\{\alpha\}, \{2\alpha\}, \ldots, \{\lfloor Q\rfloor\alpha\}$ y los siguientes tres casos:

Caso 1: Si algún $\{q\alpha\}$ pertenece a I_0, se tendría que $0 \leqslant \alpha q - \lfloor \alpha q\rfloor < \frac{1}{\lfloor Q\rfloor+1}$, de donde

$$\left|\alpha - \frac{\lfloor \alpha q\rfloor}{q}\right| < \frac{1}{q(\lfloor Q\rfloor + 1)} < \frac{1}{qQ}.$$

Caso 2: Si algún $\{q\alpha\}$ pertenece a $I_{\lfloor Q\rfloor}$, se tendría que $-\frac{1}{\lfloor Q\rfloor+1} \leqslant \alpha q - \lfloor \alpha q\rfloor - 1 < 0$, de donde

$$\left|\alpha - \frac{\lfloor \alpha q\rfloor + 1}{q}\right| < \frac{1}{q(\lfloor Q\rfloor + 1)} < \frac{1}{qQ}.$$

Caso 3: Si no sucede nunguna de las anteriores, por principio de casillas se tiene que existen $1 \leqslant q_1 < q_2 \leqslant Q$ tales que $\{\alpha q_1\}, \{\alpha q_2\} \in I_j$, para algún $1 \leqslant j \leqslant Q - 1$, entonces $\frac{j}{\lfloor Q\rfloor+1} \leqslant \alpha q_i - \lfloor \alpha q_i\rfloor < \frac{j+1}{\lfloor Q\rfloor+1}$. Entonces $|\alpha q_2 - \alpha q_1 - \lfloor \alpha q_2\rfloor + \lfloor \alpha q_1\rfloor| \leqslant \frac{1}{\lfloor Q\rfloor+1}$, de donde

$$\left|\alpha - \frac{\lfloor \alpha q_2\rfloor - \lfloor \alpha q_1\rfloor}{q_2 - q_1}\right| < \frac{1}{(\lfloor Q\rfloor + 1)(q_2 - q_1)} < \frac{1}{q_2 - q_1}.$$

■

1.3. Fórmula de Sumación de Abel

Teorema 1.3. *Sean $c_n \in \mathbb{C}$, $f(x) \in C^1[a, b]$ y $\mathcal{C}(x) = \sum_{a<n\leqslant b} c_n$. Entonces, se da la igualdad*

$$\sum_{a<n\leqslant b} c_n f(n) = -\int_a^b \mathcal{C}(u) f'(u) du + \mathcal{C}(b) f(b).$$

Demostración. Veamos primero que

$$-\int_a^b \mathcal{C}(u)f'(u)du = -\int_a^{\lceil a\rceil} \mathcal{C}(a)f'(u)du - \sum_{t=\lceil a\rceil}^{\lfloor b\rfloor -1}\int_t^{t+1} \mathcal{C}(t)f'(u)du - \int_{\lfloor b\rfloor}^b \mathcal{C}(\lfloor b\rfloor)f'(u)du$$

Como $\mathcal{C}(a) = 0$, se tiene que

$$\begin{aligned}-\int_a^b \mathcal{C}(u)f'(u)du &= -\sum_{t=\lceil a\rceil}^{\lfloor b\rfloor -1} \mathcal{C}(t)\big(f(t+1)-f(t)\big) - \mathcal{C}(\lfloor b\rfloor)\big(f(b)-f(\lfloor b\rfloor)\big)\\ &= \sum_{t=\lceil a\rceil+1}^{\lfloor b\rfloor} f(t)\big(\mathcal{C}(t)-\mathcal{C}(t-1)\big) + \mathcal{C}(\lceil a\rceil)f(\lceil a\rceil) - \mathcal{C}(b)f(b)\\ &= \sum_{t=\lceil a\rceil+1}^{\lfloor b\rfloor} c_t f(t) + \mathcal{C}(\lceil a\rceil)f(\lceil a\rceil) - \mathcal{C}(b)f(b) = \sum_{t=a}^{b} c_t f(t) - \mathcal{C}(b)f(b).\end{aligned}$$

■

1.4. Caracteres de Dirichlet

Definición 1.4. Sea $q > 1$ entero. Un *caracter de Dirichlet módulo* q es una función $\chi : \mathbb{Z} \to \mathbb{C}$ tal que:

- χ es q-periódica,
- $\chi(n) = 0 \Leftrightarrow (n, q) > 1$,
- χ es completamente multiplicativa.

Proposición 1.5. *Todo χ caracter de Dirichlet módulo q cumple las siguientes propiedades:*

(*i*) $\chi(1) = 1$,

(*ii*) *Si h es el orden de a módulo q, entonces* $\chi(a)^h = 1$,

(*iii*) *En particular, $\chi(a)$ es una $\varphi(q)$-ésima raíz de la unidad para toda $a \in \mathbb{Z}$ con* $(a, q) = 1$.

Demostración. (*i*)] Se tiene que $\chi(1) = \chi(1 \cdot 1) = \chi(1)^2$, y como $\chi(1) \neq 0$, entonces $\chi(1) = 1$.
(*ii*)] Sea h el orden de a módulo q, entonces $\chi(a)^h = \chi(a^h) = \chi(1) = 1$.
(*iii*)] Se sigue del inciso anterior y de que, por el Teorema de Euler, el orden de a módulo q divide a $\varphi(q)$. ■

Definición 1.6. Sea $q = p^\alpha$ para algún $p > 2$ primo, sea g una raíz primitiva módulo q y sea $X = \{n \in \mathbb{Z} : (n, q) = 1\}$. Una *función de índice* módulo q relativa a g es una función $\nu : X \to \{0, 1, 2, \ldots, \varphi(q) - 1\}$ tal que $g^{\nu(n)} \equiv n(\text{mod } q)$ para cualquier $n \in X$.

Observación 1.7. Si $(ab, q) = 1$, entonces $\nu(ab) \equiv \nu(a) + \nu(b)(\text{mod } \varphi(q))$, puesto que $g^{\nu(ab)} \equiv ab \equiv g^{\nu(a)} \cdot g^{\nu(b)}(\text{mod } q)$.

Teorema 1.8. *Sea $q = p^\alpha$ con p un número primo, y $\alpha \in \mathbb{N}$. Existen exáctamente $\varphi(q)$ caracteres de Dirichlet módulo q.*

Demostración. Se analizará primero el caso $p \neq 2$. Sea g una raíz primitiva módulo q, y ν la función de índice módulo q relativa a g. Para cada $k \in \{0, 1, 2, \ldots, \varphi(q) - 1\}$ se define la función

$$\chi_k(n) = \begin{cases} e^{\frac{2\pi i k \nu(n)}{\varphi(q)}} & \text{si } (n,q) = 1, \\ 0 & \text{si } (n,q) > 1. \end{cases}$$

Veamos que estas funciones son un caracter para cualquier $k \in \{0, 1, 2, \ldots, \varphi(q) - 1\}$. χ_k es una función q-periódica, puesto que $(n,q) = (n+q,q) = 1$ implica que $\nu(n) \equiv \nu(q+n) (\mathrm{mod}\ \varphi(q))$; también cumple que $\chi_k(n) = 0 \Leftrightarrow (n,q) > 1$; y es completamente multiplicativa ya que, si $p \nmid ab$, entonces $\chi(ab) = e^{\frac{2\pi i \nu(ab)}{\varphi(q)}} = e^{\frac{2\pi i \nu(a)+\nu(b)}{\varphi(q)}} = e^{\frac{2\pi i \nu(a)}{\varphi(q)}} \cdot e^{\frac{2\pi i \nu(b)}{\varphi(q)}} = \chi(a) \cdot \chi(b)$ y, si $p \mid ab$, entonces $\chi(ab) = 0 \Leftrightarrow p|ab \Leftrightarrow p|a$ o $p|b \Leftrightarrow \chi(a) \cdot \chi(b) = 0$. Estos $\varphi(q)$ caracteres son distintos entre sí, ya que $\chi_k = \chi_l$ implicaría que $\chi_k(g) = \chi_l(g)$, es decir, $e^{\frac{2\pi i k}{\varphi(q)}} = e^{\frac{2\pi i l}{\varphi(q)}}$ ya que $\nu(g) = 1$, de donde $k = l$. No existen más caracteres, ya que si χ es caracter, $\chi(g)$ es raíz $\varphi(q)-$ésima de la unidad, y por la multipplicidad de χ se extiende de manera única a uno de los caracteres ya mencionados.

Para el caso $q = 2$ sólo existe el caracter trivial; y para $q = 4$ está el caracter trivial y el caracter que cumple $\chi(4t + 3) = -1$ para cualquier k entero.

Analicemos ahora el caso $q = 2^\alpha$ con $\alpha \geqslant 3$. El orden de 5 módulo 2^α es $2^{\alpha-2}$, ya que:
• su orden divide a $2^{\alpha-2}$ porque las potencias de 5 módulo 2^α son un subgrupo del grupo multiplicativo formado por los elementos de la forma $4a + 1$ módulo 2^α;
• si fuera menor $2^{\alpha-3}$, en particular $2^\alpha | 5^{2^{\alpha-3}} - 1 = (5-1)(5+1)(5^2+1)\cdots(5^{2^{\alpha-4}}+1)$, lo cual es falso.

De lo anterior se deduce que -1 y 5 generan a $\mathbb{Z}^*_{2^\alpha}$. Se toman las funciones $v_0 : \mathbb{Z}\backslash 2\mathbb{Z} \to \mathbb{Z}_2$ y $v_1 : \mathbb{Z}\backslash 2\mathbb{Z} \to \mathbb{Z}_{2^{\alpha-2}}$ tales que $m \equiv (-1)^{\nu_0(m)}(5)^{\nu_1(m)} (\mathrm{mod}\ 2^\alpha)$. Para cada $(k,l) \in \mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$ se define la función

$$\chi_{k,l}(m) = \begin{cases} e^{2\pi i (\frac{k\nu_0(m)}{2} + \frac{l\nu_1(m)}{2^{\alpha-2}})} & \text{si } 2 \nmid m, \\ 0 & \text{si } 2 \mid 0. \end{cases}$$

De manera análoga al caso $p \neq 2$, se puede ver $\chi_{k.l}$ es multiplicativa, q-periódica y que $\chi_{k,l}(m) = 0 \Leftrightarrow (m,q) > 0$. Cada uno de estos caracteres es distinto, pues $(k,l) \neq (k',l')$ si y sólo si $(\chi_{k,l}(-1), \chi_{k,l}(5)) \neq (\chi_{k',l'}(-1), \chi_{k',l'}(5))$, ya que la definición de $\chi_{k,l}$ se extiende de manera única conociendo $\chi_{k,l}(-1)$ y de $\chi_{k,l}(5)$. De lo anterior también se puede ver que no hay más caracteres, ya que dado un caracter χ, se tiene que $\chi(-1) \in \{1, -1\}$ y $\chi(5)$ es raíz $2^{\alpha-2}$-ésima de la unidad,y se extiende de manera única a uno de los $\varphi(2^\alpha)$ caracteres ya mencionados. ∎

Teorema 1.9. *Para todo $q \in \mathbb{N}$ existen exáctamente $\varphi(q)$ caracteres módulo q.*

Demostración. El caso $q = 1$ es claro. Sea $1 < q = 2^\alpha p_1^{\alpha_1} \cdots p_t^{\alpha_t}$. Sea $\chi(n, p^\gamma)$ un caracter módulo p^γ, entonces la función $\chi(n) := \chi(n, 2^\alpha) \cdot \chi(n, p_1^{\alpha_1}) \cdots \chi(n, p_t^{\alpha_t})$ es un caracter módulo q, ya que:

- es multiplicativa y q-periódica ya que cada $\chi(n, p^\gamma)$ lo es;
- $\chi(n) = 0 \Leftrightarrow \chi(n, p^\gamma) = 0$ para algún p divisor de q, si y sólo si $(n,p) > 1 \Leftrightarrow (n,q) > 1$.

Veamos que son todos distintos y que no hay más caracteres. Para esto, tomemos g_i raíz primitiva módulo $p_i^{\alpha_i}$, y sea n_i solución del sistema de congruencias

$$n_i \equiv \begin{cases} g_i (\text{mod } p_i^{\alpha_i}), \\ 1\,(\text{mod } p_j^{\alpha_j}) & \text{para } j \neq i, \\ 1\,(\text{mod } 2^{\alpha}), \end{cases}$$

y en caso que $\alpha \geqslant 1$, tomamos

$$n_0 = n_0^* = 1 \quad \text{si } \alpha = 1,$$

$$n_0 \equiv \begin{cases} 5(\text{mod } 2^{\alpha}), \\ 1(\text{mod } p_j^{\alpha_j}), \end{cases} \quad \text{y} \quad n_0^* \equiv \begin{cases} -1(\text{mod } 2^{\alpha}), \\ 1(\text{mod } p_j^{\alpha_j}), \end{cases} \qquad \text{si } \alpha \geqslant 2.$$

Tomemos dos de estos caracteres χ y χ'. Si $\chi(\_, p_i^{\alpha_i}) \neq \chi'(\_, p_i^{\alpha_i})$, en particular se tendría que $\chi(n_i) = \chi(n_i, p_i^{\alpha_i}) \neq \chi'(n_i, p_i^{\alpha_i}) = \chi'(n_i)$, y lo análogo sucede si $\chi(\_, 2^{\alpha}) \neq \chi'(\_, 2^{\alpha})$. Entonces con esta construcción se obtienen $\varphi(2^{\alpha}) \cdot \varphi(p_1^{\alpha_1}) \cdots \varphi(p_t^{\alpha_t}) = \varphi(q)$ caracteres distintos.

Veamos que estos son todos los caracteres módulo q. Sea χ un caracter módulo q. Notemos que $\chi(n_i)^{\varphi(p_i^{\alpha_i})} = \chi\left(n_i^{\varphi(p_i^{\alpha_i})}\right) = \chi(1) = 1$, por lo que $\chi(n_i)$ es raíz $\varphi(p_i^{\alpha_i})$-ésima de la unidad. Se hace lo análogo para 2^{α}. Sean $\chi(\_, p_i^{\alpha_i})$, $\chi(\_, 2^{\alpha})$ los caracteres que mandan n_i a $\chi(n_i)$, (y dependiendo del valor de α, que mandan n_0 y/o n_0^* a $\chi(n_0)$ y a $\chi(n_0^*)$. Como todo entero n con $(n, q) = 1$ se puede representar de manera única módulo q como

$$n \equiv (n_0^*)^{\nu_0^*} \cdot n_0^{\nu_0} \cdot n_1^{\nu_1} \cdots n_t^{\nu_t} (\text{mod } q),$$

donde $\nu_i \in \{0, 1, \ldots, \varphi(p_i^{\alpha_i}) - 1\}$, y dependiendo del valor de α, se tiene que ν_0 y ν_0^* son nulos o deben cumplir $\nu_0 \in \{0, 1, \ldots, 2^{\alpha-2}\}, \nu_0^* \in \{0, 1\}$. Entonces

$$\chi(n) = \chi(n_0^*)^{\nu_0^*} \chi(n_0)^{\nu_0} \chi(n_1)^{\nu_1} \cdots \chi(n_t)^{\nu_t} = \chi(n, 2^{\alpha}) \chi(n, p_1^{\alpha_1}) \cdots \chi(n, p_t^{\alpha_t}).$$

Por lo tanto, era uno de los $\varphi(q)$ caracteres ya mencionados. ■

Definición 1.10. Se define y denota el *caracter principal* módulo q al caracter

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

Teorema 1.11. *Los caracteres módulo q forman un grupo isomorfo al grupo $\mathbb{Z}_q^*$.*

Demostración. Es un grupo ya que:

• es cerrado, pues dados χ y χ' caracteres módulo q, $\chi\chi' := \chi \cdot \chi'$ es caracter. Es q-periódico ya que $\chi\chi'(n) = \chi(n)\chi'(n) = \chi(n + q)\chi'(n + q) = \chi\chi'(n + q)$; también es multiplicativo pues $\chi\chi'(ab) = \chi(ab)\chi'(ab) = \chi(a)\chi(b)\chi'(a)\chi'(b) = \chi\chi'(a)\chi\chi'(b)$; y además $\chi\chi'(n) = 0 \Leftrightarrow (n, q) > 1$;

• χ_0 funge como el inverso, pues $\chi\chi_0(n) = \chi(n)\chi_0(n) = \chi(n) = \chi_0(n)\chi(n) = \chi_0\chi(n)$;

• Si χ es caracter, entonces

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

es un caracter, y cumple $\chi\chi^*(n) = \chi_0(n) = \chi^*\chi(n)$.
Por lo tanto, los caracteres módulo q forman un grupo.

Usando la notación de la demostración anterior, tenemos que el grupo de unidades de $\mathbb{Z}_q$ es:

$$\mathcal{U}(\mathbb{Z}_q) \cong \mathcal{G} \times \mathbb{Z}_{\varphi(p_1^{\alpha_1})} \times \cdots \times \mathbb{Z}_{\varphi(p_t^{\alpha_t})},$$

$$\text{donde} \quad \mathcal{G} = \begin{cases} \mathbb{Z}_1 \times \mathbb{Z}_1 & \text{si } \alpha \in \{0,1\}, \\ \mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}} & \text{si } \alpha \geqslant 2. \end{cases}$$

La identificación está determinada por $f(\chi) = ([m_0^*],[m_0],\ldots,[m_t])$, donde $([m_0^*],[m_0]) \in \mathcal{G}$; y $[m_i] \in \mathbb{Z}_{\varphi(p_i^{\alpha_i})}$ son tales que

$$\chi(n_0^*) = e^{2\pi i \frac{\nu_0^*(n_0^*)m_0^*}{2}}, \qquad \chi(n_0) = e^{2\pi i \frac{\nu_0(n_0)m_0}{2^{\alpha-2}}}, \qquad \chi(n_i) = e^{2\pi i \frac{\nu_i(n_i)m_i}{\varphi(p_i^{\alpha_i})}}.$$

Nótese que lo anterior no depende del representante que se tome. f define una biyección pues es inyectiva y $|\mathcal{U}(\mathbb{Z})| = \varphi(q) = \#\{\chi : \chi \text{ caracter módulo } q\}$. Además es un morfismo, ya que si $f(\chi) = (m_0^*, m_0, m_1, \ldots, m_t)$ y $f(\chi') = (m_0'^*, m_0', m_1', \ldots, m_t')$, entonces

$$f(\chi\chi') = (m_0^* + m_0'^*, m_0 + m_0', m_1 + m_1', \ldots, m_t + m_t')$$

puesto que $\chi\chi'(a) = \chi(a)\chi'(a)$. Por lo tanto son isomorfos. ■

Teorema 1.12. *Los caracteres módulo q tienen las siguientes propiedades:*

i) $\displaystyle\sum_{n=0}^{q-1} \chi(n) = \begin{cases} \varphi(q) & \textit{si } \chi = \chi_0, \\ 0 & \textit{en otro caso.} \end{cases}$

ii) $\displaystyle\sum_{\chi (mod\ q)} \chi(n) = \begin{cases} \varphi(q) & \textit{si } n \equiv 1 (mod\ q), \\ 0 & \textit{en otro caso.} \end{cases}$

Demostración. i] Si $\chi = \chi_0$, como $\chi_0(n)$ es igual a 1 para los $\varphi(q)$ valores de n que son primos relativos a q, y cero en los otros casos, es claro que la suma resulta $\varphi(q)$.

Si $\chi \neq \chi_0$, entonces existe $m \in \{0,1,2,\ldots,q-1\}$ con $(m,q) = 1$ tal que $\chi(m) \notin \{0,1\}$. Luego, como $(m,q) = 1$, tenemos que $\{0, m, 2m, 3m, \ldots, (q-1)m\}$ forman una clase completa de residuos módulo q, por lo que

$$\sum_{n=0}^{q-1} \chi(n) = \sum_{n=0}^{q-1} \chi(mn) = \chi(m) \sum_{n=0}^{q-1} \chi(n),$$

y dada la elección de m se concluye que $\sum_{n=0}^{q-1} \chi(n) = 0$.

ii] Si $n \equiv 1(\text{mod } q)$ se tiene que $\chi(n) = 1$ para cada uno de los $\varphi(q)$ caracteres distintos, por lo que la suma resulta $\varphi(q)$. Si $(n, q) > 1$ es claro, pues $\chi(n) = 0$ para cualquier caracter.

Si $n \not\equiv 1(\text{mod } q)$ y $(n, q) = 1$, existe un $\hat{\chi}$ tal que $\hat{\chi}(n) \neq 1$. Esto se puede deducir del hecho de que (retomando la notación del Teorema 1.9) $n \equiv (n_0^*)^{\mu_0^*} \cdot n_0^{\mu_0} \cdot n_1^{\mu_1} \cdots n_t^{\mu_t}(\text{mod } q)$ con algún $\mu_\kappa \neq 0$. Tomando $\hat{\chi}$ como el caracter que manda $(n_0^*)^{\nu_0^*} \cdot n_0^{\nu_0} \cdot n_1^{\nu_1} \cdots n_t^{\nu_t} \mapsto e^{\frac{2\pi i \nu_\kappa}{M}}$, para

$$M = \begin{cases} \varphi(p_\kappa^{\alpha_\kappa}) & \text{con } p_\kappa^{\alpha_\kappa} || q \text{ si } p_\kappa \neq 2, \\ 2^{\alpha-3} & \text{con } 2^\alpha || q \text{ si } p_\kappa = 2 \text{ y } \mu_\kappa = \mu_0, \\ 2 & \text{si } p_\kappa = 2 \text{ y } \mu_\kappa = \mu_0^*, \end{cases}$$

se tendría que $\hat{\chi}(n) \neq 1$. Además, $\hat{\chi}(n) \neq 0$ puesto que $(n, q) = 1$. Como los caracteres forman un grupo, se obtiene la igualdad

$$\sum_{\chi(\text{mod } q)} \chi(n) = \sum_{\chi(\text{mod } q)} (\hat{\chi}\chi)(n) = \hat{\chi}(n) \sum_{\chi(\text{mod } q)} \chi(n).$$

Como $\hat{\chi}(n) \notin \{0, 1\}$ se concluye que $\sum_{\chi(\text{mod } q)} \chi(n) = 0$. ■

Corolario 1.13. *Si $(a, q) = 1$, entonces*

$$\frac{1}{\varphi(q)} \sum_{\chi(mod\ q)} \overline{\chi(a)}\chi(n) = \begin{cases} 1 & si\ n \equiv a(mod\ q), \\ 0 & en\ otro\ caso. \end{cases}$$

Demostración. Notemos primero que $\overline{\chi(a)} = \chi(a^*)$, donde $aa^* \equiv 1(\text{mod } q)$. Sea $N = na^*$. Del Teorema 1.12 se sigue que

$$\frac{1}{\varphi(q)} \sum_{\chi(\text{mod } q)} \overline{\chi(a)}\chi(n) = \frac{1}{\varphi(q)} \sum_{\chi(\text{mod } q)} \chi(N) = \begin{cases} 1 & \text{si } N \equiv 1(\text{mod } q), \\ 0 & \text{en otro caso.} \end{cases}.$$

Observando que $na^* \equiv N \equiv 1(\text{mod } q)$ si y sólo si $n \equiv a(\text{mod } q)$, se deduce el Corolario. ■

Definición 1.14. Sea χ un caracter módulo q. Se dice que χ es un *caracter imprimitivo* módulo q si existe $q^* < q$ tal que $\chi(n)$, restringida a los enteros n que son primos relativos a q, es q^* periódica. En otro caso se dirá que χ es un *caracter primitivo* módulo q.

Observación 1.15. Sea χ un caracter módulo q, y sean $q_1, q_2 \in \mathbb{N}$ tales que χ es q_1 periódico y q_2 periódico cuando se restringe a los enteros n que son primos relativos a q, entonces también es (q_1, q_2) periódico.

Proposición 1.16. *Sea χ caracter imprimitivo módulo q, y sea q^* el menor periodo de $\chi(n)$ restringido a los enteros n que son primos relativos a q. Entonces existe único caracter primitivo χ^* módulo q^* tal que $\chi(n) = \chi^*(n)\chi_0(n)$, donde χ_0 es el caracter principal módulo q.*

Demostración. Defínase $\chi^*(n)$ como

$$\chi^*(n) = \begin{cases} 0 & \text{si } (n, q^*) > 1, \\ \chi(n) & \text{si } (n, q) = 1, \\ \chi(n + q^*t) & \text{si } (n, q^*) = 1, (n, q) > 1 \text{ y } (n + q^*t, q) = 1. \end{cases}$$

Veamos que dicha función está bien definida. Sólo es necesario analizar el tercer caso:
• Por la Observación 1.15, se deduce que $q^*|q$, pues en caso contrario se contradiría la minimalidad del periodo con (q^*, q).
• Sea $\hat{q}$ el máximo divisor de q tal que $(\hat{q}, q^*) = 1$, esto garantiza la existencia de una t tal que $(n + q^*t, \hat{q}) = 1$. Como $(n, q^*) = 1$ se deduce que $(n + q^*t, q) = 1$.
• $\chi^*(n)$ no depende de la elección de t, ya que χ es q^* periódica restringida a los n que son primos relativos a q.
Veamos que χ^* es un caracter módulo q^* ya que:
- $\chi^*(n) = 0 \Leftrightarrow (n, q^*) > 1$.
- Partiendo en casos se sigue que χ^* es q^* periódica.
- χ^* es multiplicativa. Se sigue de la multiplicidad de χ y de que:
  - $\chi^*(m)\chi^*(n) \neq 0 \Leftrightarrow \chi^*(mn) \neq 0$ y
  - $\chi^*(n)\chi^*(m) = \chi(m + t_1q^*)\chi(n + t_2q^*) = \chi(nm + q^*(t_1 + t_2 + t_1t_2q^*)) = \chi^*(nm)$.

Se tiene que χ^* es caracter primitivo módulo q^* pues en caso contrario, se contradiría la minimalidad del periodo de χ. Por cómo se definió, se sigue que

$$\chi(n) = \begin{cases} 0 = \chi^*(n)\chi_0(n) & \text{si } (n, q) > 1 \\ \chi^*(n) = \chi^*(n)\chi_0(n) & \text{si } (n, q) = 1, \end{cases}$$

por lo que $\chi(n) = \chi^*(n)\chi_0(n)$. ■

Definición 1.17. Dados χ y χ^* como en la proposición anterior, se dirá que χ^* *induce* a χ o que χ es *inducido* por χ^*.

Observación 1.18. Si $q^*|q$ y χ^* es caracter primitivo módulo q^*, entonces existe único χ caracter módulo q inducido por χ^*.

Proposición 1.19. *Sea $q = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ y $\chi(n) = \chi(n, p_1^{\alpha_1}) \cdots \chi(n, p_t^{\alpha_t})$ caracter módulo q. Se tiene que $\chi(n)$ es primitivo si y sólo si cada $\chi(n, p_t^{\alpha_t})$ es primitivo.*

Demostración. $\Rightarrow$] Supongamos que $\chi(n, p_1^{\alpha_1})$ no es primitivo, entonces existe $\beta < \alpha_1$ tal que $\chi(n, p_1^{\alpha_1}) = \chi^*(n, p_1^{\beta})\chi_0(n, p_1^{\alpha_1})$, por lo que

$$\chi(n) = \chi(n, p_1^{\alpha_1}) \cdots \chi(n, p_t^{\alpha_t}) = \chi^*(n, p_1^{\beta})\chi_0(n, p_1^{\alpha_1})\chi(n, p_2^{\alpha_2}) \cdots \chi(n, p_t^{\alpha_t})$$

$$= \chi^*(n, p_1^{\beta})\chi(n, p_2^{\alpha_2}) \cdots \chi(n, p_t^{\alpha_t})\chi_0(n, p_1^{\alpha_1}) = \hat{\chi}(n, \hat{q})\chi_0(n, q),$$

donde $\hat{q} = p_1^{\beta} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, entonces el caracter χ^* que induce a $\hat{\chi}$, induce también a χ, por lo cual no sería primitivo. Entonces $\chi(n, p_t^{\alpha_t})$ es primitivo para cada t.

$\Leftarrow$] Supóngase que χ no es primitivo, entonces es inducido por el caracter primitivo χ^*, el cual es producto de caracteres primitivos $\chi^*(n) = \chi^*(n, p_1^{\beta_1}) \cdots \chi^*(n, p_k^{\beta_k})$, donde $\beta_t \leqslant \alpha_t$ con desigualdad estricta para alguna t. Sean $\hat{\chi}(n, p_t^{\alpha_t})$ el caracter inducido por $\chi^*(n, p_t^{\beta_t})$, por lo que

$$\begin{aligned}\chi(n) &= \chi^*(n)\chi_0(n) = \chi^*(n, p_1^{\beta_1}) \cdots \chi^*(n, p_k^{\beta_k})\chi_0(n, p_1^{\alpha_1}) \cdots \chi_0(n, p_k^{\alpha_k}) \\ &= \hat{\chi}(n, p_1^{\alpha_1}) \cdots \hat{\chi}(n, p_k^{\alpha_k}) = \chi(n, p_1^{\alpha_1}) \cdots \chi(n, p_k^{\alpha_k}),\end{aligned}$$

y como la representación es única se tiene que $\chi(n, p_t^{\alpha_t}) = \chi_0(n, p_t^{\alpha_t})\chi^*(n, p_t^{\beta_t})$, contradiciendo la primitividad de alguno de ellos. Por lo tanto, χ sí es primitivo. ■

Definición 1.20. Se dice que un caracter χ es *real* si sólo toma valores reales.

Proposición 1.21. *Sea $p > 2$ primo. Existe único caracter real primitivo módulo p, el cual está dado por el símbolo de Kronecker $\left(\frac{n}{p}\right)$; y para $\alpha \geqslant 2$ no existen caracteres reales primitivos módulo p^α.*

Demostración. Sea χ un caracter módulo p^α, entonces

$$\chi(n) = \begin{cases} e^{2\pi i \frac{t\nu(n)}{p^{\alpha-1}(p-1)}} & \text{si } (n, p) = 1, \\ 0 & \text{si } p | n, \end{cases}$$

para algún $0 \leqslant t < p^{\alpha-1}(p-1)$. Como $\nu(n) = 1$ para algún n entero, para que el caracter sea real se necesita que $\frac{1}{2}p^{\alpha-1}(p-1)|t$. Si $t = 0$, el caracter es el caracter principal, el cual no es primitivo. Si $t = \frac{1}{2}p^{\alpha-1}(p-1)$, el caracter está dado por $\chi(n) = e^{\pi i \nu(n)} = (-1)^{\nu(n)}$ si $(n, p) = 1$. Entonces χ es inducido por el caracter primitivo módulo p dado por

$$\chi_p(n) = \left. \begin{cases} \left(\frac{n}{p}\right) & \text{si} (n, p) = 1, \\ 0 & \text{si } p | n, \end{cases} \right\} = \left(\frac{n}{p}\right).$$

■

Proposición 1.22. *Existe un caracter real primitivo módulo 4, dos caracteres reales primitivos módulo 8, y para cualquier otra potencia de 2 no existen caracteres reales primitivos.*

Demostración. Módulo 2 es claro, pues sólo existe el caracter principal. Módulo 2^α con $\alpha > 3$ un caracter está dado por

$$\chi(n) = \begin{cases} e^{2\pi i \left(\frac{t\nu(n)}{2} + \frac{t^*\nu^*(n)}{2^{\alpha-2}}\right)} & \text{si } (2, n) = 1, \\ 0 & \text{si } 2 | n. \end{cases}$$

Como existe n tal que $\nu(0)$ y $\nu^*(n) = 1$, para que sea un caracter real se tiene que $2^{\alpha-3}|t^*$. Así, el caracter resulta ser un caracter inducido y por lo tanto, no primitivo.

Para el caso módulo 4, sólo existe el caracter principal y el caracter primitivo

$$\chi_4(n) = \begin{cases} 1 & \text{si } n \equiv 1 (\text{mod } 4), \\ -1 & \text{si } n \equiv -1 (\text{mod } 4), \\ 0 & \text{si } 2|n. \end{cases}$$

Para el caso módulo 8 tiene cuatro caracteres, dos inducidos por los caracteres módulo 4, y otros dos caracteres reales primitivos dados por

$$\chi_8(n) \begin{cases} 1 & \text{si } n \equiv \pm 1 (\text{mod } 8), \\ -1 & \text{si } n \equiv \pm 3 (\text{mod } 8), \\ 0 & \text{si } 2|n, \end{cases} \qquad \text{y} \qquad \chi_8(n)\chi_4(n).$$

■

Proposición 1.23. *Cada caracter real primitivo módulo q se puede representar con el símbolo de Kronecker como $\chi(n) = \left(\frac{\pm q}{n}\right)$ para cada $n > 0$.*

Demostración. Dado p primo impar se define $p' = (-1)^{\frac{p-1}{2}} p$. Notemos que:

$$\chi_4 = \left.\begin{cases} \left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} & \text{si } 2 \nmid n, \\ 0 & \text{si } 2 \mid n, \end{cases}\right\} = \left(\frac{-4}{n}\right),$$

$$\chi_8(n) = \left.\begin{cases} \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} & \text{si } 2 \nmid n, \\ 0 & \text{si } 2 \mid n, \end{cases}\right\} = \left(\frac{8}{n}\right),$$

$$\chi_8(n)\chi_4(n) = \left(\frac{8}{n}\right)\left(\frac{-4}{n}\right) = \left(\frac{-32}{n}\right) = \left(\frac{-8}{n}\right),$$

$$\chi_p(n) = \left(\frac{n}{p}\right) = \left(\frac{p'}{n}\right).$$

Como el símbolo de Kronecker tiene la propiedad de que, para cualquier $n \geqslant 1$ se da la igualdad $\left(\frac{a}{n}\right)\left(\frac{b}{n}\right) = \left(\frac{ab}{n}\right)$ y, por la descomposición de caracteres, se concluye la demostración. ■

Definición 1.24. Dado χ caracter módulo q se define su *suma gaussiana* como

$$\tau(\chi) := \sum_{m=1}^{q} \chi(m) e^{\frac{2\pi i m}{q}}.$$

Proposición 1.25. *Para cualquier $n \in \mathbb{N}$ y χ caracter primitivo módulo q se tiene que*

$$\chi(n)\tau(\overline{\chi}) = \sum_{h=1}^{q} \overline{\chi}(h) e^{\frac{2\pi i n h}{q}}.$$

Demostración. Se dividirá la demostración en tres casos.
Caso 1. $(n, q) = 1$**:** Se sigue de que

$$\chi(n)\tau(\overline{\chi}) = \sum_{m=1}^{q} \overline{\chi}(m)\chi(n)e^{\frac{2\pi i m}{q}} = \sum_{h=1}^{q} \overline{\chi}(nh)\chi(n)e^{\frac{2\pi i n h}{q}} = \sum_{h=1}^{q} \overline{\chi}(h)e^{\frac{2\pi i n h}{q}}.$$

Caso 2. $(n, q) > 1$ **y** $q|n$**:** Este caso es cierto ya que $\chi(n)\tau(\overline{\chi}) = 0$, y

$$\sum_{h=1}^{q} \overline{\chi}(h)e^{\frac{2\pi i n h}{q}} = \sum_{h=1}^{q} \overline{\chi}(h)e^{2\pi i h \frac{n}{q}} = \sum_{h=1}^{q} \overline{\chi}(h) = 0.$$

Caso 3. $(n, q) > 1$ **y** $q \nmid n$**:** Sea $\frac{n}{q} = \frac{n_1}{q_1}$, donde $(n_1, q_1) = 1$, y sea $q_2 = \frac{q}{q_1}$. En este caso sucede que $\chi(n)\tau(\overline{\chi}) = 0$, y $\{uq_1 + v : 0 \leqslant v < q_1, 0 \leqslant u < q_2\}$ es un sistema completo de residuos módulo q, entonces

$$\sum_{h=1}^{q} \overline{\chi}(h)e^{\frac{2\pi i n h}{q}} = \sum_{h=1}^{q} \overline{\chi}(h)e^{\frac{2\pi i n_1 h}{q_1}} = \sum_{v=0}^{q_1-1}\sum_{u=0}^{q_2-1} \overline{\chi}(uq_1+v)e^{\frac{2\pi i n_1(uq_1+v)}{q_1}} = \sum_{v=0}^{q_1-1} e^{\frac{2\pi i n_1 v}{q_1}} \sum_{u=0}^{q_2-1} \overline{\chi}(uq_1+v).$$

Basta ver que $\sum_{u=0}^{q_2-1} \overline{\chi}(uq_1 + v) = 0$ para cualquier $v \in \{0, 1, 2, \ldots, q_1 - 1\}$. Como χ es un caracter primitivo, existe un entero $c \equiv 1(\text{mod } q_1)$ tal que $\chi(c) \neq 1$, entonces

$$\overline{\chi}(c) \sum_{u=0}^{q_2-1} \overline{\chi}(uq_1 + v) = \sum_{u=0}^{q_2-1} \overline{\chi}(cuq_1 + cv) = \sum_{u=0}^{q_2-1} \overline{\chi}(uq_1 + v),$$

y como $\overline{\chi}(c) \notin \{0, 1\}$ se concluye que $\sum_{u=0}^{q_2-1} \overline{\chi}(uq_1+v) = 0$, obteniendo la veracidad de este caso. ■

Teorema 1.26. *Para cualquier caracter primitivo χ módulo q se tiene que*

$$|\tau(\chi)| = q^{1/2}.$$

Demostración. Por el Lema anterior, para cualquier n entero se tiene que

$$|\chi(n)|^2|\tau(\chi)|^2 = \chi(n)\tau(\overline{\chi}) \cdot \overline{\chi}(n)\tau(\chi) = \sum_{h_1=1}^{q}\sum_{h_2=1}^{q} \overline{\chi}(h_1)\chi(h_2)e^{\frac{2\pi i n(h_1-h_2)}{q}}.$$

De aquí se sigue que

$$\varphi(q)|\tau(\chi)|^2 = \sum_{n=1}^{q} |\chi(n)|^2|\tau(\chi)|^2 = \sum_{n=1}^{q}\sum_{h_1=1}^{q}\sum_{h_2=1}^{q} \overline{\chi}(h_1)\chi(h_2)e^{\frac{2\pi i n(h_1-h_2)}{q}}$$

$$= \sum_{h_1=1}^{q}\sum_{h_2=1}^{q} \overline{\chi}(h_1)\chi(h_2) \sum_{n=1}^{q} e^{\frac{2\pi i n(h_1-h_2)}{q}} = \sum_{h_1=1}^{q} \overline{\chi}(h_1)\chi(h_1)q = q\varphi(q),$$

de donde se deduce que $|\tau(\chi)| = q^{1/2}$. $\blacksquare$

Capítulo 2

La función ζ de Riemann y las funciones L de Dirichlet

2.1. La función ζ de Riemann

La *función ζ de Riemann* está definida para toda $s \in \mathbb{C}$ con $\Re(s) > 1$, como

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

La función ζ es holomorfa en $\Re(s) > 1$ puesto que, si tomamos $\zeta_N(s) = \sum_{n=1}^{N} \frac{1}{n^s}$ y $\delta > 1$, si $\Re(s) \geqslant \delta$, entonces

$$|\zeta_M(s) - \zeta_N(s)| \leqslant \sum_{n=N}^{M} \frac{1}{n^\delta} \leqslant \int_{N-1}^{\infty} \frac{1}{x^\delta} dx = \frac{1}{(\delta-1)(N-1)^{\delta-1}}.$$

Entonces, en cualquier compacto del semiplano $\Re(s) > 1$, $\zeta_N(s)$ converge uniformemente a $\zeta(s)$ cuando $N \to \infty$, y como $\zeta_N(s)$ es holomorfa en todo el plano, se concluye que $\zeta(s)$ es holomorfa en $\Re(s) > 1$.

Teorema 2.1 (Identidad de Euler)**.** *Sea $s \in \mathbb{C}$ con $\Re(s) > 1$, entonces se tiene la igualdad*

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

Demostración. Por los Teoremas A.2 y A.3 se tiene que el producto converge a una función analítica. Veamos que

$$\left| \sum_{n=1}^{M} \frac{1}{n^s} - \sum_{\substack{n \text{ tal que} \\ p|n \Rightarrow p \leqslant M}} \frac{1}{n^s} \right| \leqslant \sum_{\substack{n>M \text{ tal que} \\ p|n \Rightarrow p \leqslant M}} \frac{1}{n^{\Re(s)}} < \frac{1}{\Re(s) M^{\Re(s)-1}} \to 0$$

cuando $M \to \infty$. La demostración se sigue de esto y de que

$$\sum_{\substack{n \text{ tal que} \\ p|n \Rightarrow p \leqslant M}} \frac{1}{n^s} = \prod_{\substack{p \leqslant M \\ p \text{ primo}}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) = \prod_{\substack{p \leqslant M \\ p \text{ primo}}} \frac{1}{1 - \frac{1}{p^s}}.$$

■

Definición 2.2. Para cada $x \in \mathbb{R}$ con $x > 0$ se definen las funciones $\theta(x)$ y $\omega(x)$ como

$$\theta(x) = \sum_{n=-\infty}^{\infty} e^{-\pi x n^2} \qquad \omega(x) = \sum_{n=1}^{\infty} e^{-\pi x n^2}.$$

No es difícil ver que dichas funciones están bien definidas pues su convergencia se deduce fácilmente de la integral Gaussiana, que cumple la igualdad

$$\int_{-\infty}^{\infty} e^{-(at-b)^2} dt = \frac{\sqrt{\pi}}{a}.$$

Teorema 2.3 (Ecuación funcional de la función θ). *Para cualquier $x > 0$ se tiene que*

$$\theta\left(\frac{1}{x}\right) = \sqrt{x} \cdot \theta(x).$$

Demostración. Sea $h(t) = e^{-ct^2}$. Como h es una función entera y $h(x+iy) \ll \frac{e^{ca^2}}{1+x^2}$ para cualquier $a > 0$, se puede aplicar la Fórmula de Sumación de Poisson (Teorema D.4) a la función h. Si

$$\hat{h}(t) = \int_{-\infty}^{\infty} h(t) e^{-2\pi i t n} dt$$

es la transformada de Fourier de h, entonces

$$\theta(x) = \sum_{n \in \mathbb{Z}} h(n) = \sum_{n \in \mathbb{Z}} \hat{h}(n) = \sum_{n \in \mathbb{Z}} \int_{-\infty}^{\infty} h(t) e^{-2\pi i t n} dt = \sum_{n \in \mathbb{Z}} \int_{-\infty}^{\infty} e^{-\pi x t^2 - 2\pi i t n} dt$$

$$= \sum_{n \in \mathbb{Z}} e^{-\frac{\pi n^2}{x}} \int_{-\infty}^{\infty} e^{-\pi(\sqrt{x}t + \frac{in}{\sqrt{x}})^2} dt = \sum_{n \in \mathbb{Z}} e^{-\frac{\pi n^2}{x}} \frac{\sqrt{\pi}}{\sqrt{\pi}\sqrt{x}} = \frac{1}{\sqrt{x}} \theta\left(\frac{1}{x}\right).$$

■

Corolario 2.4 (Ecuación funcional de la función ω). *Para cualquier $x \in \mathbb{R}$ con $x > 0$ se tiene la igualdad*

$$\omega\left(\frac{1}{x}\right) = \frac{\sqrt{x}}{2} - \frac{1}{2} + \sqrt{x} \cdot \omega(x).$$

Teorema 2.5. *Para todo $s \in \mathbb{C}$ con $\Re(s) > 1$ se cumple la igualdad*

$$\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s) = \frac{1}{s(s-1)} + \int_1^{\infty} \omega(x)[x^{-\frac{1+s}{2}} + x^{\frac{s}{2}-1}] dx.$$

Demostración. Haciendo un cambio de variable a la función Γ se obtiene la igualdad

$$\Gamma\left(\frac{s}{2}\right) = n^s \pi^{\frac{s}{2}} \int_0^\infty e^{-\pi n^2 y} y^{\frac{s}{2}-1} dy, \tag{2.1}$$

por lo que

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \sum_{n=1}^{\infty}\int_0^\infty e^{-\pi n^2 x} x^{\frac{s}{2}-1}dx = \int_0^\infty \omega(x)x^{\frac{s}{2}-1}dx = \int_0^1 \omega(x)x^{\frac{s}{2}-1}dx + \int_1^\infty \omega(x)x^{\frac{s}{2}-1}dx.$$

Haciendo otro cambio de variable y usando la ecuación funcional para ω (Teorema 2.4), se deduce que

$$\begin{aligned}
\int_0^1 \omega(x)x^{\frac{s}{2}-1}dx + \int_1^\infty \omega(x)x^{\frac{s}{2}-1}dx &= \int_1^\infty \omega\left(\frac{1}{x}\right)x^{-1-\frac{s}{2}}dx + \int_1^\infty \omega(x)x^{\frac{s}{2}-1}dx \\
&= \frac{1}{2}\int_1^\infty x^{\frac{-1-s}{2}}dx - \frac{1}{2}\int_1^\infty x^{-1-\frac{s}{2}}dx + \int_1^\infty \omega(x)x^{-\frac{s+1}{2}}dx + \int_1^\infty \omega(x)x^{\frac{s}{2}-1}dx \\
&= -\frac{1}{1-s} - \frac{1}{s} + \int_1^\infty \omega(x)[x^{-\frac{s+1}{2}} + x^{\frac{s}{2}-1}]dx = \frac{1}{s(s-1)} + \int_1^\infty \omega(x)[x^{-\frac{1+s}{2}} + x^{\frac{s}{2}-1}]dx.
\end{aligned}$$

■

Definición 2.6. Para cada $s \in \mathbb{C}$ se define la función ξ como

$$\xi(s) = \frac{1}{2}\left(1 + s(s-1)\int_1^\infty \omega(x)[x^{-\frac{s+1}{2}} + x^{\frac{s}{2}-1}]dx\right).$$

Como $\omega(x)$ decae de manera exponencial, se sigue que la función $\xi(s)$ es entera.

Proposición 2.7 (Ecuación funcional de la función ξ)**.** *Para cualquier $s \in \mathbb{C}$ se tiene que*

$$\xi(s) = \xi(1-s).$$

Demostración. Se sigue de la definición de la función ξ. ■

Teorema 2.8. *La función ζ de Riemman tiene continuación meromorfa en $\mathbb{C}$, cuyo único polo se localiza en $s = 1$ y es simple. Dicha extensión está dada por la ecuación*

$$\zeta(s) = \frac{2\pi^{\frac{s}{2}}}{s(s-1)\Gamma\left(\frac{s}{2}\right)}\xi(s).$$

Demostración. Por el Teorema 2.5, la igualdad es cierta cuando $\Re(s) > 1$. Por continuación analítica, bastaría ver que el lado derecho de la igualdad es una función meromorfa con único polo en $s = 1$, el cual es simple. Como $\Gamma(s)$ y $\xi(s)$ son analíticas y $\Gamma(s)$ no se anula, la función resulta ser holomorfa. Como $\Gamma(s)$ tiene polo simple en $s = 0$ el polo del factor $\frac{1}{s}$ se anula, y como $\xi(1) = \frac{1}{2}$ y $\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$, dicha función tiene un único polo simple en $s = 1$. ■

Teorema 2.9 (Ecuación funcional de la función ζ de Riemann). *Para cualquier $s \in \mathbb{C}\backslash\{0,1\}$ se cumple la igualdad*

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-\frac{1}{2}(1-s)}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s),$$

y para $s \in \{0,1\}$ el residuo de ambos lados de la igualdad coincide.

Demostración. Se sigue de la ecuación funcional de la función $\xi(s)$ y del Teorema 2.8. ∎

Proposición 2.10. *El residuo de $\zeta(s)$ en $s = 1$ es 1.*

Demostración. Se sigue de que

$$\mathrm{Res}_{s=1}\zeta(s) = \lim_{s\to 1}(s-1)\frac{2\pi^{-\frac{s}{2}}}{s(s-1)\Gamma\left(\frac{s}{2}\right)}\xi(s) = \frac{2\sqrt{\pi}}{\Gamma\left(\frac{1}{2}\right)}\xi(1) = 1.$$

∎

Teorema 2.11. *La función ζ de Riemman tiene ceros en $\{0,-2,-4,-6,\dots\}$, y sus otros ceros se localizan en la región $0 \leqslant \Re(s) \leqslant 1$.*

Demostración. Por la Identidad de Euler (ver Teorema 2.1), la función ζ no tiene ceros en $\Re(s) > 1$, ya que

$$|\zeta(s)| = \left|\prod_{p \text{ primo}} \frac{1}{1-\frac{1}{p^s}}\right| \geqslant \prod_{p \text{ primo}} \frac{1}{1+\frac{1}{p^{\Re s}}},$$

lo cual es mayor que 0 ya que, por el Teorema A.2 y como $\displaystyle\sum_{p \text{ primo}} \frac{1}{p^{\Re(s)}}$ es absolutamente convergente, se tiene que

$$\prod_{p \text{ primo}}\left(1+\frac{1}{p^{\Re(s)}}\right) < \infty.$$

Para $\Re(s) < 0$, usando la ecuación funcional de la función ζ y el Teorema C.7 se tiene que

$$\zeta(s) = \pi^{s+\frac{1}{2}}\frac{\zeta(1-s)}{\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right)\operatorname{sen}\left(\frac{(1-s)\pi}{2}\right)}.$$

De aquí que, en $\Re(s) < 0$, sus ceros son los polos de $\Gamma\left(\frac{s}{2}\right)$, pues los de $\Gamma\left(\frac{s+1}{2}\right)$ se anulan con los ceros de $\operatorname{sen}\left(\frac{(1-s)\pi}{2}\right)$ y $\zeta(1-s)$ no se anula en $\Re(s) < 0$. Entonces los ceros de $\zeta(s)$ en $\Re(s) < 0$ están en $\{-2,-4,-6,\dots\}$. ∎

Proposición 2.12. *En la región $\Re(s) > 0$ se cumple la igualdad*

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

Demostración. Si $\Re(s) > 1$ se tiene que

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s} = \sum_{n=1}^{\infty} n\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right) = s\sum_{n=1}^{\infty} n\int_n^{n+1}\frac{1}{x^{s+1}}dx = s\int_1^{\infty}\frac{\lfloor x\rfloor}{x^{s+1}}dx$$

$$= s\int_1^\infty \frac{1}{x^s}dx - s\int_1^\infty \frac{\{x\}}{x^{s+1}}dx = \frac{1}{s-1} + 1 - s\int_1^\infty \frac{\{x\}}{x^{s+1}}dx.$$

Ahora, nótese que la integral converge absolutamente en la región $\Re(s) > 0$, y uniformemente en $\Re(s) \geqslant \delta$ para cualquier $\delta > 0$, por lo tanto, es holomorfa. Por extensión analítica se da igualdad en la región $\Re(s) > 0$. ■

2.2. L-funciones de Dirichlet

Definición 2.13. Para cada χ caracter módulo q y $s \in \mathbb{C}$ tal que $\Re(s) > 1$ se define la *L-función de Dirichlet relativa a* χ (o simplemente L-función) como

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

Es claro que las L-funciones convergen en $\Re(s) > 1$, ya que

$$\sum_{n=1}^{\infty} \left|\frac{\chi(n)}{n^s}\right| \leqslant \sum_{n=1}^{\infty} \frac{1}{n^s} \leqslant 1 + \int_1^\infty \frac{1}{x^s}dx = 1 + \frac{1}{s-1}.$$

Proposición 2.14. *Para cualquier χ caracter de Dirichlet se tiene que la función $L(s,\chi)$ es holomorfa en la región $\Re(s) > 1$.*

Demostración. Sean $f_N(s) = \displaystyle\sum_{n=1}^{N} \frac{\chi(n)}{n^s}$ y $\delta > 1$. Veamos que si $\Re(s) \geqslant \delta$, se tiene que

$$|f_M(s) - f_N(s)| \leqslant \sum_{n=N}^{M} \frac{1}{n^\delta} \leqslant \int_{N-1}^\infty \frac{1}{x^\delta}dx = \frac{1}{(\delta-1)(N-1)^{\delta-1}}.$$

Entonces $f_N(s)$ converge uniformemente a $L(s,\chi)$ cuando $N \to \infty$ en cualquier compacto del semiplano $\Re(s) > 1$, y como $f_N(s)$ es holomorfa en todo el plano, se concluye que $L(s,\chi)$ es holomorfa en esta región. ■

Teorema 2.15 (Identidad de Euler)**.** *Para toda L-función de Dirichlet y $s \in \mathbb{C}$ con $\Re(s) > 1$ se tiene la igualdad*

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

Demostración. Como $\displaystyle\sum_{p \text{ primo}} \left|\frac{\chi(p)}{p^s}\right|$ converge y $-\dfrac{\chi(p)}{p^s} \neq -1$ para cualquier p primo, por el Teorema A.2 se tiene que el producto $\displaystyle\prod_{p \text{ primo}} \left[1 - \frac{\chi(p)}{p^s}\right]$ existe y es distinto de 0, por lo que su recíproco también existe. Notemos que

$$\prod_{\substack{p \leqslant M \\ p \text{ primo}}} \frac{1}{1 - \frac{\chi(p)}{p^s}} = \sum_{\substack{p \text{ primo} \\ p|n \Leftrightarrow p \leqslant M}} \frac{\chi(n)}{n^s}.$$

Entonces

$$\left|\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}-\prod_{\substack{p\leqslant M\\ p\text{ primo}}}\frac{1}{1-\frac{\chi(p)}{p^s}}\right|=\left|\sum_{\substack{n=1\\ \text{tal que } p|n \text{ para}\\ \text{algún } p>M \text{ primo}}}^{\infty}\frac{\chi(n)}{n^s}\right|\leqslant\sum_{n>M}\frac{1}{n^{\Re(s)}}$$

$$<\frac{1}{\Re(s)M^{\Re(s)-1}}\xrightarrow[K\to\infty]{}0,$$

por lo tanto, este producto converge a $L(s,\chi)$. ■

Proposición 2.16. *Sea χ_0 el caracter principal módulo q y $s\in\mathbb{C}$. Si $\Re(s)>1$ se tiene que*

$$L(s,\chi_0)=\zeta(s)\prod_{\substack{p|q\\ p\text{ primo}}}\left(1-\frac{1}{p^s}\right).$$

Demostración. Se deduce directamente de la Identidad de Euler de las funciones ζ y $L(s,\chi_0)$. ■

Teorema 2.17. *La función $L(s,\chi_0)$ se puede extender de manera meromorfa en todo el plano con sólo un polo en $s=1$, con residuo*

$$\prod_{p|q}\left(1-\frac{1}{p}\right)=\frac{\varphi(q)}{q}.$$

Demostración. Se sigue de la Proposición 2.12 y la Proposición 2.16, y de que $\zeta(s)$ es holomorfa en $\mathbb{C}\backslash\{1\}$ y de que $\prod_{p|q}\left(1-\frac{1}{p}\right)$ es constante. ■

Proposición 2.18. *Sea $\chi\neq\chi_0$, entonces para cualquier $s\in\mathbb{C}$ con $\Re(s)>0$ se cumple la igualdad*

$$L(s,\chi)=s\int_1^{\infty}\frac{R(x)}{x^{s+1}}dx,$$

donde $R(x)=\sum_{n\leqslant x}\chi(n)$.

Demostración. Nótese que la función $R(x)$ es $q-$periódica, y por lo tanto es acotada. Luego, si $\Re(s)>1$, se tiene que

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}=\sum_{n=1}^{\infty}R(n)\left(\frac{1}{n^s}-\frac{1}{(n+1)^s}\right)=s\int_1^{\infty}\frac{R(x)}{x^{s+1}}dx.$$

Nótese que la integral es absolutamente convergente en la región $\Re(s)>0$ y converge uniformemente en la región $\Re(s)\geqslant\delta$ para cualquier $\delta>0$, por lo tanto, dicha integral es analítica en $\Re(s)>0$, y por la unicidad de la extensión analítica, la igualdad se cumple en dicha región. ■

Proposición 2.19. *Sea χ un caracter imprimitivo módulo q, y χ^* el caracter primitivo módulo*

q^* que induce a χ entonces, para cualquier $s \in \mathbb{C}$ con $\Re(s) > 0$ se tiene que

$$L(s,\chi) = L(s,\chi^*) \prod_{\substack{p|q \\ p \text{ primo}}} \left(1 - \frac{\chi^*(p)}{p^s}\right).$$

Demostración. Para $\Re(s) > 1$ se tiene que

$$L(s,\chi) = \prod_{p \text{ primo}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \prod_{\substack{p\nmid q \\ p \text{ primo}}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

$$= \prod_{p \text{ primo}} \left(1 - \frac{\chi^*(p)}{p^s}\right)^{-1} \prod_{\substack{p|q \\ p \text{ primo}}} \left(1 - \frac{\chi^*(p)}{p^s}\right) = L(s,\chi^*) \prod_{\substack{p|q \\ p \text{ primo}}} \left(1 - \frac{\chi^*(p)}{p^s}\right).$$

La igualdad se sigue en $\Re(s) > 0$ por la unicidad de la extensión analítica. ∎

Definición 2.20. Dado caracter χ módulo q y $x \in \mathbb{R}$ con $x > 0$ se definen las funciones

$$\theta_1(x,\chi) = \sum_{n=-\infty}^{\infty} \chi(n) e^{-\frac{n^2\pi x}{q}},$$

$$\theta_2(x,\chi) = \sum_{-\infty}^{\infty} n\chi(n) e^{-\frac{n^2\pi x}{q}}.$$

Teorema 2.21 (Ecuación funcional de θ_1 y θ_2)**.** *Sea $x > 0$ y χ un caracter primitivo módulo q, entonces*

$$\tau(\overline{\chi})\theta_1(x,\chi) = \frac{q^{\frac{1}{2}}}{x^{\frac{1}{2}}} \theta_1\left(\frac{1}{x}, \overline{\chi}\right),$$

$$\tau(\overline{\chi})\theta_2(x,\chi) = \frac{iq^{\frac{1}{2}}}{x^{\frac{3}{2}}} \theta_2\left(\frac{1}{x}, \overline{\chi}\right).$$

Demostración. Sea $h(t) = e^{-\pi x t^2 + 2\pi i t\alpha}$. Nótese que h es una función entera y que para cualquier $a > 0$ se tiene que $h(\sigma + it) \ll \frac{e^{ca^2}}{1+x^2}$ entonces, aplicando la Fórmula de Sumación de Poisson (Teorema D.4) a $h(t)$ y usando la integral gaussiana se tiene que

$$\sum_{n\in\mathbb{Z}} e^{-\pi x n^2 + 2\pi i n\alpha} = \sum_{n\in\mathbb{Z}} h(n) = \sum_{n\in\mathbb{Z}} \int_{-\infty}^{\infty} h(t) e^{-2\pi i t n} dt = \sum_{n\in\mathbb{Z}} \int_{-\infty}^{\infty} e^{-\pi x t^2 - 2\pi i t(n-\alpha)} dt$$

$$= \sum_{n\in\mathbb{Z}} e^{-\frac{\pi(n-\alpha)^2}{x}} \int_{-\infty}^{\infty} e^{-\pi\left(\sqrt{x}t + \frac{i(n-\alpha)}{\sqrt{x}}\right)^2} dt = \sum_{n\in\mathbb{Z}} e^{-\frac{\pi(n-\alpha)^2}{x}} \frac{\sqrt{\pi}}{\sqrt{\pi x}} = \frac{1}{\sqrt{x}} \sum_{n\in\mathbb{Z}} e^{-\frac{\pi(n-\alpha)^2}{x}}.$$

La ecuación funcional de θ_1 se cumple, ya que

$$\tau(\overline{\chi})\theta_1(x,\chi) = \sum_{n\in\mathbb{Z}} e^{-\frac{\pi x n^2}{q}} \sum_{m=1}^{q} \overline{\chi}(m) e^{\frac{2\pi i m n}{q}} = \sum_{m=1}^{q} \overline{\chi}(m) \sum_{n\in\mathbb{Z}} e^{-\pi \frac{x}{q} n^2 + 2\pi i n \frac{m}{q}}$$

$$= \sum_{m=1}^{q} \overline{\chi}(m) \frac{q^{\frac{1}{2}}}{x^{\frac{1}{2}}} \sum_{n\in\mathbb{Z}} e^{-\frac{\left(n+\frac{m}{q}\right)^2 \pi q}{x}} = \frac{q^{\frac{1}{2}}}{x^{\frac{1}{2}}} \sum_{m=1}^{q} \overline{\chi}(m) \sum_{n\mathbb{Z}} e^{-\frac{(nq+m)^2\pi}{xq}} = \frac{q^{\frac{1}{2}}}{x^{\frac{1}{2}}} \sum_{l\in\mathbb{Z}} \overline{\chi}(l) e^{-\frac{l^2\pi}{xq}} = \frac{q^{\frac{1}{2}}}{x^{\frac{1}{2}}} \theta_1\left(\frac{1}{x}, \overline{\chi}\right).$$

Si se deriva respecto de α la igualdad que se dedujo con la Fórmula de Sumación de Poisson, se tiene que

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

Entonces, la ecuación funcional de θ_2 se cumple, ya que

$$\tau(\overline{\chi})\theta_2(x,\chi) = \sum_{n\in\mathbb{Z}} n e^{-\frac{\pi x n^2}{q}} \chi(n)\tau(\overline{\chi}) = \sum_{n\in\mathbb{Z}} n e^{-\frac{\pi x n^2}{q}} \sum_{m=1}^{q} \overline{\chi}(m) e^{\frac{2\pi i m n}{q}}$$

$$= \sum_{m=1}^{q} \overline{\chi}(m) \sum_{n\in\mathbb{Z}} n e^{\frac{-\pi x n^2 + 2\pi i m n}{q}} = i\frac{q^{\frac{3}{2}}}{x^{\frac{3}{2}}} \sum_{m=1}^{q} \overline{\chi}(m) \sum_{n\in\mathbb{Z}} \left(n + \frac{m}{q}\right) e^{-\frac{\pi\left(n+\frac{m}{q}\right)^2 q}{x}}$$

$$= i\frac{q^{\frac{1}{2}}}{x^{\frac{3}{2}}} \sum_{m=1}^{q} \sum_{n\in\mathbb{Z}} \overline{\chi}(nq+m)(nq+m) e^{-\frac{\pi(nq+m)^2}{xq}} = i\frac{q^{\frac{1}{2}}}{x^{\frac{3}{2}}} \sum_{l\in\mathbb{Z}} \overline{\chi}(l) l e^{-\frac{\pi l^2}{xq}} = i\frac{q^{\frac{1}{2}}}{x^{\frac{3}{2}}} \theta_2\left(\frac{1}{x}, \overline{\chi}\right).$$

■

Teorema 2.22. *Las funciones L tienen extensión meromorfa en todo el plano. Dos representaciones posibles son*

$$L(s,\chi) = \begin{cases} \dfrac{\pi^{\frac{s}{2}}}{2q^{\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)} \left[\displaystyle\int_1^\infty x^{\frac{s}{2}-1}\theta_1(s,\chi)dx + \frac{q^{1/2}}{\tau(\overline{\chi})}\int_1^\infty x^{-\frac{s+1}{2}}\theta_1(s,\overline{\chi})dx\right], \\ \dfrac{\pi^{\frac{s+1}{2}}}{2q^{\frac{s+1}{2}}\Gamma\left(\frac{s+1}{2}\right)} \left[\displaystyle\int_1^\infty x^{\frac{s-1}{2}}\theta_2(x,\chi)dx + \frac{iq^{1/2}}{\tau(\overline{\chi})}\int_1^\infty x^{-\frac{s}{2}}\theta_2(x,\overline{\chi})dx\right]. \end{cases}$$

Demostración. Veamos primero que se cumplen las igualdades en $\Re(s) > 0$. Fijando $y = \frac{x}{q}$ en la ecuación (2.1), se obtiene la primer fórmula ya que

$$\pi^{-\frac{s}{2}} q^{\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) L(s,\chi) = \frac{1}{2}\int_0^\infty x^{\frac{s}{2}-1}\theta_1(x,\chi)dx$$

$$= \frac{1}{2}\int_1^\infty x^{\frac{s}{2}-1}\theta_1(x,\chi)dx + \frac{1}{2}\int_0^1 x^{\frac{s}{2}-1}\theta_1(x,\chi)dx$$

$$= \frac{1}{2}\int_1^\infty x^{\frac{s}{2}-1}\theta_1(x,\chi)dx + \frac{1}{2}\int_1^\infty x^{-\frac{s}{2}-1}\theta_1\left(\frac{1}{x},\chi\right)dx$$

$$= \frac{1}{2}\int_1^\infty x^{\frac{s}{2}-1}\theta_1(x,\chi)dx + \frac{q^{\frac{1}{2}}}{2\tau(\overline{\chi})}\int_1^\infty x^{-\frac{s+1}{2}}\theta_1(x,\overline{\chi})dx.$$

La segunda fórmula se deduce al cambiar s por $s+1$ y $y = \frac{x}{q}$ en la ecuación (2.1), ya que

$$\pi^{-\frac{s+1}{2}} q^{\frac{s+1}{2}} \Gamma\left(\frac{s+1}{2}\right) L(s,\chi) = \frac{1}{2}\int_0^\infty \theta_2(x,\chi) x^{\frac{s-1}{2}} dx$$

$$= \frac{1}{2}\int_1^\infty \theta_2(x,\chi)x^{\frac{s-1}{2}}dx + \frac{1}{2}\int_0^1 \theta_2(x,\chi)x^{\frac{s-1}{2}}dx$$
$$= \frac{1}{2}\int_1^\infty \theta_2(x,\chi)x^{\frac{s-1}{2}}dx + \frac{1}{2}\int_1^\infty \theta_2\left(\frac{1}{x},\chi\right)x^{\frac{-s-3}{2}}dx$$
$$= \frac{1}{2}\int_1^\infty \theta_2(x,\chi)x^{\frac{s-1}{2}}dx + \frac{iq^{\frac{1}{2}}}{2\tau(\overline{\chi})}\int_1^\infty \theta_2(x,\overline{\chi})x^{-\frac{s}{2}}dx.$$

La igualdad en todo el plano se sigue de que dichas integrales están bien definidas para cualquier $s \in \mathbb{C}$ ya que θ_1 y θ_2 decaen de manera exponencial. ■

Teorema 2.23 (Ecuación funcional de las funciones L)**.** *Dado χ caracter primitivo se cumple la igualdad*

$$\frac{q^{\frac{1-s}{2}}}{\pi^{\frac{1-s}{2}}}\Gamma\left(\frac{1-s}{2}\right)L(1-s,\overline{\chi}) = \frac{q^{\frac{s+1}{2}}}{\tau(\chi)\pi^{\frac{s}{2}}}\Gamma\left(\frac{s}{2}\right)L(s,\chi) \qquad \textit{si } \chi(-1)=1,$$

$$\frac{q^{1-\frac{s}{2}}}{\pi^{1-\frac{s}{2}}}\Gamma\left(1-\frac{s}{2}\right)L(1-s,\overline{\chi}) = \frac{iq^{\frac{s}{2}+1}}{\tau(\chi)\pi^{\frac{s+1}{2}}}\Gamma\left(\frac{s+1}{2}\right)L(s,\chi) \qquad \textit{si } \chi(-1)=-1.$$

Demostración. Para cualquier caracter primitivo se tiene que

$$\overline{\chi}(1)\tau(\chi)\cdot\chi(-1)\tau(\overline{\chi}) = \sum_{m=1}^{q}\chi(m)e^{\frac{2\pi i m}{q}}\sum_{m=1}^{q}\overline{\chi}(m)e^{-\frac{2\pi i m}{q}} = \left|\sum_{m=1}^{q}\chi(m)e^{\frac{2\pi i m}{q}}\right|^2 > 0.$$

Si $\chi(-1)=1$, entonces $\tau(\chi)\tau(\overline{\chi})=q$ y, si $\chi(-1)=-1$, entonces $\tau(\chi)\tau(\overline{\chi})=-q$. Usando estas igualdades y el Teorema 2.22, se concluye. ■

Teorema 2.24. *Para cualquier χ caracter primitivo la función $L(s,\chi)$ es libre de ceros en la región $\Re(s)>1$. Si $\chi(-1)=1$, entonces los ceros de $L(s,\chi)$ en la región $\Re(s)<0$ son los puntos $s \in \{0,-2,-4,-6,\dots\}$; y si $\chi(-1)=-1$, son los puntos $s \in \{-1,-3,-5,\dots\}$.*

Demostración. Como se vio en la demostración de la Identidad de Euler (Teorema 2.15), se tiene que $L(s,\chi)\neq 0$ en $\Re(s)>1$. Por el Teorema 2.23 es claro que los ceros en la región $\Re(s)<0$ coincide con los polos de $\Gamma\left(\frac{s}{2}\right)$ o de $\Gamma\left(\frac{s+1}{2}\right)$, dependiendo el caso, ya que en dicha región $L(1-s,\overline{\chi})$ no genera ceros. El resultado se sigue de los ceros que genera la función Γ. ■

Definición 2.25. Para cualquier caracter primitivo se define la función $\xi(s,\chi)$ como

$$\xi(s,\chi) = \left(\frac{\pi}{q}\right)^{-\frac{1}{2}(s+a_\chi)}\Gamma\left(\frac{1}{2}(s+a_\chi)\right)L(s,\chi),$$

donde

$$a_\chi = \frac{1-\chi(-1)}{2} = \begin{cases} 0 & \text{si } \chi(-1)=1,\\ 1 & \text{si } \chi(-1)=-1.\end{cases}$$

Corolario 2.26 (Ecuación funcional de la función $\xi(x,\chi)$)**.** *Para cualquier caracter primitivo χ se cumple la igualdad*

$$\xi(1-s,\overline{\chi}) = \frac{i^{a_\chi} q^{\frac{1}{2}}}{\tau(\chi)} \xi(s,\chi).$$

2.3. Identidad de Vaughan

Definición 2.27. Se define la función Λ de Von Mangoldt, $\Lambda : \mathbb{N} \to \mathbb{R}$, como

$$\Lambda(n) = \begin{cases} \log p & \text{si } n = p^\alpha \text{ para algún } p \text{ primo y } \alpha \text{ entero,} \\ 0 & \text{en otro caso.} \end{cases}$$

La identidad de Vaughan es un método para aproximar sumas del tipo $\sum_{n \leqslant N} f(n)\Lambda(n)$, donde f es una función aritmética.

Definición 2.28. Se definen las funciones $\Lambda_i(n)$, para $i \in \{1,2,3,4\}$, como

$$\Lambda_1(n) = \begin{cases} \Lambda(n) & \text{si } n \leqslant U, \\ 0 & \text{si } n > U, \end{cases} \qquad \Lambda_2(n) = -\sum_{\substack{md \mid n \\ m \leqslant U \\ d \leqslant V}} \Lambda(m)\mu(d),$$

$$\Lambda_3(n) = \sum_{\substack{hd = n \\ d \leqslant V}} \mu(d)\log(h), \qquad \Lambda_4(n) = -\sum_{\substack{mk = n \\ m > U \\ k > 1}} \Lambda(m) \sum_{\substack{d \mid k \\ d \leqslant V}} \mu(d),$$

para cualesquiera U, V números positivos.

Teorema 2.29 (Teorema de Unicidad de Series de Dirichlet)**.** *Sean $F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ y $G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s}$ dos series de Dirichlet absolutamente convergentes en el semiplano complejo $\Re(s) > \sigma_0$. Si $F(s) = G(s)$ en $\Re(s) > \sigma_0$, entonces $f(n) = g(n)$ para todo $n \in \mathbb{N}$.*

Demostración. Sea $h(n) = f(n) - g(n)$, y sea $s = \sigma + it$ con $\sigma > c > \sigma_0$. Supongamos que N es el mínimo natural tal que $h(N) \neq 0$, entonces

$$0 = F(s) - G(s) = \frac{h(n)}{N^s} \sum_{n=N+1}^{\infty} \frac{h(n)}{n^s}.$$

Por lo tanto,

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

y haciendo tender σ a ∞, se concluye la demostración. ∎

Teorema 2.30 (Identidad de Vaughan)**.** *Para cualquier función aritmética f se tiene la igualdad*

$$\sum_{n\leqslant N} f(n)\Lambda(n) = S_1 + S_2 + S_3 + S_4,$$

donde

$$S_i = \sum_{n\leqslant N} f(n)\Lambda_i(n).$$

Demostración. Claramente bastaría demostrar que $\Lambda(n) = \Lambda_1(n) + \Lambda_2(n) + \Lambda_3(n) + \Lambda_4(n)$ para cualquier $n \in \mathbb{N}$. Sean $U, V \leqslant N$ y $s \in \mathbb{C}$ con $Re(s) > 1$. Sean

$$F(s) = \sum_{m\leqslant U} \frac{\Lambda(m)}{m^s} \qquad y \qquad G(s) = \sum_{d\leqslant V} \frac{\mu(d)}{d^s}.$$

Es claro que

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

La derivada logarítmica de la Identidad de Euler de la función ζ (Teorema 2.1) es

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

entonces

$$\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = \sum_{m\leqslant U} \frac{\Lambda(s)}{m^s} - \left(\sum_{r=1}^{\infty} \frac{1}{r^s}\right)\left(\sum_{m\leqslant U} \frac{\Lambda(m)}{m^s}\right)\left(\sum_{d\leqslant V} \frac{\mu(d)}{d^s}\right) + \left(\sum_{r=1}^{\infty} \frac{\log r}{r^s}\right)\left(\sum_{d\leqslant V} \frac{\mu(d)}{d^s}\right)$$
$$+ \left(\sum_{r=1}^{\infty} \frac{\Lambda(r)}{r^s} - \sum_{m\leqslant U} \frac{\Lambda(m)}{m^s}\right)\left(1 - \left(\sum_{k=1}^{\infty} \frac{1}{k^s}\right)\left(\sum_{d\leqslant V} \frac{\mu(d)}{d^s}\right)\right).$$

De lo anterior se deduce que

i] $$\sum_{m\leqslant U} \frac{\Lambda(s)}{m^s} = \sum_{n=1}^{\infty} \frac{\Lambda_1(n)}{n^s}.$$

ii] $$-\left(\sum_{r=1}^{\infty} \frac{1}{r^s}\right)\left(\sum_{m\leqslant U} \frac{\Lambda(m)}{m^s}\right)\left(\sum_{d\leqslant V} \frac{\mu(d)}{d^s}\right) = -\sum_{n=1}^{\infty} \sum_{\substack{rmd=n \\ m\leqslant U \\ d\leqslant V}} \frac{\Lambda(m)\mu(d)}{(mdr)^s} = \sum_{n=1}^{\infty} \frac{\Lambda_2(n)}{n^s}.$$

iii] $$\left(\sum_{r=1}^{\infty} \frac{\log r}{r^s}\right)\left(\sum_{d\leqslant V} \frac{\mu(d)}{d^s}\right) = \sum_{n=1}^{\infty} \sum_{\substack{hd=n \\ d\leqslant V}} \frac{\mu(d)\log h}{(dh)^s} = \sum_{n=1}^{\infty} \frac{\Lambda_3(n)}{n^s}.$$

iv] $$\left(\sum_{r=1}^{\infty} \frac{\Lambda(r)}{r^s} - \sum_{m\leqslant U} \frac{\Lambda(m)}{m^s}\right)\left(1 - \left(\sum_{k=1}^{\infty} \frac{1}{k^s}\right)\left(\sum_{d\leqslant V} \frac{\mu(d)}{d^s}\right)\right) = \left(\sum_{r>U} \frac{\Lambda(r)}{r^s}\right)\left(-\sum_{\substack{k=1 \\ d\leqslant V \\ kd>1}}^{\infty} \frac{\mu(d)}{(kd)^s}\right)$$

$$= \sum_{\substack{r>U\\ d\leqslant V\\ kd\neq 1}} \frac{\Lambda(r)\mu(d)}{(rkd)^s} = -\sum_{\substack{r>U\\ m>1}} \frac{\Lambda(r)}{(rm)^s}\left(\sum_{\substack{d|m\\ d\leqslant V}} \mu(d)\right) = -\sum_{n=1}^{\infty} \frac{1}{n^s}\left(\sum_{\substack{mk=n\\ m>U\\ k>1}} \Lambda(m)\left(\sum_{\substack{d|k\\ d\leqslant V}} \mu(d)\right)\right)$$
$$= \sum_{n=1}^{\infty} \frac{\Lambda_4(n)}{n^s}.$$

Por la unicidad de los coeficientes de las series de Dirichlet (Teorema 2.29) se sigue que

$$\Lambda(n) = \Lambda_1(n) + \Lambda_2(n) + \Lambda_3(n) + \Lambda_4(n),$$

con lo que se concluye la demostración. ∎

2.4. La Fórmula de Dirichlet para el Número de Clases

Una *forma cuadrática* $F(x,y)$ es una expresión de la forma $F(x,y) = ax^2 + bxy + cy^2$, donde $a,b,c \in \mathbb{Z}$. El *discriminante* de una forma cuadrática está definido por $\Delta_F = b^2 - 4ac$. Otra forma de representar una forma cuadrática es con la expresión

$$F(x,y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},$$

Dada $g = \begin{pmatrix} \alpha & \beta \\ \kappa & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$ se define como gF a la forma

$$gF(x,y) = \begin{pmatrix} x & y \end{pmatrix} g^T \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} g \begin{pmatrix} x \\ y \end{pmatrix}.$$

Definición 2.31. Se dice que una forma cuadrática F *representa* al entero n si existen enteros x_1, y_1 tales que $F(x_1, y_1) = n$.

Definición 2.32. Se dice que dos formas cuadráticas $F_1(x,y)$ y $F_2(x,y)$ son *equivalentes* si existe $g \in SL_2(\mathbb{Z})$ tal que $F_2 = gF_1$. Esto se denotará por $F_1 \sim F_2$.

No es difícil ver que la equivalencia de formas cuadráticas es una relación de equivalencia y que, si dos formas son equivalentes entonces tienen el mismo discriminante. Además, es claro que dos formas equivalentes representan a los mismos enteros.

Notemos que los posibles discriminantes son $\Delta = b^2 - 4ac \equiv 0, 1 (\bmod 4)$ y, para cada uno de estos, existe al menos una forma cuadrática dada por

$$F(x,y) = \begin{cases} x^2 - \frac{\Delta}{4}y^2 & \text{si } \Delta \equiv 0 (\bmod 4), \\ x^2 + xy + \frac{1-\Delta}{4}y^2 & \text{si } \Delta \equiv 1 (\bmod 4). \end{cases}$$

A estas formas se les llama formas principales.

Teorema 2.33. *Sea $\Delta \in \mathbb{Z}$ no cuadrado perfecto. Entonces hay un número finito de clases de equivalencia de formas cuadráticas de discriminante Δ.*

Demostración. Sea $F(x,y) = ax^2 + bxy + cy^2$ una forma cuadrática con discriminante Δ. Sea $A_0 = \{j \in \mathbb{Z}\backslash\{0\} : j \text{ se puede representar por } F\}$ y $a' = \text{mín}\{|a| : a \in A_0\}$, entonces existen α, κ enteros primos relativos entre si tales que $a' = a\alpha^2 + b\alpha\kappa + c\kappa^2$. Sean β y δ enteros tales que $\alpha\delta - \beta\kappa = 1$, y defínase

$$G = \begin{pmatrix} \alpha & \beta \\ \kappa & \delta \end{pmatrix} F \sim F.$$

Si $G(x,y) = a'x^2 + b''xy + c''y^2$, entonces por la minimalidad de a', se tiene que $|a'| \leqslant |c''|$. Sea n tal que $|b'' - 2a'n| \leqslant |a'|$ y sea $H = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} G$, entonces $H \sim F$ y

$$H(x,y) = a'x^2 + (b'' - 2a'n)xy + (a'n^2 - b''n + c'')y^2 = a'x^2 + b'xy + c'y^2,$$

donde $|b'| \leqslant |a'| \leqslant |c'|$. Nótese que $|\Delta| = |(b')^2 - 4a'c'| \geqslant 4|a'c'| - |b'|^2 \geqslant 3|a'|^2$. Por lo tanto, $|a'|$ y $|b'|$ esán acotados por $\sqrt{\frac{|\Delta|}{3}}$ y c' se determina de manera única por a', b'. Entonces hay una cantidad finita de relaciones de equivalencia con determinante Δ. ■

De aquí en adelante sólo se considerarán formas cuadráticas con $|b| \leqslant |a| \leqslant |c|$, y con $a \neq 0$. Se dirá que una forma cuadrática $F(x,y) = ax^2 + bxy + cy^2$ es *primitiva* si $(a,b,c) = 1$. Además se dirá que F es *indefinida* si su discriminante es positivo; *positiva definida* si $\Delta_F < 0$ y $a > 0$; y *negativa definida* si $\Delta_F < 0$ y $a < 0$.

Definición 2.34. Para cada determinante Δ no cuadrado perfecto, se define el *número de clase* como

$$h(\Delta) = \begin{cases} \text{la cantidad de clases de equivalencia de formas cuadráticas} & \\ \text{primitivas con discriminante } \Delta & \text{si } \Delta > 0, \\ \text{la cantidad de clases de equivalencia de formas cuadráticas} & \\ \text{primitivas positivo definidas con discriminante } \Delta & \text{si } \Delta < 0. \end{cases}$$

Si todas las formas cuadráticas de discriminante Δ son primitivas, se dirá que Δ es un *discriminante fundamental.*

Proposición 2.35. *$\Delta \in \mathbb{Z}$ es un discriminante fundamental si y sólo si $\Delta \neq m^2k$ para todo $m > 1$ y $k \equiv 0, 1(mod\ 4)$.*

Demostración. Si $\Delta = m^2k$ para algún $m > 1$ y $k \equiv 0, 1 (\text{mod } 4)$ entonces no es un discriminante fundamental. Para ver esto, basta con tomar la forma principal de discriminante k y multiplicar sus coeficientes por m, lo cual resulta en una forma no primitiva de discriminante Δ.

Si $\Delta \neq m^2k$ para cualquier $m > 1$ y $k \equiv 0, 1(\text{mod } 4)$ entonces es un discriminante fundamental. Supóngase que no lo es, entonces una forma cuadrática $ax^2 + bxy + cy^2$ no primitiva de discriminante Δ, entonces $(a,b,c) = l > 1$, y así $\Delta = l^2\left(\left(\frac{b}{l}\right)^2 - 4\frac{ac}{l^2}\right)$, lo que es una contradicción. ■

Definición 2.36. Se dice que una forma cuadrática F *representa propiamente* a un entero n si existen $x, y \in \mathbb{Z}$ primos relativos entre si tales que $F(x, y) = n$.

Proposición 2.37. *Dada una forma cuadráitca $F(x, y) = ax^2 + bxy + cy^2$ y $n \in \mathbb{Z}$, las siguientes afirmaciones son equivalentes:*

i] F representa propiamente a n,

ii] F es equivalente a una forma cuadrática $G = nx^2 + mxy + ly^2$, con $m^2 \equiv \Delta(mod\ 4n)$ y $0 \leqslant m < 2n$, donde Δ es el discriminante de F.

Demostración. ii]$\Rightarrow$ i] Si $G(x, y) = nx^2 + mxy + ly^2$ y $\begin{pmatrix} \alpha & \beta \\ \kappa & \delta \end{pmatrix} F = G$, entonces F representa a n, ya que como $n = G(1, 0)$ se tiene que $F(1\alpha + 0\beta, 1\kappa + 0\delta) = G(1, 0) = n$.

i]$\Rightarrow$ ii] Si F representa propiamente a n, entonces existen enteros α, κ coprimos tales que $n = a\alpha^2 + b\alpha\kappa + c\kappa^2$. Sean β, δ tales que $\alpha\delta - \beta\kappa = 1$, entonces

$$F \sim \begin{pmatrix} \alpha & \beta \\ \kappa & \delta \end{pmatrix} F = \begin{pmatrix} n & \frac{m'}{2} \\ \frac{m'}{2} & l'. \end{pmatrix}$$

La congruencia buscada se cumple ya que $\Delta = (m')^2 - 4l'n$. Sea N tal que $0 \leqslant m' - 2nN < n$, entonces tomando $H = \begin{pmatrix} 1 & -N \\ 0 & 1 \end{pmatrix} G \sim F$ se concluye. ∎

Teorema 2.38. *Sean $k, \Delta \in \mathbb{Z}$ con $k > 0$ y $(k, \Delta) = 1$. El número de soluciones módulo $4k$ de la ecuación $x^2 \equiv \Delta(mod\ 4k)$ es*

$$2 \sum_{\substack{t|k \\ t \text{ libre de} \\ \text{cuadrados}}} \left(\frac{\Delta}{t}\right),$$

donde $\left(\frac{a}{b}\right)$ representa al símbolo de Kronecker.

Demostración. En el caso de que Δ sea impar se tiene que $\Delta \equiv 1(\text{mod } 4)$. Sea k primo relativo a Δ, entonces $(\Delta, 4k) = 1$. Se tiene entonces que para cualquier potencia de primo p^l que divida a $4k$, el número de soluciones de la congruencia $x^2 \equiv \Delta(\text{mod } 4k)$ es

$$\begin{array}{cl} 2 & \text{si } p = 2, l = 2, \\ 2\left(1 + \left(\frac{d}{p}\right)\right) & \text{si } p = 2, l > 2, \\ \left(1 + \left(\frac{d}{p}\right)\right) & \text{si } p > 2. \end{array}$$

Por el Teorema Chino del Residuo se puede deducir que, en este caso, el número de soluciones de $x^2 \equiv \Delta(\text{mod } 4k)$ es

$$2 \prod_{\substack{p|k \\ p \text{ primo}}} \left(1 + \left(\frac{\Delta}{p}\right)\right) = 2 \sum_{\substack{t|k \\ t \text{ libre de} \\ \text{cuadrados}}} \left(\frac{\Delta}{t}\right).$$

En caso de que Δ sea par, se tiene que k es impar y $4|\Delta$. Entonces hay dos soluciones de $x^2 \equiv \Delta(\text{mod } 4)$, y $\left(1 + \left(\frac{\Delta}{p}\right)\right)$ soluciones de $x^2 \equiv \Delta(\text{mod } p^l)$ para cada primo divisor de k. Por

Teorema Chino del Residuo se deduce que en este caso hay

$$2\prod_{\substack{p|k\\ p \text{ primo}}}\left(1+\left(\frac{\Delta}{p}\right)\right)=2\sum_{\substack{t|k\\ t\text{ libre de}\\ \text{cuadrados}}}\left(\frac{\Delta}{t}\right)$$

soluciones de la congruencia $x^2 \equiv \Delta (\text{mod } 4k)$. ■

Sea F una forma cuadrática de discriminante Δ. Por la Proposición 2.37, para cada k que F representa propiamente, existe un entero l único tal que $l^2 \equiv \Delta(\text{mod } 4k)$ y $0 \leqslant l < 2k$.

Para un discriminante fijo Δ, se denotará por $F_1, F_2, \ldots, F_{h(\Delta)}$ a un sistema de representantes de las clases de equivalencia de formas cuadráticas primitivas de discriminante Δ (en caso de que $\Delta < 0$, se consideran únicamente las positivo definidas), y supondremos, sin pérdida de generalidad, que el coeficiente de x^2 de cada uno de estos representantes es positivo.

Dado k, se denotará por $\mathcal{R}_\Delta(k)$ al número de representantes de las clases de equivalencia de formas cuadráticas primitivas de discriminante Δ que representan a k.

Definición 2.39. Se dirá que $g \in SL_2(\mathbb{Z})$ es una *transformación automorfa* de la forma cuadrática F si $gF = F$.

Teorema 2.40. *Sea $F(x,y) = ax^2 + bxy + cy^2$ una forma cuadrática primitiva de discriminante Δ. Las transformaciones automorfas de F están dadas por las matrices*

$$\begin{pmatrix} \frac{t-bu}{2} & -cu \\ au & \frac{t+bu}{2} \end{pmatrix},$$

donde t, u son solución de la Ecuación de Pell $t^2 - \Delta u^2 = 4$.

Demostración. Sean t, u soluciones de $t^2 - \Delta u^2 = 4$. Como $t^2 - \Delta u^2 \equiv 0(\text{mod } 2)$, $b \equiv \Delta(\text{mod } 2)$ y $t + \Delta u \equiv t^2 \pm \Delta u^2(\text{mod } 2)$ se tiene que $\frac{t\pm bu}{2} \in \mathbb{Z}$. Por otro lado, como

$$\frac{t-bu}{2}\frac{t+bu}{2} + au \cdot cu = \frac{t^2 + (4ac - b^2)u^2}{4} = \frac{t^2 - \Delta u^2}{4} = 1,$$

se tiene que

$$g := \begin{pmatrix} \frac{t-bu}{2} & -cu \\ au & \frac{t+bu}{2} \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Podemos escribir entonces

$$\begin{aligned} gF(x,y) &= a\left(\frac{t-bu}{2}x - cuy\right)^2 + b\left(\frac{t-bu}{2}x - cuy\right)\left(aux + \frac{t+bu}{2}y\right) + c\left(aux + \frac{t+bu}{2}y\right)^2 \\ &= a_1x^2 + b_1xy + c_1y^2. \end{aligned}$$

Notemos que

$$a_1 = a\left(\frac{t-bu}{2}\right)^2 + b\left(\frac{t-bu}{2}\right)(au) + c(au)^2 = \frac{a}{4}(t^2 - (bu)^2 + 4acu^2) = \frac{a}{4}(t^2 - \Delta u^2) = a$$

$$\begin{aligned} b_1 &= 2a\left(\frac{t-bu}{2}(-cu)\right)+b\left[\left(\frac{t^2-(bu)^2}{4}\right)-acu^2\right]+2c(au)\left(\frac{t+bu}{2}\right) \\ &= 2auc(bu)+\frac{b}{4}\left[t^2-b^2u^2-4acu^2\right]=\frac{b}{4}(t^2-b^2u^2+4acu^2)=\frac{b}{4}(t^2-\Delta u^2)=b, \end{aligned}$$

y despejando del discriminante, $c_1 = c$. Por lo tanto, g es una transformación automorfa de F.

Ahora, dada $g = \begin{pmatrix} r & s \\ m & n \end{pmatrix}$ una transformación automorfa de F, se tiene que

$$ax^2+bxy+cy^2 = F(x,y) = gF(x,y) = a(rx+sy)^2+b(rx+sy)(mx+ny)+c(mx+ny)^2,$$

de donde $a = ar^2+brm+cm^2$, $b = 2ars+b(rn+sm)+2cmn$ y $c = as^2+bsn+cn^2$. Por la igualdad de b y como $rn-sm = 1$ se tiene que $0 = ars+bsm+cmn$. De estas ecuaciones se deduce que

$$as = ar^2s+brms+cm^2s = cm(ms-nr) = -cm,$$

y

$$an = ar^2n+brmn+cm^2n = ar(rn-sm)+bm(rn-sm) = ar+bm,$$

entonces $a(n-r) = bm$. Entonces $a|cm$ y $a|bm$, y como $(a,b,c) = 1$ por ser primitiva, se deduce que $a|m$, y por lo tanto $m = au$ para algún entero u. Como $as = -cm = -cau$ se tiene que $s = -cu$, y como $a(n-r) = bm = bau$ se tiene que $n-r = bu$, entonces

$$(n+r)^2 = (n-r)^2+4nr = b^2u^2+4(1+sm) = b^2u^2+4-4acu^2 = \Delta u^2+4.$$

Sea $t = n+r$, entonces $t^2-\Delta u^2 = 4$ y $n = \frac{t+bu}{2}$ y $r = \frac{t-bu}{2}$, de donde se ve que la matriz g es de la forma que se buscaba demostrar. ■

Es claro de aquí que, el número de transformaciones automorfas para cada forma cuadrática F de discriminante Δ es:

$$2 \text{ si } \Delta < -4, \qquad 4 \text{ si } \Delta = -4, \qquad 6 \text{ si } \Delta = -3, \qquad \infty \text{ si } \Delta > 0.$$

Denotaremos por W_Δ a dicho número, pero en el caso $\Delta > 0$ se considerará $W_\Delta = 1$. En el caso de que $\Delta > 0$ se denotará a la solución fundamental $t+u\sqrt{\Delta}$ de la ecuación de Pell $t^2-\Delta u^2 = 4$ por ϵ_Δ.

Proposición 2.41. *Si $k \in \mathbb{Z}$ se puede representar por la forma cuadrática F de discriminante $\Delta > 0$, entonces existe una única representación $F(x,y)$ tal que $1 \leqslant \frac{2ax+(b+\sqrt{\Delta})y}{2ax+(b-\sqrt{\Delta})y} < \epsilon_\Delta^2$.*

Demostración. Sean $\theta = \frac{-b+\Delta}{2a}$ y $\theta' = \frac{-b-\sqrt{\Delta}}{2a}$, y sea $t_0+u_0\sqrt{\Delta} = \epsilon_\Delta$. Notemos primero que $ax^2+bxy+cy^2 = a(x-\theta y)(x-\theta' y)$. Supongamos que $F(x,y) = F(X,Y) = k$, con $x,y,X,Y > 0$, entonces $(X,Y) = g(x,y)$, donde g es una transformación automorfa de F como la descrita en el Teorema 2.40. De aquí se puede deducir que $x-\theta y = \frac{1}{2}(t-u\sqrt{\Delta})(X-\theta Y)$ y que

$x - \theta' y = \frac{1}{2}(t + u\sqrt{\Delta})(X - \theta' Y)$, y donde $t + u\sqrt{\Delta} = \epsilon_\Delta^m$ para alguna $m > 0$. Entonces

$$\frac{x - \theta' y}{x - \theta y} = \frac{\frac{1}{2}(t + u\sqrt{\Delta})(X - \theta' Y)}{\frac{1}{2}(t - u\sqrt{\Delta})(X - \theta Y)} = \epsilon_\Delta^{2m} \frac{X - \theta' Y}{X - \theta Y}.$$

De esto se sigue claramente la demostración. ∎

Observación 2.42. Sea $k \in \mathbb{Z}$ un entero representado propiamente por F, y sean x_0, y_0 enteros primos relativos entre si tales que $F(x_0, y_0) = k$. Entonces, existen únicos enteros r, l, s con $l^2 \equiv \Delta (\text{mod } 4k)$, $0 \leqslant l < 2k$ y $sx_0 - ry_0 = 1$ tales que

$$\begin{pmatrix} x_0 & r \\ y_0 & s \end{pmatrix} F = kX^2 + lXY + mY^2$$

y $l^2 - \Delta = 4km$.

Proposición 2.43. *Sea $l \in \mathbb{Z}$ tal que $l^2 \equiv \Delta(mod\ 4k)$ con $0 \leqslant l < 2k$ con $\Delta < 0$, entonces existen exáctamente W_Δ representaciones propias de k asociadas a l.*

Demostración. Sea k solución de la forma cuadrática $F(x, y)$ positivo definida con discriminante $\Delta < 0$. Consideremos $F_1, \ldots, F_{h(\Delta)}$ un sistema de representantes de formas primitivas positivo definida de discriminante Δ, y sea l que cumpla las hipótesis del enunciado. Consideremos la forma $G(x, y) = kx^2 + lxy + my^2$ de discriminante Δ, entonces G es equivalente a exáctamente una de las formas del sistema de representantes, digamos $G = gF_1$, entonces F_1 representa propiamente a k, y las representaciones de k asociadas a l provienen de F. De aquí que hay una biyección entre las representaciones propias de k asociadas a l y las matrices g tales que $gF_1 = G$. Nótese que cualquier matriz que cumpla lo anterior es de la forma gh, donde h es una matriz automorfa a F_1. Entonces hay W_Δ representaciones propias de k asociadas a l. ∎

Teorema 2.44. *Dados $k \in \mathbb{N}$ y $\Delta \in \mathbb{Z}$ con $(\Delta, k) = 1$, se tiene la igualdad*

$$\mathcal{R}_\Delta(k) = W_\Delta \sum_{t \mid k} \left(\frac{\Delta}{t} \right).$$

Demostración. El número de representaciones propias de k por las formas del sistema reducido es

$$W_\Delta \cdot \#\{l : l^2 \equiv \Delta (\text{mod } 4k), 0 \leqslant l < 2k\} = W_\Delta \sum_{\substack{t \mid k \\ t \text{ libre de} \\ \text{cuadrados}}} \left(\frac{\Delta}{t} \right).$$

Las representaciones impropias se deducen de la misma forma, considerando los enteros de la forma $\frac{\Delta}{a^2}$. Entonces

$$\mathcal{R}_\Delta(k) = W_\Delta \sum_{\substack{a > 0 \\ a^2 \mid k}} \sum_{\substack{t \mid \frac{k}{a^2} \\ t \text{ libre de} \\ \text{cuadrados}}} \left(\frac{\Delta}{t} \right) = W_\Delta \sum_{\substack{a > 0 \\ a^2 \mid k}} \sum_{\substack{t \mid \frac{k}{a^2} \\ t \text{ libre de} \\ \text{cuadrados}}} \left(\frac{\Delta}{ta^2} \right) = W_\Delta \sum_{t \mid k} \left(\frac{\Delta}{t} \right).$$

■

Recordemos que cada caracter de Dirichlet real primitivo se puede representar por el símbolo de Kronecker $\chi_\Delta(n) = \left(\frac{\Delta}{n}\right)$. Se denotará por

$$H_\Delta(N) = \sum_{\substack{1 \leqslant k \leqslant N \\ (k,\Delta)=1}} \mathcal{R}_\Delta(k).$$

Proposición 2.45. *Dado $\Delta \in \mathbb{Z}$ se tiene que*

$$\lim_{N\to\infty} \frac{H_\Delta(N)}{N} = W_\Delta \frac{\varphi(|\Delta|)}{|\Delta|} L(1, \chi_\Delta).$$

Demostración. Denotemos por $A(N;\Delta,n) = \sum_{\substack{1 \leqslant k \leqslant \frac{N}{n} \\ (k,\Delta)=1}} 1$. Se tiene que

$$\frac{H_\Delta(N)}{W_\Delta \cdot N} = \frac{1}{W_\Delta \cdot N} \sum_{\substack{1 \leqslant k \leqslant N \\ (k,\Delta)=1}} \mathcal{R}_\Delta(k) = \frac{1}{N} \sum_{\substack{1 \leqslant k \leqslant N \\ (k,\Delta)=1}} \sum_{n|k} \left(\frac{\Delta}{n}\right)$$

$$= \frac{1}{N} \sum_{n=1}^{\infty} \left(\frac{\Delta}{n}\right) \sum_{\substack{1 \leqslant k \leqslant \frac{N}{n} \\ (k,\Delta)=1}} 1 = \sum_{n=1}^{\infty} \left(\frac{\Delta}{n}\right) \frac{A(N;\Delta,n)}{N}.$$

Notemos que

$$A(N;\Delta,n) = \sum_{\substack{1 \leqslant k \leqslant \frac{N}{n} \\ (k,\Delta)=1}} 1 = \sum_{1 \leqslant k \leqslant \frac{N}{n}} \sum_{j|(k,\Delta)} \mu(j) = \sum_{j|\Delta} \sum_{\substack{1 \leqslant k \leqslant \frac{N}{n} \\ j|k}} \mu(j) = \sum_{j|\Delta} \mu(j) \left\lfloor \frac{N}{nj} \right\rfloor$$

$$= \frac{N}{n} \sum_{j|\Delta} \frac{\mu(j)}{j} + O(\Delta) = \frac{N}{n} \frac{\varphi(|\Delta|)}{|\Delta|} + O(\Delta).$$

Podemos deducir entonces que

$$\lim_{N\to\infty} \frac{A(N;\Delta,n)}{N} = \lim_{N\to\infty} \frac{\varphi(|\Delta|)}{n|\Delta|} + \frac{O(|\Delta|)}{N} = \frac{\varphi(|\Delta|)}{n|\Delta|},$$

para finalmente concluir que

$$\lim_{N\to\infty} \frac{H_\Delta(N)}{N} = W_\Delta \lim_{N\to\infty} \sum_{n=1}^{\infty} \left(\frac{\Delta}{n}\right) \frac{A(N;\Delta,n)}{N} = W_\Delta \frac{\varphi(|\Delta|)}{|\Delta|} L(1, \chi_\Delta).$$

■

Ahora, se denotará por $\mathcal{R}_\Delta(k, F)$ al número de representaciones de k por una forma cuadrática F fija, y se define $H_\Delta(N,F) = \sum_{\substack{1\leqslant k\leqslant N\\(k,\Delta)=1}} \mathcal{R}_\Delta(k,F)$. Es claro que $\mathcal{R}_\Delta(k) = \sum_{n=1}^{h(\Delta)} \mathcal{R}_\Delta(k,F_n)$. Veremos ahora que $\lim_{N\to\infty} \frac{H_\Delta(N,F_n)}{N}$ existe y depende únicamente de Δ.

Lema 2.46. *Sea $m \in \mathbb{N}$ y sea E una elipse o un sector de una hipérbola, centrada en el origen. Sea I el área de E. Si a E se le aplica la transformación $T : \mathbb{R}^2 \to \mathbb{R}^2$ tal que $T(x,y) = (\sqrt{c}x, \sqrt{c}y)$; y $U(c)$ es el número de puntos enteros en $T(E)$ tales que*

$$x \equiv x_0(mod\ m) \qquad y \qquad y \equiv y_0(mod\ m)$$

para algunos $x_0, y_0 \in \mathbb{Z}$ fijos, entonces

$$\lim_{c\to\infty} \frac{U(c)}{c} = \frac{I}{m^2}.$$

Demostración. Consideremos la cuadrícula formada por las rectas $x = \frac{x_0+rm}{\sqrt{c}}, y = \frac{y_0+sm}{\sqrt{c}}$. Sea $J(c)$ el número de estos cuadrados que tienen su vértice inferior izquierdo en E, entonces $J(c) = U(c)$. Luego

$$I = \int\int_E dxdy = \lim_{c\to\infty} J(c)\frac{m^2}{c},$$

de donde se concluye que $\frac{I}{m^2} = \lim_{c\to\infty} \frac{U(c)}{c}$. ∎

Proposición 2.47. *Dado $\Delta \in \mathbb{Z}$ se cumple la igualdad*

$$\lim_{N\to\infty} \frac{H_\Delta(N,F)}{N} = \begin{cases} \frac{2\pi}{\sqrt{|\Delta|}}\frac{\varphi(|\Delta|)}{|\Delta|} & si\ \Delta < 0,\\ \frac{\log\epsilon_\Delta}{\sqrt{\Delta}}\frac{\varphi(\Delta)}{\Delta} & si\ \Delta > 0.\end{cases}$$

Demostración. Consideremos primero el caso $\Delta < 0$. Sea $U(c,x_0,y_0)$ el número de soluciones de $0 \leqslant F(x,y) \leqslant c$, con $x \equiv x_0(\text{mod } |\Delta|)$ y $y \equiv y_0(\text{mod } |\Delta|)$. Entonces

$$H_\Delta(T,F) = \sum_{\substack{1\leqslant k\leqslant c\\(k,\Delta)=1}} R_\Delta(k,F) = \sum_{\substack{x,y(\text{mod } |\Delta|)\\(F(x,y),\Delta)=1}} U(c,x,y).$$

El área de la región $|F(x,y)| \leqslant 1$ es $\frac{2\pi}{\sqrt{|\Delta|}}$ y, por lo tanto,

$$\lim_{c\to\infty}\frac{H_\Delta(c,F)}{c} = \lim_{c\to\infty}\sum_{\substack{x,y(\text{mod } |\Delta|)\\(F(x,y),\Delta)=1}}\frac{U(c,x,y)}{c} = \sum_{\substack{x,y(\text{mod } |\Delta|)\\(F(x,y),\Delta)=1}}\frac{2\pi}{|\Delta|^{5/2}} = \varphi(|\Delta|)|\Delta|\frac{2\pi}{|\Delta^{5/2}|} = \frac{2\pi\varphi(|\Delta|)}{|\Delta|^{3/2}}.$$

Ahora consideremos el caso $\Delta > 0$. Sea $U(c,x_0,y_0)$ el número de soluciones de $0 \leqslant F(x,y) \leqslant c$, con $x \equiv x_0(\text{mod } \Delta), y \equiv y_0(\text{mod } \Delta)$ y $1 \leqslant |\frac{L}{L'}| < \epsilon_\Delta^2$, donde $L = 2ax + (b+\sqrt{\Delta})y$ y

$L' = 2ax + (b - \sqrt{\Delta})y$. Por el Teorema 2.41 podemos deducir que

$$H_\Delta(T, F) = \sum_{\substack{1 \leqslant k \leqslant c \\ (k,\Delta)=1}} R_\Delta(k, F) = \sum_{\substack{x,y (\mathrm{mod}\ |\Delta|) \\ (F(x,y),\Delta)=1 \\ 1 \leqslant \frac{L}{L'} \leqslant \epsilon_\Delta^2}} U(c, x, y).$$

El área de la región $|F(x, y)| \leqslant 1$ que cumple las condiciones anteriores es $\frac{\log \epsilon_\Delta}{\Delta^{5/2}}$, entonces

$$\lim_{c\to\infty} \frac{H_\Delta(c, F)}{c} = \lim_{c\to\infty} \sum_{\substack{x,y (\mathrm{mod}\ |\Delta|) \\ (F(x,y),\Delta)=1}} \frac{U(c, x, y)}{c} = \sum_{\substack{x,y (\mathrm{mod}\ |\Delta|) \\ (F(x,y),\Delta)=1}} \frac{\log \epsilon_\Delta}{|\Delta|^{5/2}}$$

$$= \varphi(|\Delta|)|\Delta| \frac{\log \epsilon_\Delta}{|\Delta^{5/2}|} = \frac{\log \epsilon_\Delta \varphi(|\Delta|)}{|\Delta|^{3/2}}.$$

■

Teorema 2.48 (Fórmula de Dirichlet para el Número de Clase)**.** *Para cualquier caracter real* χ_Δ *se tiene que*

$$h(\Delta) = \begin{cases} \frac{w_\Delta \sqrt{-\Delta}}{2\pi} L(1, \chi_\Delta) & si\ \Delta < 0 \\ \frac{\sqrt{\Delta}}{\log_{\epsilon_\Delta}} L(1, \chi_\Delta) & si\ \Delta > 0. \end{cases}$$

Demostración. Se sigue de la Proposición 2.47 y de que

$$h(\Delta) \lim_{N\to\infty} \frac{H_\Delta(N, F_n)}{N} = \lim_{N\to\infty} \frac{H_\Delta(N)}{N} = \frac{W_\Delta \varphi(|\Delta|)}{|\Delta|} L(1, \chi_\Delta).$$

■

Capítulo 3

El Teorema de Siegel-Walfisz

3.1. Los ceros no triviales de las funciones ζ y L

En esta sección se demostrará que la función ζ de Riemann y las L-funciones de Dirichlet tienen una infinidad de ceros no triviales y se establecerán regiones en las que estas funciones son libres de ceros. A lo largo de la sección se considerarán únicamente caracteres primitivos, a menos de que se afirme lo contrario.

Teorema 3.1. *Las funciones* $\xi(s)$ *y* $\xi(s,\chi)$ *son funciones de orden* 1.

Demostración. Por la ecuación funcional de $\xi(s)$ (Teorema 2.7), es claro que basta demostrar que $\xi(s)$ es de orden 1 en $\Re(s) \geqslant \frac{1}{2}$. Por el Teorema 2.8 sabemos que $\xi(s) = \dfrac{1}{2\pi^{\frac{s}{2}}} s(s-1)\Gamma\left(\dfrac{s}{2}\right)\zeta(s)$. Tenemos que

- $\left|\dfrac{s}{2\pi^{\frac{s}{2}}}\right| < e^{c_1|s|}$,
- de la Fórmula de Stirling (Teorema C.14) se deduce que $\left|\Gamma\left(\frac{s}{2}\right)\right| < e^{c_2|s|\log|s|}$ en la región $|\arg s| < \frac{\pi}{2}$,
- por la Proposición 2.12 sabemos que $\zeta(s) = \dfrac{1}{s-1} + 1 + s\displaystyle\int_1^\infty \frac{\{x\}}{x^{s+1}}dx$ y, como $\Re(s) \geqslant \frac{1}{2}$, se tiene que

$$\left|\int_1^\infty \frac{\{x\}}{x^{s+1}}\right| \leqslant \int_1^\infty \frac{1}{x^{Re(s)+1}}dx = \frac{1}{\Re(s)} \leqslant 2,$$

por lo que $(s-1)\zeta(s) \ll e^{c_3|s|}$.

De todo anterior se concluye que $\xi(s)$ es una función de orden 1.

Por la ecuación funcional de $\xi(s,\chi)$ (Corolario 2.26) y como el Teorema 1.26 implica que $\left|\dfrac{i^{a_\chi}q^{\frac{1}{2}}}{\tau(\chi)}\right| = 1$, bastaría ver que $\xi(x,\chi)$ es de orden 1 en la región $\Re(s) \geqslant \frac{1}{2}$. Tenemos que

- $\left|\dfrac{\pi}{q}\right|^{-\frac{1}{2}(s+a_\chi)} \leqslant e^{c_4 \log q|s|}$,
- por la Proposición 2.18 se tiene que

$$L(s,\chi) = s\int_1^\infty \frac{R(x)}{x^{s+1}}dx,$$

donde $R(x) = \sum_{n \leqslant x} \chi(n)$. Como $R(x)$ está acotada, se deduce que $|L(s,\chi)| \leqslant c_5|s| \leqslant e^{c_5|s|}$.

Se concluye entonces que $\xi(s,\chi) = \left(\frac{\pi}{q}\right)^{-\frac{1}{2}(s+a_\chi)} \Gamma\left(\frac{1}{2}(s+a_\chi)\right) L(s,\chi)$ es de orden 1. ■

Corolario 3.2. *Las funciones $\zeta(s)$ y $L(s,\chi)$ tienen una infinidad de ceros no triviales que coinciden con los ceros de las funciones $\xi(s)$ y $\xi(s,\chi)$, respectivamente.*

Demostración. Cuando s tiende a $+\infty$, $\zeta(s)$ y $L(s,\chi)$ tienden a 1 y, por el Teorema C.14 sabemos que $\Gamma(s) \sim e^{s\log s}$. Como consecuencia de esto y de las ecuaciones funcionales de $\xi(s)$ y de $\xi(s,\chi)$, y de la Proposición B.8, se tiene que las funciones $\xi(s)$ y $\xi(s,\chi)$ tienen una infinidad de ceros.

Como $\zeta(s) = \frac{2\pi^{\frac{s}{2}}}{s(s-1)} \frac{\xi(s)}{\Gamma\left(\frac{s}{2}\right)}$ y $L(s,\chi) = \left(\frac{\pi}{q}\right)^{\frac{1}{2}(s+a_\chi)} \frac{\xi(s,\chi)}{\Gamma\left(\frac{1}{2}(s+a_\chi)\right)}$ y por el Teorema 2.11 y el Teorema 2.24, es claro que sus ceros no triviales coinciden con los ceros de $\xi(s)$ y $\xi(s,\chi)$. ■

De ahora en adelante se denotarán por $\rho_n = \beta_n + i\gamma_n$ y $\varrho_n = \hat{\beta}_n + i\hat{\gamma}_n$ a los ceros de las funciones ζ y $L(s,\chi)$, respectivamente. Aunque $\varrho_n, \hat{\beta}_n, \hat{\gamma}_n$ dependan del caracter, no se hará distinción en la notación a menos de que sea necesario.

Por la Proposición B.5 se tiene que, para cualquier $\epsilon > 0$ las series $\sum_{n=1}^{\infty} \frac{1}{|\rho_n|^{1+\epsilon}}$ y $\sum_{n=1}^{\infty} \frac{1}{|\varrho_n|^{1+\epsilon}}$ convergen; y, como se vio en la demostración del Corolario 3.2, ni $\zeta(s)$, ni $L(s,\chi)$, son $O(e^{c|s|})$ entonces, por la Proposición B.9, se deduce que las series $\sum_{n=1}^{\infty} \frac{1}{|\rho_n|}$ y $\sum_{n=1}^{\infty} \frac{1}{|\varrho_n|}$ divergen.

Como $\xi(s)$ y $\xi(s,\chi)$ son de orden 1, existen A_0, B_0, A_χ, B_χ tales que

$$\xi(s) = e^{A_0+B_0 s} \prod_{n=1}^{\infty} \left(1 - \frac{s}{\rho_n}\right) e^{\frac{s}{\rho_n}} \qquad \text{y} \qquad \xi(s,\chi) = e^{A_\chi+B_\chi s} \prod_{n=1}^{\infty} \left(1 - \frac{s}{\varrho_n}\right) e^{\frac{s}{\varrho_n}}.$$

De lo anterior, y por cómo están definidos $\xi(s)$ y $\xi(s,\chi)$, se deduce que sus derivadas logarítmicas son

$$\frac{\xi'(s)}{\xi(s)} = B_0 + \sum_{n=1}^{\infty} \left(\frac{1}{s-\rho_n} + \frac{1}{\rho_n}\right) = \frac{\zeta'(s)}{\zeta(s)} + \frac{1}{s-1} - \frac{1}{2}\log\pi + \frac{1}{2}\frac{\Gamma'(\frac{1}{2}s+1)}{\Gamma(\frac{1}{2}s+1)}, \tag{3.1}$$

$$\frac{\xi'(s,\chi)}{\xi(s,\chi)} = B_\chi + \sum_{n=1}^{\infty} \left(\frac{1}{s-\varrho_n} + \frac{1}{\varrho_n}\right) = \frac{L'(s,\chi)}{L(s,\chi)} - \frac{1}{2}\log\frac{\pi}{q} + \frac{1}{2}\frac{\Gamma'(\frac{1}{2}(s+a_\chi))}{\Gamma(\frac{1}{2}(s+a_\chi))}. \tag{3.2}$$

Proposición 3.3. *$A_0 = \log\frac{1}{2}$ y $B_0 = -\frac{1}{2}\gamma - 1 + \frac{1}{2}\log 4\pi$, donde γ es la constante de Euler.*

Demostración. Notemos primero que $e^{A_0} = \xi(0) = \xi(1) = \frac{1}{2}\pi^{-\frac{1}{2}}\Gamma\left(\frac{1}{2}\right) \lim_{s\to 1}(s-1)\zeta(s) = \frac{1}{2}$, de donde se deduce que $A_0 = \log\frac{1}{2}$.

Por otro lado, tenemos que $B_0 = \frac{\xi'(0)}{\xi(0)} = -\frac{\xi'(1)}{\xi(1)} = -\lim_{s\to 1}\left[\frac{\zeta'(s)}{\zeta(s)} + \frac{1}{s-1}\right] + \frac{1}{2}\log\pi - \frac{1}{2}\frac{\Gamma'(\frac{3}{2})}{\Gamma(\frac{3}{2})}$.

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

$$\begin{aligned}
\lim_{s\to 1}\left[\frac{\zeta'(s)}{\zeta(s)} + \frac{1}{s-1}\right] &= \lim_{s\to 1}\frac{\zeta(s) + (s-1)\zeta'(s)}{(s-1)\zeta(s)} \\
&= \lim_{s\to 1}\frac{\frac{s}{s-1} - sI(s) - \frac{1}{s-1} - (s-1)I(s) - s(s-1)I'(s)}{s - s(s-1)I(s)} \\
&= \lim_{s\to 1}\frac{1 - sI(s) - (s-1)I(s) - s(s-1)I'(s)}{s - s(s-1)I(s)} = 1 - I(1),
\end{aligned}$$

y como

$$I(1) = \int_1^\infty \frac{x - \lfloor x \rfloor}{x^2}dx = \lim_{n\to\infty}\left(\int_1^n \frac{1}{x}dx - \int_1^n \frac{\lfloor x \rfloor}{x^2}dx\right) = \lim_{n\to\infty}\left(\log n - \sum_{t=1}^{n-1} t\int_t^{t+1}\frac{1}{x^2}dx\right)$$

$$= \lim_{n\to\infty}\left(\log n - (1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}) + 1\right) = 1 - \gamma,$$

deducimos que $B_0 = -\gamma + \frac{1}{2}\log\pi - \frac{1}{2}\frac{\Gamma'(\frac{3}{2})}{\Gamma(\frac{3}{2})}$. Tomando la derivada logarítmica del producto de Weierstrass (Teorema C.11) de $\Gamma\left(\frac{1}{2}s + 1\right)$ en $s = 1$ se concluye que

$$B_0 = -\gamma + \frac{1}{2}\log\pi + \frac{1}{2}\gamma + \sum_{n=1}^{\infty}\left(\frac{1}{2n} - \frac{1}{2n+1}\right) = -\frac{1}{2}\gamma + \frac{1}{2}\log\pi - 1 + \log 2 = -1 - \frac{1}{2}\gamma + \frac{1}{2}\log 4\pi.$$

■

Del teorema anterior se deduce fácilmente que $B_0 < 0$. Notemos que los ceros no triviales de ζ y $L(s,\chi)$ tienen las siguientes propiedades:

• por la ecuación funcional de $\xi(s)$ y como $\overline{\zeta(s)} = \zeta(\overline{s})$ se tiene que si s es cero de ζ entonces $\overline{s}$, $1 - s$ y $1 - \overline{s}$ lo son,

• por la ecuación funcional de $\xi(s,\chi)$ y como $\overline{L(s,\chi)} = L(\overline{s},\overline{\chi})$ se tiene que si s es cero de $L(s,\chi)$ entonces $L(1-\overline{s},\chi) = L(\overline{s},\overline{\chi}) = L(1-s,\overline{\chi}) = 0$.

Ahora se mostrará una relación entre B_0 y B_χ con sus respectivos ceros.

Proposición 3.4. *Se cumplen las igualdades*

$$B_0 = -\sum_{n=1}^{\infty}\frac{1}{\rho_n} = -2\sum_{n=1}^{\infty}\sum_{\substack{n=1\\ \gamma_n>0}}^{\infty}\frac{\beta_n}{\beta_n^2 + \gamma_n^2} \qquad y \qquad \Re(B_\chi) = -\sum_{n=1}^{\infty}\Re\frac{1}{\varrho_n}.$$

Demostración. Usando la ecuación (3.1) tenemos que

$$B_0 + \sum_{n=1}^{\infty}\left(\frac{1}{s-\rho_n} + \frac{1}{\rho_n}\right) = \frac{\xi'(s)}{\xi(s)} = -\frac{\xi'(1-s)}{\xi(1-s)} = -B_0 - \sum_{n=1}^{\infty}\left(\frac{1}{1-s-\rho_n} + \frac{1}{\rho_n}\right),$$

por lo que

$$-2B_0 = \sum_{n=1}^{\infty}\left(\frac{1}{s-\rho_n}+\frac{1}{1-s-\rho_n}+\frac{2}{\rho_n}\right).$$

Como ρ_n es cero si y sólo si lo es $1-\rho_n$, se tiene que

$$-2B_0 = \sum_{n=1}^{\infty}\left(\frac{2}{\rho_n}\right),$$

y como ρ_n es cero si y sólo si lo es $\overline{\rho_n}$, se concluye que

$$-B_0 = \sum_{n=1}^{\infty}\frac{1}{\rho_n} = \sum_{\substack{n=1\\ \gamma_n>0}}^{\infty}\left(\frac{1}{\beta_n+i\gamma_n}+\frac{1}{\beta_n-i\gamma_n}\right) = \sum_{\substack{n=1\\ \gamma_n>0}}^{\infty}\frac{2\beta_n}{\beta_n^2+\gamma_n^2}.$$

Para calcular $\Re(B_\chi)$ notemos primero que, por la ecuación (3.4), se tiene que

$$B_\chi = \frac{\xi'(0,\chi)}{\xi(0,\chi)} = -\frac{\xi'(1,\overline{\chi})}{\xi(1,\overline{\chi})} = -B_{\overline{\chi}} - \sum_{n=1}^{\infty}\left(\frac{1}{1-\overline{\varrho_n}}+\frac{1}{\overline{\varrho_n}}\right).$$

Como $B_\chi = \frac{\xi'(s,\chi)}{\xi(s,\chi)}$, podemos deducir que $\overline{B_\chi} = B_{\overline{\chi}}$. Entonces

$$2\Re(B_\chi) = -\sum_{n=1}^{\infty}\Re\left(\frac{1}{1-\overline{\varrho_n}}+\frac{1}{\overline{\varrho_n}}\right).$$

Como $L(\overline{s},\chi)=0$ si y sólo si $L(1-s,\overline{\chi})=0$, concluimos que

$$\Re(B_\chi) = -\frac{1}{2}\sum_{n=1}^{\infty}\Re\left(\frac{1}{\varrho_n}+\frac{1}{\overline{\rho_n}}\right) = -\sum_{n=1}^{\infty}\Re\frac{1}{\varrho_n}.$$

■

Lema 3.5. *Para toda $\theta\in\mathbb{R}$ se cumple la desigualdad*

$$0 \leqslant 3+4\cos\theta+\cos 2\theta.$$

Demostración. Se sigue de que $0 \leqslant 2(1+\cos\theta)^2 = 2+4\cos 2\theta+2\cos^2\theta = 2+4\cos\theta+\cos 2\theta$. ■

Proposición 3.6. *La función ζ no tiene ceros en la recta $\Re(s)=1$.*

Demostración. Notemos primero que

$$\log\zeta(s) = \sum_{p\text{ primo}}\log\left(\frac{1}{1-\frac{1}{p^s}}\right) = -\sum_{p\text{ primo}}\sum_{m=1}^{\infty}\frac{(-1)^{m-1}}{m}\frac{(-1)^m}{p^{ms}} = \sum_{p\text{ primo}}\sum_{m=1}^{\infty}\frac{1}{mp^{ms}}, \tag{3.3}$$

por lo tanto,

$$\Re\log\zeta(s) = \sum_{p\text{ primo}}\sum_{m=1}^{\infty}\frac{1}{mp^{m\sigma}}\cos(t\log p^m).$$

Supongamos que $\sigma + it$ es cero de ζ. Usando lo anterior y el Lema 3.5 se tiene que

$$3 \log \zeta(\sigma) + 4\Re \log \zeta(\sigma + it) + \Re \log \zeta(\sigma + 2it) \geqslant 0,$$

por lo tanto $\zeta^3(\sigma)|\zeta^4(\sigma + it)\zeta(\sigma + 2it)| \geqslant 1$. Cuando $\sigma \sim 1$ se tiene que

$$\zeta(\sigma) \sim \frac{1}{\sigma - 1}, \quad |\zeta(\sigma + it)| < c_1(\sigma - 1), \quad |\zeta(\sigma + 2it)| < c_2,$$

para algunas constantes c_1, c_2. Llegamos entonces a una contradicción, pues con lo anterior tendríamos que

$$\lim_{\sigma \to 1^+} \zeta^3(\sigma)|\zeta^4(\sigma + it)\zeta(\sigma + 2it)| = 0.$$

■

Teorema 3.7. *La función $\zeta(s) = \zeta(\sigma + it)$ no tiene ceros en la región*

$$\sigma \geqslant 1 - \frac{c}{\log(|t| + 2)}$$

para alguna constante positiva absoluta c.

Demostración. Veremos primero que no hay ceros, aparte de los triviales, con $|t| < 2$. De la Proposición 3.3 se puede calcular que $B_0 > -0.03$. Supongamos que hay un cero $\beta_n + i\gamma_n$ con $|\gamma_n| < 2$. Como los ceros no triviales son simétricos respecto a la recta $\Re(s) = \frac{1}{2}$, podemos suponer que $\frac{1}{2} \leqslant \beta_n < 1$. Por la Proposición 3.4 se tiene que $-0.03 < -2\frac{\beta_n}{\beta_n^2 + \gamma_n^2}$, entonces podemos deducir que $|\gamma_n| > 2$. Por la simetría de los ceros respecto al eje real, basta con demostrar el teorema para el semiplano superior. Por la ecuación (3.1) sabemos que

$$\frac{\zeta'(s)}{\zeta(s)} = B_0 - \frac{1}{s-1} + \frac{1}{2}\log \pi - \frac{1}{2}\frac{\Gamma'\left(\frac{1}{2}s + 1\right)}{\Gamma\left(\frac{1}{2}s + 1\right)} + \sum_{n=1}^{\infty}\left(\frac{1}{s - \rho_n} + \frac{1}{\rho_n}\right).$$

Consideraremos ahora $s = \sigma + it$ con $\sigma \in [1, 2]$ y $t > 2$. De la fórmula de Stirling (Teorema C.14) y la ecuación anterior se deduce que

$$-\Re\left(\frac{\zeta'(s)}{\zeta(s)}\right) < c_1 \log t - \sum_{n=1}^{\infty} \Re\left(\frac{1}{s - \rho_n} + \frac{1}{\rho_n}\right)$$

para alguna constante positiva c_1. Como $\sigma \geqslant 1$, se cumple que $\Re\left(\frac{1}{s - \rho_n} + \frac{1}{\rho_n}\right) > 0$, de donde deducimos que

$$-Re\left(\frac{\zeta'(s)}{\zeta(s)}\right) < c_1 \log t.$$

Como la derivada logarítmica de $\zeta(s)$ en $\Re(s) > 1$ es $-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^\sigma} e^{it \log n}$, por el Lema 3.5 se puede deducir que

$$3\left[-\frac{\zeta'(\sigma)}{\zeta(\sigma)}\right]+4\left[-\Re\frac{\zeta'(\sigma+it)}{\zeta(\sigma+it)}\right]+\left[-\Re\frac{\zeta'(\sigma+2it)}{\zeta(\sigma+2it)}\right]\geqslant 0.$$

Por la ecuación (3.1) y el Teorema C.15, existen constantes A_1 y A_2 tales que, si tomamos $t=\gamma_n>2$, entonces

$$-\Re\frac{\zeta'(\sigma)}{\zeta(\sigma)}<\frac{1}{\sigma-1}+A_1,\qquad -\Re\frac{\zeta'(\sigma+it)}{\zeta(\sigma+it)}<A_2\log\gamma_n-\frac{1}{\sigma-\beta_n},\qquad -\Re\frac{\zeta'(\sigma+2it)}{\zeta(\sigma+2it)}<A_2\log 2\gamma_n.$$

Por lo tanto, $0\leqslant\frac{3}{\sigma-1}+A_4\log\gamma_n-\frac{4}{\sigma-\beta_n}$, es decir, $\beta_n\leqslant\sigma-\dfrac{4(\sigma-1)}{3+(\sigma-1)A_4\log\gamma_n}$. Fijando $\sigma=1+\frac{\delta}{\log\gamma_n}$ con $\delta<\frac{1}{A_4}$ se concluye que $\beta_n\leqslant 1+\left(1-\dfrac{4}{3+A_4\delta}\right)\dfrac{\delta}{\log\gamma_n}\leqslant 1-\dfrac{c}{\log(\gamma_n+2)}$. ■

Ahora se hará una estimación similar para las funciones L. Por conveniencia, se denotará por $\mathcal{L}=\log q+\log(|t|+2)$ al hablar de un caracter χ módulo q y de un número complejo con parte imaginaria t. Primero veamos que la Identidad de Euler (Teorema 2.15) implica que

$$-\frac{L'(s,\chi)}{L(s,\chi)}=\sum_{p\text{ primo}}\frac{\log p}{p^s}\frac{\chi(p)}{1-\frac{\chi(p)}{p^s}}=\sum_{n=1}^{\infty}\Lambda(n)\frac{\chi(n)}{n^s},\tag{3.4}$$

además, para cualquier caracter χ módulo q y χ^* su caracter inducido se cumple la desigualdad

$$\left|\frac{L'(s,\chi)}{L(s,\chi)}-\frac{L'(s,\chi^*)}{L(s,\chi^*)}\right|=\left|\sum_{p\text{ primo}}\log p\left(\frac{\chi^*(p)\chi_0(p)}{p^s\left(1-\frac{\chi^*(p)\chi_0(p)}{p^s}\right)}-\frac{\chi^*(p)}{p^s\left(1-\frac{\chi^*(p)}{p^s}\right)}\right)\right|$$

$$\leqslant\sum_{p|q}\log p\left|\frac{1}{p^s}\frac{\chi^*(p)}{1-\frac{\chi^*(p)}{p^s}}\right|\leqslant\sum_{p|q}\log p\leqslant\log q.\tag{3.5}$$

En el caso de estar considerando un caracter principal, dicha desigualdad se toma restando $\frac{\zeta'(s)}{\zeta(s)}$ en vez de $\frac{L'(s,\chi^*)}{L(s,\chi^*)}$.

Por la ecuación (3.4), la Proposición 3.4 y el Teorema C.15, existe $c>0$ tal que, para cualquier caracter primitivo χ^* y $s=\sigma+it$ complejo con $\sigma\in(1,2)$, se tiene que

$$-\Re\frac{L'(\sigma+it,\chi^*)}{L(\sigma+it,\chi^*)}=\frac{1}{2}\log\frac{q}{\pi}+\frac{1}{2}\Re\frac{\Gamma'(\frac{1}{2}(s+a_{\chi^*}))}{\Gamma(\frac{1}{2}(s+a_{\chi^*}))}-\Re\sum_{n=1}^{\infty}\frac{1}{s-\varrho_n}<c\mathcal{L}-\Re\frac{1}{s-\varrho_n}.\tag{3.6}$$

Usando esta desigualdad, junto con la ecuación (3.5), se llega a que existe $c>0$ tal que para cualquier caracter no principal χ se cumple la desigualdad

$$-\Re\frac{L'(s,\chi)}{L(s,\chi)}<c\mathcal{L}-\Re\frac{1}{s-\varrho_n}\tag{3.7}$$

para cualquier n, y tal que también se cumple la desigualdad

$$-\frac{L'(\sigma,\chi_0)}{L(\sigma,\chi_0)} < \frac{1}{\sigma-1} + c\mathcal{L}. \tag{3.8}$$

Lema 3.8. *Sea χ un caracter complejo módulo q, entonces la función $L(\sigma+it,\chi)$ no tiene ceros en la región*

$$\sigma \geqslant 1 - \frac{c}{\mathcal{L}}$$

donde c es una constante positiva absoluta.

Demostración. Por el Lema 3.5 y la ecuación (3.4) se tiene la desigualdad

$$-3\frac{L'(\sigma,\chi_0)}{L(\sigma,\chi_0)} - 4\Re\frac{L'(\sigma+it,\chi)}{L(\sigma+it,\chi)} - \Re\frac{L'(\sigma+2it,\chi^2)}{L(\sigma+2it,\chi^2)}$$

$$= \sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^\sigma}\Big(3 + 4\Re(\chi(n)e^{-it\log n}) + \Re(\chi^2(n)e^{-2it\log n})\Big) \geqslant 0.$$

De las ecuaciones (3.7) y (3.8), y tomando $t = \hat{\gamma}_n$, se deduce que $0 < \dfrac{3}{\sigma-1} + A_1\mathcal{L} - \dfrac{4}{\sigma-\hat{\beta}_n}$. Fijando $\sigma = 1 + \frac{A_2}{\mathcal{L}}$ tenemos que

$$\beta_n < 1 + \frac{A_2}{\mathcal{L}}\left(1 - \frac{4}{3+A_1A_2}\right).$$

Es suficiente considerar $A_2 < A_1$ para concluir la demostración. ■

Lema 3.9. *Sea χ un caracter real no principal módulo q, si $0<\delta<c$ y $|\hat{\gamma}_n| \geqslant \frac{\delta}{\log q}$, entonces*

$$\hat{\beta}_n < 1 - \frac{\delta}{5\mathcal{L}},$$

donde c es una constante positiva absoluta.

Demostración. Como χ es caracter real se tiene que $\chi_0 = \chi^2$. De manera similar que en la demostración del lema anterior, tomando $t = \hat{\gamma}_n$ se deduce que

$$0 < \frac{3}{\sigma-1} - \frac{4}{\sigma-\hat{\beta}_n} + \Re\frac{1}{\sigma-1+2i\hat{\gamma}_n} + A_1\mathcal{L}.$$

Como se está considerando $\hat{\gamma}_n \geqslant \frac{\delta}{\log q} > \frac{\delta}{\mathcal{L}}$, y si se toma $\sigma = 1 + \frac{\delta}{\mathcal{L}}$, se tiene que $\Re\frac{1}{\sigma-1+2i\hat{\gamma}_n} < \frac{\mathcal{L}}{5\delta}$. Por lo tanto, $\frac{4}{\sigma-\hat{\beta}_n} < \frac{16\mathcal{L}+5A_1\delta\mathcal{L}}{5\delta}$. Si se toma $\delta < \frac{4}{5A_1} = c$ se concluye que

$$\hat{\beta}_n < \sigma - \frac{20\delta}{(16+5A_1\delta)\mathcal{L}} < 1 - \frac{\delta}{5\mathcal{L}}.$$

■

Lema 3.10. *Sea χ un caracter real no principal módulo q, $0 < \delta < c$ y $0 < |\hat{\gamma}_n| < \frac{\delta}{\log q}$, entonces*

$$\hat{\beta}_n < 1 - \frac{\delta}{\log q},$$

donde c es una constante positiva absoluta.

Demostración. Como χ es un caracter real, sus ceros son simétricos respecto al eje real, entonces

$$-\frac{1}{\sigma - 1} - A_1 < \frac{\zeta'(s)}{\zeta(s)} \leqslant -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^{\sigma}} \leqslant \sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^{\sigma}} = -\frac{L'(\sigma,\chi)}{L(\sigma,\chi)}$$

$$< A_2 \log q - \left(\frac{1}{\sigma - \varrho_n} + \frac{1}{\sigma - \overline{\varrho}_n}\right) = A_2 \log q - \frac{2(\sigma - \hat{\beta}_n)}{(\sigma - \hat{\beta}_n)^2 + \hat{\gamma}_n^2}.$$

Si se toma $0 < \delta$, $0 < |\hat{\gamma}_n| < \frac{\delta}{\log q}$ y $\sigma = 1 + \frac{2\delta}{\log q}$, se tiene que $|\hat{\gamma}_n| < \frac{\delta}{\log q} = \frac{1}{2}(\sigma - 1) < \frac{1}{2}(\sigma - \hat{\beta}_n)$. Por lo tanto,

$$0 < \frac{1}{\sigma - 1} + A_3 \log q - \frac{8}{5(\sigma - \hat{\beta}_n)} \Rightarrow \hat{\beta}_n < 1 + \frac{\delta}{\log q}\left(2 - \frac{16}{5(2\delta A_3 + 1)}\right).$$

Si se considera $\delta < \frac{3}{10A_3}$, se concluye la demostración. ■

Corolario 3.11. *Sea χ un caracter real no principal módulo q y $0 < \delta < c$, donde c es la misma constante que la del lema anterior. La función $L(s,\chi)$ no tiene más de dos ceros reales ϱ_1, ϱ_2 con*

$$\varrho_1, \varrho_2 > 1 - \frac{\delta}{\log q}.$$

Demostración. Se procede como en la demostración anterior, pero tomando ϱ_1 y ϱ_2 en vez de ϱ_n y $\overline{\varrho}_n$. ■

Teorema 3.12. *Existe una constante c tal que, en la región*

$$\sigma \geqslant \begin{cases} 1 - \frac{c}{\log q|t|} & \text{si } |t| \geqslant 1, \\ 1 - \frac{c}{\log q} & \text{si } |t| \leqslant 1, \end{cases}$$

- *$L(\sigma + it, \chi)$ es libre de ceros para cualquier caracter complejo χ,*
- *$L(\sigma + it, \chi)$ es libre de ceros, salvo posiblemente un cero real, para cualquier caracter real χ.*

Demostración. Se sigue claramente de los resultados previos. ■

Lema 3.13. *Sean χ_1 y χ_2 caracteres reales primitivos módulo q_1 y q_2, respectivamente, y sean $\hat{\sigma}_1, \hat{\sigma}_2$ ceros reales de $L(s,\chi_1)$ y $L(s,\chi_2)$, respectivamente. Entonces*

$$\min\{\hat{\sigma}_1, \hat{\sigma}_2\} < 1 - \frac{c}{\log q_1 q_2},$$

donde c es una constante absoluta.

Demostración. Nótese que $\chi_1\chi_2$ es un caracter real no principal módulo q_1q_2 entonces, para cualquier $\sigma \in (1,2)$ se tiene que

$$0 \leqslant \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^\sigma}(1+\chi_1(n))(1+\chi_2(n)) = -\frac{\zeta'(\sigma)}{\zeta(\sigma)} - \frac{L'(\sigma,\chi_1)}{L(\sigma,\chi_1)} - \frac{L'(\sigma,\chi_2)}{L(\sigma,\chi_2)} - \frac{L'(\sigma,\chi_1\chi_2)}{L(\sigma,\chi_1\chi_2)}$$

$$< 2A_1 \log q_1q_2 - \frac{1}{\sigma-\hat{\sigma}_1} - \frac{1}{\sigma-\hat{\sigma}_2} + \frac{1}{\sigma-1}.$$

Por lo tanto,

$$\frac{2}{\sigma - \min\{\hat{\sigma}_1,\hat{\sigma}_2\}} < 2A_1 \log q_1q_2 + \frac{1}{\sigma-1}.$$

Si se fija $\sigma = 1 + \frac{\delta}{\log q_1q_2}$, se deduce que

$$\min\{\hat{\sigma}_1,\hat{\sigma}_2\} < 1 + \frac{\delta}{\log q_1q_2}\left(1 - \frac{2}{2\delta A_1 + 1}\right),$$

y si se toma $\delta < \frac{1}{2A_1}$ fijo, se concluye la demostración. ■

Del lema que se acaba de demostrar se pueden deducir directamente los siguientes dos corolarios.

Corolario 3.14. *Para cada q existe a lo más para un caracter real χ módulo q tal que la función $L(s,\chi)$ tiene un cero real $\hat{\sigma}$ con*

$$\hat{\sigma} > 1 - \frac{c}{\log q},$$

donde c es una constante absoluta.

Corolario 3.15. *Sean $q_1 < q_2 < \cdots$ todos los módulos para los que existe χ_i caracter real primitivo módulo q_i tal que $L(s,\chi_i)$ tiene un cero real $\hat{\sigma}_i > 1 - \frac{\hat{c}}{\log q_i}$, donde $\hat{c}$ es un tercio de la constante del Lema 3.13. Entonces $q_{j+1} > q_j^2$.*

Corolario 3.16. *Existe $c > 0$ tal que para cualquier $z \geqslant 3$ hay a lo más un caracter real primitivo χ cuyo módulo está acotado por z tal que $L(s,\chi)$ tienen un cero real $\hat{\sigma}$ tal que $\hat{\sigma} > 1 - \frac{c}{\log z}$.*

Demostración. Sea $c = \frac{\hat{c}}{2}$ la mitad de la constante $\hat{c}$ del Lema 3.13, y supóngase que existen dos caracteres χ_1, χ_2 con ceros $\hat{\sigma}_1, \hat{\sigma}_2 > 1 - \frac{c}{\log z}$, entonces

$$\hat{\sigma}_1, \hat{\sigma}_2 > 1 - \frac{\hat{c}}{\log q_1q_2},$$

teniendo una contradicción. ■

De lo anterior es fácil deducir que, para una constante c adecuada, si existe un caracter real primitivo χ^* para un módulo $q \leqslant z$ tal que la función $L(s,\chi^*)$ tiene un cero $\hat{\sigma} > 1 - \frac{c}{\log z}$ implica que los únicos caracteres cuyo módulo acotado por z que tienen algún cero con esta propiedad, son los caracteres que induce el caracter χ^*.

Por la Fórmula del Número de Clase de Dirichlet (Teorema 2.48), y como $h(D) \geqslant 1$, podemos deducir que para cualquier caracter real primitivo χ existe una constante absoluta c tal que

$$L(1, \chi) > cq^{-\frac{1}{2}}.$$

Teorema 3.17. *Para cualquier caracter no pricnipal χ, las series $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ y $-\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \log n$ coinciden con las funciones $L(s, \chi)$ y $L'(s, \chi)$ en el semiplano $\Re(s) > 0$, respectivamente.*

Demostración. Notemos primero que, por el criterio de convergencia de Dirichlet, la serie $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ converge para $s \in \mathbb{R}^+$.

Sea $\epsilon > 0$, y $s = \sigma + it$ con $\sigma > \epsilon$. Sea $M > 0$ tal que $\left| \sum_{n \leqslant x} \frac{\chi(n)}{n^\epsilon} \right| < M$, para todo $x > 1$. Aplicando la Fórmula de sumación de Abel (Teorema 1.3) con $c_n = \frac{\chi(n)}{n^\epsilon}$ y $f(x) = x^{\epsilon - s}$, se tiene que

$$\sum_{a<n\leqslant b} \frac{\chi(n)}{n^s} = \mathbb{C}(b) b^{\epsilon-s} - \mathbb{C}(a) a^{\epsilon-s} + (s-\epsilon) \int_a^b \mathbb{C}(t) t^{\epsilon-s-1} dt.$$

Por lo tanto,

$$\left| \sum_{a<n\leqslant b} \frac{\chi(n)}{n^s} \right| \leqslant M(b^{\epsilon-\sigma} + a^{\epsilon-\sigma}) + |s-\epsilon| M \int_a^b t^{\epsilon-\sigma-1} dt \leqslant 2M a^{\epsilon-\sigma} \left(1 + \frac{|\epsilon - s|}{\sigma - \epsilon} \right).$$

Haciendo tender $a \to \infty$, se tiene que la serie converge puntualmente por el criterio de Cauchy.

Denotando por $L_N(s, \chi)$ a la serie

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

tenemos que las funciones $L_N(s, \chi)$ son analíticas y convergen uniformemente en cada compacto del semiplano $\Re(s) > 0$, por lo tanto, la serie $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ es analítica en el semiplano $\Re(s) > 0$, y como una extensión analítica es única, se sigue que $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ en $\Re(s) > 0$. De lo anterior también se deduce que $L'(s, \chi) = -\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \log n$. ∎

Proposición 3.18. *Existe una constante absoluta c tal que, si $1 - \frac{1}{\log q} \leqslant \sigma \leqslant 1$, entonces*

$$|L(\sigma, \chi)| < c \log q \qquad y \qquad |L'(\sigma, \chi)| < c \log^2 q$$

para cualquier caracter χ no principal.

Demostración. Por el Teorema 3.17, sabemos que si $\sigma > 0$, entonces $L(\sigma, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^\sigma}$. Para

$\sigma > 1 - \frac{1}{\log q}$ se tiene que

$$\left|\sum_{n=1}^{q} \frac{\chi(n)}{n^\sigma}\right| \leqslant \sum_{n=1}^{q} \frac{e}{n} < c_1 \log q$$

y aplicando la Fórmula de sumacion de Abel (Teorema 1.3) se tiene que

$$\left|\sum_{n=q+1}^{\infty} \frac{\chi(n)}{n^\sigma}\right| = \lim_{N\to\infty}\left|\sum_{n=q+1}^{N} \frac{\chi(n)}{n^\sigma}\right| \leqslant \lim_{N\to\infty}\left|\frac{1}{N^\sigma}\sum_{n=q+1}^{N}\chi(n) - \sum_{n=q+1}^{N-1}\chi(n)\left(\frac{1}{(n+1)^\sigma} - \frac{1}{n^\sigma}\right)\right|$$

$$\leqslant \frac{1}{q^\sigma}\max_N\left|\sum_{n=q+1}^{N}\chi(n)\right| + \frac{1}{q^\sigma} \leqslant \frac{q}{q^\sigma} = q^{1-1+\frac{1}{\log q}} = e.$$

El primer resultado se sigue de las dos desigualdades.

Del Teorema 3.17 también sabemos que, si $\sigma > 0$, entonces $L'(\sigma,\chi) = -\sum_{n=1}^{\infty}\frac{\chi(n)}{n^\sigma}\log n$. Por lo tanto, si $\sigma > 1 - \frac{1}{\log q}$, se tiene que

$$\left|\sum_{n=1}^{q} \frac{\chi(n)}{n^\sigma}\log n\right| \leqslant \sum_{n=1}^{q} \log q \frac{e}{n} < c_1 \log^2 q$$

y usando nuevamente la Fórmula de sumación de Abel, se tiene que

$$\left|\sum_{n=q+1}^{\infty} \frac{\chi(n)}{n^\sigma}\log n\right| = \lim_{N\to\infty}\left|\sum_{n=q+1}^{N} \frac{\chi(n)}{n^\sigma}\log n\right|$$

$$\leqslant \lim_{N\to\infty}\left|\frac{\log N}{N^\sigma}\sum_{n=q+1}^{N}\chi(n) - \sum_{n=q+1}^{N-1}\chi(n)\left(\frac{\log(n+1)}{(n+1)^\sigma} - \frac{\log n}{n^\sigma}\right)\right|$$

$$\leqslant \frac{\log q}{q^\sigma}\max_N\left|\sum_{n=q+1}^{N}\chi(n)\right| + \frac{\log q}{q^\sigma} \leqslant \frac{q\log q}{q^\sigma} = q^{1-1+\frac{1}{\log q}}\log q = e\log q.$$

De estas dos desigualdades se sigue el segundo resultado. ■

3.2. La densidad de los ceros no triviales de las funciones ζ y L.

Se denotará por R_T al rectángulo delimitado por los vértices $-1, 2, 2+iT, -1+iT$. Sea $T \in \mathbb{R}$ tal que en la recta $\Im(s) = T$, la función ζ no tiene ceros. Por el principio del argumento y la ecuación funcional de $\xi(s)$ se tiene que el número de ceros dentro de R_T, que se denotará por $N(T)$, es

$$N(T) = \frac{1}{2\pi i}\int_{\partial R_T}\frac{\xi'(s)}{\xi(s)}ds = \frac{1}{2\pi}\int_{\partial R_T}(\arg\xi(s))'ds.$$

Notemos que $\xi(s)$ es real y no se anula en el eje real, por lo que

$$\int_{-1}^{2}(\arg\xi(s))'ds = 0.$$

Sea L_1 la trayectoria por la frontera de R_T, en sentido contrario al de las manecillas del reloj, que va de 2 a $\frac{1}{2}+iT$; y L_2 de $\frac{1}{2}+iT$ a -1. Como $\xi(\sigma+it)=\overline{\xi(1-\sigma+it)}$ y por la ecuación funcional de ξ se tiene que

$$\int_{L_1}(\arg\xi(s))'ds=\int_{L_2}(\arg\xi(s))'ds,$$

entonces

$$\pi N(T)=\int_{L_1}(\arg\xi(s))'ds=\int_{L_1}(\arg(s-1)+\arg\pi^{-\frac{1}{2}s}+\arg\Gamma(\frac{1}{2}s+1)+\arg(s))'ds.$$

Como

$$\int_{L_1}(\arg(s-1))'ds=\arg\left(iT-\frac{1}{2}\right)=\frac{1}{2}\pi+O(T^{-1}),$$

$$\int_{L_1}(\arg\pi^{-\frac{1}{2}s})'ds=-\frac{T}{2}\log\pi,$$

y por la fórmula de Stirling se consluye que

$$\int_{L_1}(\arg\Gamma(\frac{1}{2}s+1))'ds=\int_{L_1}\left(\Im\log\Gamma\left(\frac{1}{2}s+1\right)\right)'ds=\Im\log\Gamma\left(\frac{1}{2}iT+\frac{5}{4}\right)$$

$$=\Im\left[\left(\frac{1}{2}iT+\frac{3}{4}\right)\log\left(\frac{1}{2}iT+\frac{5}{4}\right)-\frac{1}{2}iT-\frac{5}{4}+\frac{1}{2}\log 2\pi+O(T^{-1})\right]$$

$$=\frac{1}{2}T\log\frac{1}{2}T-\frac{1}{2}T+\frac{1}{2}T\log\left|i+\frac{5}{2T}\right|-\frac{5}{4}+\frac{3}{4}\arg\left(\frac{1}{2}iT\right)+\frac{3}{4}\arg\left(1+\frac{10}{4iT}\right)+O(T^{-1})$$

$$=\frac{1}{2}T\log\frac{1}{2}T-\frac{1}{2}T+\frac{3}{8}\pi+O(T^{-1}).$$

Entonces

$$N(T)=\frac{T}{2\pi}\log\frac{T}{2\pi}-\frac{T}{2\pi}+\frac{7}{8}+G(T)+O(T^{-1}),$$

donde $G(T)=\dfrac{1}{\pi}\displaystyle\int_{L_1}(\arg\zeta(s))'ds.$

Lema 3.19. *Para T suficientemente grande se tiene que*

$$\sum_{n=1}^{\infty}\frac{1}{1+(T-\gamma_n)^2}=O(\log T).$$

Demostración. Si $s=2+it$ y $t\geqslant 2$ se tiene que

$$\left|-\Re\frac{\zeta'(s)}{\zeta(s)}\right|=\left|\Re\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}\right|=\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^2}\cos(t\log n)\leqslant\left|\frac{\zeta'(2)}{\zeta(2)}\right|,$$

y como

$$-\Re\frac{\zeta'(2+it)}{\zeta(2+it)}<c_1\log t-\sum_{n=1}^{\infty}\Re\left(\frac{1}{2+it-\rho_n}+\frac{1}{\rho_n}\right),$$

se deduce que

$$\sum_{n=1}^{\infty} \Re\left(\frac{1}{2+it-\rho_n}\right) < c_2 \log t.$$

Con esto se concluye la demostración, ya que

$$\sum_{n=1}^{\infty} \frac{1}{4+(t-\gamma_n)^2} \leqslant \sum_{n=1}^{\infty} \Re \frac{1}{2+i(t-\gamma_n)} < \sum_{n=1}^{\infty} \Re\left(\frac{1}{2+it-\rho_n}\right) < A_2 \log t.$$

■

Corolario 3.20. *El número de ceros no triviales de la función ζ de Riemman con parte imaginaria en el intervalo $[T-1, T+1]$ es $O(\log T)$.*

Corolario 3.21. *Para cualquier T grande se tiene que*

$$\sum_{\substack{n=1 \\ \gamma_n \notin [T-1, T+1]}}^{\infty} \frac{1}{(T-\gamma_n)^2} = O(\log T).$$

Lema 3.22. *Para T suficientemente grande tal que ningún cero de ζ tenga parte imaginaria T, y para cualquier $\sigma \in [-1, 2]$, se tiene que*

$$\frac{\zeta'(\sigma+iT)}{\zeta(\sigma+iT)} = \sum_{\substack{n=1 \\ |\gamma_n - T|<1}}^{\infty} \frac{1}{\sigma+iT-\rho_n} + O(\log T)$$

Demostración. Se denotará por $s = \sigma + iT$. Notemos que, si $|\gamma_n - T| \geqslant 1$, entonces

$$\left|\frac{1}{s-\rho_n} - \frac{1}{2+iT-\rho_n}\right| = \frac{2-\sigma}{|(s-\rho_n)(2+iT-\rho_n)|} \leqslant \frac{3}{|\gamma_n - T|^2},$$

y por el Corolario 3.21 la suma sobre todos estos términos es $O(\log T)$. Por la ecuación (3.1), y aplicando en esta ecuación el Teorema 3.4 y la fórmula de Stirling, tenemos que

$$\frac{\zeta'(s)}{\zeta(s)} = B_0 - \frac{1}{s-1} + \frac{1}{2}\log\pi - \frac{1}{2}\frac{\Gamma'(\frac{1}{2}s+1)}{\Gamma(\frac{1}{2}s+1)} + \sum_{n=1}^{\infty}\left(\frac{1}{s-\rho_n} + \frac{1}{\rho_n}\right)$$

$$= \sum_{n=1}^{\infty} \frac{1}{s-\rho_n} + O(\log T) = \sum_{\substack{n=1 \\ |\gamma_n - T|<1}}^{\infty} \frac{1}{s-\rho_n} + \sum_{\substack{n=1 \\ |\gamma_n - T|\geqslant 1}}^{\infty} \left(\frac{1}{s-\rho_n} - \frac{1}{2+iT-\rho_n}\right) + O(\log T)$$

$$= \sum_{\substack{n=1 \\ |\gamma_n - T|<1}}^{\infty} \frac{1}{s-\rho_n} + O(\log T).$$

■

Como en $\sigma = 2$ se tiene que $-\frac{\zeta'(s)}{\zeta(s)} = 1 + \sum_{n=2}^{\infty} \frac{\Lambda(n)}{n^2} e^{it\log n}$ se puede deducir que

$$G(T) = O(1) + \int_{2+iT}^{\frac{1}{2}+iT} \Im \frac{\zeta'(s)}{\zeta(s)} ds.$$

Por el Lema 3.22 se tiene que

$$\int_{2+iT}^{\frac{1}{2}+iT} \Im \frac{\zeta'(s)}{\zeta(s)} ds = \int_{2+iT}^{\frac{1}{2}+iT} \left(\sum_{\substack{n=1 \\ |\gamma_n - T|<1}}^{\infty} \frac{1}{\sigma + iT - \rho_n} + O(\log T) \right) ds = O(\log T).$$

Entonces se puede concluir el siguiente Teorema.

Teorema 3.23. *Para cualquier $T > 0$ tenemos que*

$$N(T) = \frac{T}{2\pi} \log \frac{T}{2\pi} - \frac{T}{2\pi} + O(\log T).$$

Dado un caracter χ primitivo módulo q se denotará por $N(T, \chi)$ al número de ceros no triviales de la función $L(s, \chi)$ dentro del rectángulo $\hat{R}_T$, donde $\hat{R}_T$ es el rectángulo que tiene como vértices los puntos $\frac{5}{2} - iT, \frac{5}{2} + iT, -\frac{3}{2} + iT, -\frac{3}{2} - iT$. Como dicho rectángulo contiene a un cero no trivial de $L(s, \chi)$, ya sea en $s = 0$ ó $s = -1$, se tiene que

$$2\pi[N(T, \chi) + 1] = \int_{\partial \hat{R}_T} (arg(\xi(s, \chi)))' ds.$$

Sean L_1 y L_2 las trayectorias por la frontera de $\hat{R}_T$ de $\frac{1}{2} - iT$ a $\frac{1}{2} + iT$, y su complemento, ambos en sentido contrario al de las manecillas del reloj. Por la ecuación funcional de $\xi(s, \chi)$ sabemos que $\arg \xi(\sigma + it, \chi) = \arg \overline{\xi(1 - \sigma + it, \chi)} + c$, donde c no depende de $\sigma + it$, entonces

$$\pi[N(T, \chi) + 1] = \int_{L_1} \left(\arg \left(\frac{q}{\pi} \right)^{\frac{1}{2}s + \frac{1}{2}a_\chi} + \arg \Gamma \left(\frac{1}{2}s + \frac{1}{2}a_\chi \right) + \arg L(\frac{1}{2} + iT, \chi) \right)' ds$$

$$= T \log \frac{q}{\pi} + T \log \frac{T}{2} - T + O(1) + \int_{L_1} \left(\arg L \left(\frac{1}{2} + iT, \chi \right) \right)' ds.$$

Lema 3.24. *Para cualquier caracter χ primitivo módulo q se tiene que*

$$\sum_{n=1}^{\infty} \frac{1}{1 + (T - \hat{\gamma}_n)^2} = O(\log q(|T| + 2)).$$

Demostración. La demostración es análoga a la del Lema 3.19. ■

Lema 3.25. *Sea χ un caracter primitivo módulo q. Para $T > 2$ tal que T no coincide con la* *parte imaginaria de ningún cero de* $L(s,\chi)$, *y para* $\sigma \in \left(-\frac{3}{2}, \frac{5}{2}\right)$ *se tiene que*

$$\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{\substack{n=1 \\ |\hat{\gamma}_n - T|<1}}^{\infty} \frac{1}{\sigma + iT - \varrho_n} + O(\log q(|T|+2)).$$

Demostración. La demostración es análoga a la del Lema 3.22. ■

Teorema 3.26. *Para cualquier* $T > 2$ *y* χ *caracter primitivo módulo* q *se tiene que*

$$N(T,\chi) = \frac{T}{\pi}\log\frac{qT}{2\pi} - \frac{T}{\pi} + O(\log T + \log q).$$

Demostración. La demostración es análoga a la del Teorema 3.23. ■

3.3. Las funciones $\Psi(x)$ y $\Psi(x,\chi)$

Definición 3.27. Para cada real $x > 1$ se define la función

$$\Psi(x) = \sum_{n \leqslant x} \Lambda(n).$$

Lema 3.28. *Sea* $y, T, c > 0$ *y sean*

$$\delta(y) = \begin{cases} 0 & si\ 0 < y < 1, \\ \frac{1}{2} & si\ y = 1, \\ 1 & si\ y > 1, \end{cases} \qquad I(y,T) = \frac{1}{2\pi i}\int_{c-iT}^{c+iT} \frac{y^s}{s} ds,$$

entonces

$$|I(y,T) - \delta(y)| < \begin{cases} y^c \min\{1, \frac{1}{T|\log y|}\} & si\ y \neq 1, \\ \frac{c}{T} & si\ y = 1. \end{cases}$$

Demostración. Si $0 < y < 1$ la función $\frac{y^s}{s} \to 0$ uniformemente cuando $\Re(s) \to +\infty$. Aplicando el Teorema del Residuo podemos deducir que

$$I(y,T) = \frac{1}{2\pi i}\int_{c-iT}^{\infty - iT} \frac{y^s}{s} ds - \frac{1}{2\pi i}\int_{c+iT}^{\infty + iT} \frac{y^s}{s} ds.$$

Notemos que

$$\left| \int_{c \pm iT}^{\infty \pm iT} \frac{y^s}{s} ds \right| \leqslant \frac{1}{T}\int_{c}^{\infty} y^{\Re(s)} d\Re(s) = \frac{y^c}{T|\log y|}.$$

Denotando por η a la trayectoria conformada por el arco de circunferencia de radio $R = \sqrt{c^2 + T^2}$ en sentido de las manecillas del reloj de $c - iT$ a $c + iT$, se tiene que

$$|I(y,T)| \leqslant \frac{1}{2\pi}\int_{\eta} \left|\frac{y^s}{s}\right| ds \leqslant \frac{1}{2\pi}\pi R \frac{y^c}{R} < y^c.$$

Entonces queda demostrado si $0 < y < 1$.

Para $y > 1$ se hace el mismo procedimiento que cuando $y \in (0,1)$, pero se toman las integrales hacia $-\infty$ o el complemento del arco de circunferencia, dependiendo el caso. Como $\frac{y^s}{s}$ tiene un polo en 0 con residuo 1, queda demostrado este caso.

Cuando $y = 1$ se sigue de que

$$I(1,T) = \frac{1}{2\pi}\int_0^T \frac{2c}{c^2+t^2}dt = \frac{1}{\pi}\int_0^{\frac{T}{c}} \frac{1}{1+u^2}du = \frac{1}{2} - \frac{1}{\pi}\int_{\frac{T}{c}}^{\infty} \frac{1}{1+u^2}du,$$

y como esta última integral está acotada por $\frac{c}{T}$, se conluye la demostración. ■

Del lema anterior se puede deducir que para cualesquiera $y > 0, c > 1$ se cumple la igualdad

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{y^s}{s}ds = \delta(y),$$

para demostrar esta igualdad basta hacer tender $T \to \infty$ en el lema. Definiendo la función $\Psi_0(x) = \Psi(x) - \frac{1}{2}\Lambda(x)$ podemos deducir del lema anterior que

$$\Psi_0(x) = \frac{1}{2\pi i}\sum_{n=1}^{\infty}\Lambda(n)\int_{c-i\infty}^{c+i\infty}\frac{x^s}{sn^s}ds = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} -\frac{\zeta'(s)}{\zeta(s)}\frac{x^s}{s}ds. \tag{3.9}$$

Si se denota

$$J(x,T) = \frac{1}{2\pi i}\int_{c-iT}^{c+iT}\left[-\frac{\zeta'(x)}{\zeta(x)}\right]\frac{x^s}{s}ds$$

se tiene que

$$|\Psi_0(x) - J(x,T)| < \sum_{\substack{n=1\\ n\neq x}}^{\infty}\Lambda(n)\left(\frac{x}{n}\right)^c \text{mín}\left\{1, \frac{1}{T|\log(x/n)|}\right\} + c\frac{\Lambda(x)}{T}. \tag{3.10}$$

Se denotará por $\langle x\rangle$ a la distancia que hay entre x y la potencia de primo más cercana a x, distinta de x.

Lema 3.29. *Para cualquier $x \geqslant 2$ y $T > 0$ se tiene que*

$$|\Psi_0(x) - J(x,T)| \ll \frac{x(\log x)^2}{T} + (\log x)\,\text{mín}\left\{1, \frac{x}{T\langle x\rangle}\right\}.$$

Demostración. Sea $c = 1 + \frac{1}{\log x}$. Como se vio en la demostración del Teorema 3.7, si $s > 1$, entonces $0 < -\frac{\zeta'(s)}{\zeta(s)} < \frac{1}{s-1}$. Entonces se tiene que

$$\sum_{\substack{n=1\\ n\notin(\frac{3}{4}x,\frac{5}{4}x)}}^{\infty}\Lambda(n)x^c n^{-c}\frac{1}{T|\log(x/n)|} \ll \frac{x}{T}\sum_{n=1}^{\infty}\Lambda(n)n^{-c} \ll -\frac{x}{T}\frac{\zeta'(c)}{\zeta(c)} \ll \frac{x\log x}{T}.$$

Sea x_- la mayor potencia de primo que es menor que x, entonces

$$\log\frac{x}{x_-} = -\log\left(1-\frac{x-x_-}{x}\right) \geqslant \frac{x-x_-}{x}.$$

Para $n \in \left(\frac{3}{4}x, x_-\right)$ entero y $0 < x_- - n = a < \frac{1}{4}x$, entonces

$$\log\frac{x}{n} \geqslant \log\frac{x_-}{n} = -\log\left(1-\frac{a}{x_-}\right) \geqslant \frac{a}{x_-}.$$

Entonces

$$\sum_{n\in(\frac{3}{4}x,x)} \Lambda(n)x^c n^{-c}\frac{1}{T|\log(x/n)|} \ll \log x \min\left\{1, \frac{x}{T(x-x_-)}\right\} + \frac{\log x}{T}\sum_{a\leqslant\frac{1}{4}x}\frac{x}{a}$$

$$\ll \log x \min\left\{1, \frac{x}{T(x-x_-)}\right\} + \frac{x\log^2 x}{T}.$$

Se puede hacer lo análogo cuando sumamos los términos $n \in (x, \frac{5}{4}x)$ considerando, en vez de x_-, a la menor potencia de primo mayor que x. Con lo anterior y por la ecuación (3.10) se concluye la demostración. ■

Teorema 3.30. *Para cualquier $x \geqslant 2$ se cumple la igualdad*

$$\Psi_0(x) = x - \sum_{n=1}^{\infty}\frac{x^{\rho_n}}{\rho_n} - \frac{\zeta'(0)}{\zeta(0)} - \frac{1}{2}\log\left(1-\frac{1}{x^2}\right).$$

Demostración. Sea S la trayectoria que recorre la frontera del rectángulo con vértices en los puntos $c-iT, c+iT, -U+it, -U-iT$, donde $c = 1+\frac{1}{\log x}$ y U es un natural impar. Por el Teorema de los Residuos, y usando la ecuación (3.1) y la derivada logarítmica del producto de Weiestrass (Teorema C.11) para calcular los residuos, se deduce la igualdad

$$\frac{1}{2\pi i}\int_S \left[\frac{\zeta'(s)}{\zeta(s)}\right]\frac{x^s}{s}ds = x - \sum_{\substack{n=1\\|\gamma_n|<T}}^{\infty}\frac{x^{\rho_n}}{\rho_n} - \frac{\zeta'(0)}{\zeta(0)} - \sum_{0<m<\frac{U}{2}}\frac{x^{-2m}}{-2m}.$$

Del Corolario 3.20 se puede deducir que existen $T's$ tan grandes como se quieran tales que $|\gamma_n - T| \gg \frac{1}{\log T}$ para cualquier $n \in \mathbb{N}$. Por el Lema 3.22, si $\Re(s) \in (-1,2)$, entonces

$$\frac{\zeta'(s)}{\zeta(s)} = \sum_{\substack{n=1\\|\gamma_n-T|<1}}^{\infty}\frac{1}{s-\rho_n} + O(\log T).$$

Como la suma anterior tiene $O(\log T)$ sumandos y cada sumando vale $O(\log T)$, se deduce que

$\frac{\zeta'(s)}{\zeta(s)} = O(\log^2 T)$. Entonces

$$\int_{-1\pm iT}^{c\pm iT} \left[-\frac{\zeta'(s)}{\zeta(s)}\right] \frac{x^s}{s} ds \ll \log^2 T \int_{-1}^{c} \left|\frac{x^{\sigma\pm iT}}{\sigma \pm iT}\right| d\sigma \ll \frac{\log^2 T}{T} \int_{-1}^{c} x^\sigma d\sigma \ll \frac{x\log^2 T}{T\log x}.$$

Con los Teoremas C.4, C.7 y C.13 se puede deducir la igualdad

$$\frac{\Gamma\left(\frac{1}{2}s\right)}{\Gamma\left(\frac{1}{2}-\frac{1}{2}s\right)} = \pi^{-\frac{1}{2}} 2^{1-s} \cos\left(\frac{1}{2}\pi s\right)\Gamma(s). \tag{3.11}$$

Combinando esta igualdad con la ecuacuación funcional de ζ (Teorema 2.9) se tiene que

$$\zeta(1-s) = 2^{1-s}\pi^{-s}(\cos\frac{1}{2}\pi s)\Gamma(s)\zeta(s).$$

Tomando la derivada logarítmica de la función anterior, se tiene que para cualquier s tal que $\Re(s) > 2$, se da la igualdad

$$-\frac{\zeta'(1-s)}{\zeta(1-s)} = -\log 2 - \log\pi - \frac{1}{2}\tan\frac{1}{2}\pi s + \frac{\Gamma'(s)}{\Gamma(s)} + \frac{\zeta'(s)}{\zeta(s)}.$$

Notemos que $\tan\frac{1}{2}\pi s$ está acotado si $|s-(2k+1)| \geqslant \frac{1}{2}$ para cualquier $k \in \mathbb{N}$. Como ya se ha dicho antes, $\frac{\Gamma'(s)}{\Gamma(s)} \ll \log|s|$ y $\frac{\zeta'(s)}{\zeta(s)}$ es acotado por una constante en $\Re(s) > 2$. Se deduce entonces que $-\frac{\zeta'(1-s)}{\zeta(1-s)} \ll \log|s|$ en $\Re(s) > 2$ y, por lo tanto, que $\frac{\zeta'(s)}{\zeta(s)} \ll \log 2|s|$ en $\Re(s) < -1$, siempre y cuando $|s-2k| \geqslant \frac{1}{2}$ para cualquier $k \in \mathbb{N}$. Entonces, se tiene que

$$\int_{-1\pm iT}^{-U\pm iT} \left[-\frac{\zeta'(s)}{\zeta(s)}\right] \frac{x^s}{s} ds \ll \frac{\log 2T}{T} \int_{-1}^{-U} x^\sigma d\sigma \ll \frac{\log 2T}{Tx\log x}$$

y

$$\int_{-U+iT}^{U+iT} \left[-\frac{\zeta'(s)}{\zeta(s)}\right] \frac{x^s}{s} ds \ll \frac{\log 2U}{U} \int_{T}^{-T} x^{-U} dt \ll \frac{T\log 2U}{Ux^U}.$$

Entonces, se tiene que

$$\int_{S_1} \left[-\frac{\zeta'(s)}{\zeta(s)}\right] \frac{x^s}{s} ds \ll \frac{x\log^2 T}{T\log x} + \frac{\log 2T}{Tx\log x} + \frac{T\log 2U}{Ux^U},$$

Donde S_1 es el recorrido que hace S sin incluir el intervalo de $c-iT$ a $c+iT$. Haciendo tender $U \to \infty$ y usando el Lema 3.29 se deduce que

$$\Psi_0(x) = x - \sum_{\substack{n=1\\|\gamma_n|<T}}^{\infty} \frac{x^{\rho_n}}{\rho_n} - \frac{\zeta'(0)}{\zeta(0)} - \frac{1}{2}\log\left(1-\frac{1}{x^2}\right) + O\left(\frac{x\log^2(xT)}{T} + \log x \min\left\{1, \frac{x}{T\langle x\rangle}\right\}\right),$$

y haciendo tender $T \to \infty$ en esta última igualdad, se obtiene la ecuación buscada. ∎

Teorema 3.31. *Para cualquier $x \geqslant 2$ entero se tiene que*

$$\Psi(x) - x \ll xe^{-c\sqrt{\log x}},$$

donde c es una constante positiva.

Demostración. Recordemos que, por el Teorema 3.7, existe $c > 0$ tal que, si $|\gamma_n| < T$, entonces

$$\beta_n < 1 - \frac{c}{\log T}.$$

Por lo tanto, $|x^{\rho_n}| = x^{\beta_n} < xe^{-c\frac{\log x}{\log T}}$, y con esto se deduce que

$$\sum_{\substack{n=1\\|\gamma_n|<T}}^{\infty} \frac{x^{\rho_n}}{\rho_n} \ll xe^{-c\frac{\log x}{\log T}} \sum_{\substack{n=1\\|\gamma_n|<T}}^{\infty} \frac{1}{|\gamma_n|} = xe^{-c\frac{\log x}{\log T}} \sum_{\substack{n=1\\|\gamma_n|<T}}^{\infty} \left(\frac{1}{|\gamma_n|} - \frac{1}{T}\right) + \frac{N(T)}{T}xe^{-c\frac{\log x}{\log T}}$$

$$= xe^{-c\frac{\log x}{\log T}} \left(\frac{N(T)}{T} + \int_2^T \frac{N(t)}{t^2}dt\right) = xe^{-c\frac{\log x}{\log T}} O\left(\log T + \int_2^T \frac{\log t}{t}dt\right) \ll x(\log T)^2 e^{-c\frac{\log x}{\log T}}.$$

Como se vio en la demostración anterior, se tiene que

$$\Psi_0(x) = x - \sum_{\substack{n=1\\|\gamma_n|<T}}^{\infty} \frac{x^{\rho_n}}{\rho_n} - \frac{\zeta'(0)}{\zeta(0)} - \frac{1}{2}\log\left(1 - \frac{1}{x^2}\right) + O\left(\frac{x\log^2(xT)}{T} + \log x \operatorname{mín}\left\{1, \frac{x}{T\langle x\rangle}\right\}\right),$$

por lo tanto,

$$\Psi(x) - x \ll x(\log T)^2 e^{-c\frac{\log x}{\log T}} + \frac{x\log^2(xT)}{T} + \log x \operatorname{mín}\left\{1, \frac{x}{T\langle x\rangle}\right\}.$$

Si se toma T de modo que $(\log T)^2 = \log x$, se deduce que

$$\Psi(x) - x \ll x(\log x)e^{-c\sqrt{\log x}} + x(\log x)^2 e^{-\sqrt{\log x}},$$

y con esto se concluye la demostración. ■

Definición 3.32. Para $x \geqslant 1$ y cualquier caracter χ, se definen

$$\Psi(x,\chi) = \sum_{n\leqslant x} \chi(n)\Lambda(n) \qquad \text{y} \qquad \Psi_0(x,\chi) = \Psi(x,\chi) - \frac{1}{2}\chi(x)\Lambda(x).$$

Teorema 3.33. *Para cualquier $x \geqslant 2$ y cualquier caracter χ primitivo módulo q, se da la igualdad*

$$\Psi_0(x,\chi) = -\sum_{n=1}^{\infty} \frac{x^{\varrho_n}}{\varrho_n} - (1-a_\chi)\log x - b_\chi - \sum_{n=1}^{\infty} \frac{x^{a_\chi - 2n}}{a_\chi - 2n} + O\left(\frac{x\log^2 qxT}{T} + (\log x)\operatorname{mín}\left\{1, \frac{x}{T\langle x\rangle}\right\}\right),$$

donde $b_\chi = \dfrac{L'(0,\chi)}{L(0,\chi)}$ si $\chi(-1) = -1$, y $b_\chi = \lim\limits_{s\to 0} \dfrac{L'(s,\chi)}{L(s,\chi)} - \dfrac{1}{s}$ si $\chi(-1) = 1$.

Demostración. Procediendo de una manera muy similar que al tratar la función $\Psi_0(x)$, si tomamos S como en la demostración anterior y usando el Teorema del Residuo llegamos a que

$$\frac{1}{2\pi i}\int_S \left[-\frac{L'(s,\chi)}{L(s,\chi)}\right]\frac{x^s}{s}ds = \begin{cases} -\sum\limits_{\substack{n=1\\ |\hat{\gamma}_n|<T}}^{\infty}\dfrac{x^{\varrho_n}}{\varrho_n} - b_\chi - \sum\limits_{m\leqslant\frac{U}{2}}\dfrac{x^{1-2m}}{1-2m} & \text{si } \chi(-1)=-1,\\ -\sum\limits_{\substack{n=1\\ |\hat{\gamma}_n|<T}}^{\infty}\dfrac{x^{\varrho_n}}{\varrho_n} - \log x - b_\chi - \sum\limits_{m\leqslant\frac{U}{2}}\dfrac{x^{-2m}}{-2m} & \text{si } \chi(-1)=1.\end{cases}$$

y también, de manera similar, se deduce que

$$|\Psi_0(x,\chi) - J(x,T,\chi)| \ll \frac{x(\log x)^2}{T} + (\log x)\,\text{mín}\left\{1, \frac{x}{T\langle x\rangle}\right\}$$

donde

$$J(x,T,\chi) = \frac{1}{2\pi i}\int_{c-iT}^{c+iT}\left[-\frac{L'(s,\chi)}{L(s,\chi)}\right]\frac{x^s}{s}ds.$$

Por el Lema 3.24 sabemos que el número de ceros con parte imaginaria en $[T-1, T+1]$ es $O(\log qT)$. Entonces, existen $T's$ tan grandes como se quieran de modo que, para cualquier $n \in \mathbb{N}$, se cumple que $|\hat{\gamma}_n - T| \gg \frac{1}{\log qT}$. Con lo anterior, y por el Lema 3.25, se tiene que, si $|T| > 2$ y $\sigma \in (-1, 2)$, entonces $\dfrac{L'(\sigma+iT,\chi)}{L(\sigma+iT,\chi)} \ll (\log qT)^2$. Por lo tanto

$$\int_{-1\pm iT}^{c\pm iT}\left[-\frac{L'(s,\chi)}{L(s,\chi)}\right]\frac{x^s}{s}ds \ll \frac{x(\log qT)^2}{T\log x}.$$

De manera similar que con la función ζ, usando la ecuación funcional de $L(s,\chi)$ (Teorema 2.23) y la ecuación (3.11) se tiene que

$$L(1-s,\chi) = \varepsilon(\chi)2^{1-s}\pi^{-s}q^{s-\frac{1}{2}}\cos\left(\frac{1}{2}\pi(s-a_\chi)\right)\Gamma(s)L(s,\overline{\chi}),$$

donde $|\varepsilon(\chi)| = 1$. Se deduce entonces que

$$\int_{-1\pm iT}^{-U\pm iT}\left[-\frac{L'(s,\chi)}{L(s,\chi)}\right]\frac{x^s}{s}ds \ll \frac{x\log qT}{T\log x}$$

y

$$\int_{-U+iT}^{-U-iT}\left[-\frac{L'(s,\chi)}{L(s,\chi)}\right]\frac{x^s}{s}ds \ll \frac{xT\log qU}{U\log x}.$$

Haciendo tender U a infinito se termina la demostración. ■

Por simplicidad se considerará x entero y $T \leqslant x$, de donde se deduce la fórmula

$$\Psi(x,\chi) = -\sum_{\substack{n=1\\ |\hat{\gamma}_n|<T}}^{\infty}\frac{x^{\varrho_n}}{\varrho_n} - b_\chi + O\left(\frac{x\log^2 qx}{T}\right). \tag{3.12}$$

De la derivada logarítmica de $L(s,\chi)$ (ecuación (3.4)) tenemos que

$$B_\chi + \sum_{n=1}^{\infty}\left(\frac{1}{s-\varrho_n}+\frac{1}{\varrho_n}\right) = \frac{L'(s,\chi)}{L(s,\chi)} - \frac{1}{2}\log\frac{\pi}{q} + \frac{1}{2}\frac{\Gamma'(\frac{1}{2}(s+a_\chi))}{\Gamma(\frac{1}{2}(s+a_\chi))}.$$

Si se evalúa la ecuación anterior en 2 y se restan, se deduce que

$$\frac{L'(s,\chi)}{L(s,\chi)} = -\frac{1}{2}\frac{\Gamma'(\frac{1}{2}(s+a_\chi))}{\Gamma(\frac{1}{2}(s+a_\chi))} + \sum_{n=1}^{\infty}\left(\frac{1}{s-\varrho_n}-\frac{1}{2-\varrho_n}\right).$$

Por la ecuación anterior y por la derivada logarítmica del producto de Weierstrass (Teorema C.11), es tiene que

$$b_\chi = O(1) - \sum_{n=1}^{\infty}\left(\frac{1}{\varrho_n}+\frac{1}{2-\varrho_n}\right).$$

Por el Lema 3.24 aplicado a $T=0$ se tiene que

$$\sum_{\substack{n=1\\|\hat{\gamma}_n|\geqslant 1}}^{\infty}\left|\frac{1}{\varrho_n}+\frac{1}{2-\varrho_n}\right| = 2\sum_{\substack{n=1\\|\hat{\gamma}_n|\geqslant 1}}^{\infty}\frac{1}{|\varrho_n(2-\varrho_n)|} \ll \sum_{n=1}^{\infty}\frac{1}{|2-\varrho_n|^2} \ll O(\log q).$$

y que

$$\sum_{\substack{n=1\\|\hat{\gamma}_n|<1}}^{\infty}\frac{1}{2-\varrho_n} \ll \sum_{\substack{n=1\\|\hat{\gamma}_n|<1}}^{\infty}\frac{1}{|2-\varrho_n|^2} \ll O(\log q).$$

Por lo tanto,

$$b_\chi = -\sum_{\substack{n=1\\|\hat{\gamma}_n|<1}}^{\infty}\frac{1}{\varrho_n} + O(\log q).$$

Por lo anterior y usando la ecuación (3.12) se concluye el siguiente Lema.

Lema 3.34. *Para cualesquiera $2\leqslant T\leqslant x$ y χ caracter primitivo módulo q se tiene que*

$$\Psi(x,\chi) = -\sum_{\substack{n=1\\|\hat{\gamma}_n|<T}}^{\infty}\frac{x^{\varrho_n}}{\varrho_n} + \sum_{\substack{n=1\\|\hat{\gamma}_n|<1}}^{\infty}\frac{1}{\varrho_n} + O\left(\frac{x\log^2 qx}{T}\right).$$

Teorema 3.35. *Para cualesquier $2\leqslant T\leqslant x$ y χ caracter primitivo módulo q se tiene que*

$$\Psi(x,\chi) = -\frac{x^{\varrho_1}}{\varrho_1} - \sum_{\substack{n=1\\|\hat{\gamma}_n|<T}}^{\infty\ \star}\frac{x^{\varrho_n}}{\varrho_n} + O\left(\frac{x\log^2 qx}{T} + x^{\frac{1}{4}}\log x\right),$$

en caso de que el caracter χ tenga un cero excepcional ϱ_1 como el que menciona el Teorema 3.12, y $\sum^\star$ denota la suma que no considera los ceros ϱ_1 y $1-\varrho_1$; y en caso de que χ no tenga *dicho cero, simplemente tenemos la fórmula*

$$\Psi(x,\chi) = -\sum_{\substack{n=1\\|\hat{\gamma}_n|<T}}^{\infty} \frac{x^{\varrho_n}}{\varrho_n} + O\left(\frac{x\log^2 qx}{T}\right).$$

Demostración. Podemos suponer que la constante c del Teorema 3.12 es menor que $\frac{1}{4}$, y tomaremos como punto de partida el Lema anterior. Por el Teorema 3.26 y como $\frac{c}{\log q} < \Re(\varrho_n) < 1-\frac{c}{\log q}$ para los ceros no excepcionales con parte imaginaria menor que 1, se tiene que

$$\sum_{\substack{n=1\\|\hat{\gamma}_n|<1}}^{\infty}{}^{\star} \frac{1}{\varrho_n} \ll \sum_{\substack{n=1\\|\hat{\gamma}_n|<1}}^{\infty}{}^{\star} \log q \ll \log^2 q \ll \frac{x\log^2 qx}{T}.$$

De aquí se deduce la afirmación cuando χ no cuenta con cero excepcional. En caso de que χ tenga un cero excepcional se deduce que que

$$\begin{aligned}\Psi(x,\chi) &= -\sum_{\substack{n=1\\|\hat{\gamma}_n|<T}}^{\infty}{}^{\star} \frac{x^{\varrho_n}}{\varrho_n} - \frac{x^{\varrho_1}-1}{\varrho_1} - \frac{x^{1-\varrho_1}-1}{1-\varrho_1} + O\left(\frac{x\log^2 qx}{T}\right)\\ &= -\sum_{\substack{n=1\\|\hat{\gamma}_n|<T}}^{\infty}{}^{\star} \frac{x^{\varrho_n}}{\varrho_n} - \frac{x^{\varrho_1}}{\varrho_1} - \frac{x^{1-\varrho_1}-1}{1-\varrho_1} + O\left(\frac{x\log^2 qx}{T}\right).\end{aligned}$$

Por el teorema del valor medio tenemos que $\frac{x^{1-\varrho_1}-1}{1-\varrho_1} \leqslant x^{\frac{1}{4}}\log x$, de donde se conluye la demostración. ∎

Corolario 3.36. *Sea x natural y T real, con $2 \leqslant T \leqslant x$ y χ caracter no principal módulo q, se tiene que*

$$\Psi(x,\chi) = -\frac{x^{\varrho_1}}{\varrho_1} - \sum_{\substack{n=1\\|\hat{\gamma}_n|<T}}^{\infty}{}^{\star} \frac{x^{\varrho_n}}{\varrho_n} + O\left(\frac{x\log^2 qx}{T} + x^{\frac{1}{4}}\log x\right),$$

en caso de que el caracter χ tenga un cero excepcional ϱ_1 como el que menciona el Teorema 3.12, y $\sum^{\star}$ denota la suma que no considera los ceros ϱ_1 y $1-\varrho_1$; y en caso de que χ no tenga dicho cero, simplemente tenemos la fórmula

$$\Psi(x,\chi) = -\sum_{\substack{n=1\\|\hat{\gamma}_n|<T}}^{\infty} \frac{x^{\varrho_n}}{\varrho_n} + O\left(\frac{x\log^2 qx}{T}\right).$$

Demostración. El resultado se sigue del Teorema 3.35 y de que, si χ^* es el caracter inducido por χ, se cumple la estimación

$$|\Psi(x,\chi)-\Psi(x,\chi^*)| = \sum_{\substack{n\leqslant x\\(n,q)>1}} \Lambda(n) = \sum_{\substack{p|q\\p\text{ primo}}} \sum_{k<\log_p x} \log p \ll \log x \log q.$$

■

3.4. El Teorema de Siegel-Walfisz

A lo largo de la sección se denotará por $F(s)$ al producto $\zeta(s)L(s,\chi_1)L(s,\chi_2)L(s,\chi_1\chi_2)$, donde χ_1 y χ_2 son caracteres reales primitivos módulo q_1 y q_2, respectivamente, para algunos $q_1 \neq q_2$. $F(s)$ es una función analítica en $\mathbb{C}\backslash\{1\}$, y en el 1 tiene un polo simple con residuo $r = L(1,\chi_1)L(1,\chi_2)L(1,\chi_1\chi_2)$. De manera similar a la demostración de la Proposición 3.6, se demuestra la igualdad

$$\log F(s) = \sum_{p \text{ primo}} \sum_{m=1}^{\infty} \frac{1}{mp^{ms}}[1+\chi_1(p^m)][1+\chi_2(p^m)],$$

y de lo anterior se deduce que

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

en $\Re(s) > 1$, donde $a_1 = 1$ y $a_m \geqslant 0$ para toda m. Notemos que

$$F^{(k)}(2) = (-1)^k \sum_{n=1}^{\infty} \frac{a_n}{n^2}(\log n)^k.$$

Entonces, el desarrollo en series de Taylor de $F(s)$ en $s = 2$ es

$$F(s) = \sum_{m=0}^{\infty} b_m(2-s)^m,$$

donde $b_m \geqslant 0$ para toda m y $b_0 \geqslant 1$. El radio de convergencia de esta serie es 1. Notemos que la función $F(s) - \frac{r}{s-1}$ es entera, por lo tanto

$$F(s) - \frac{r}{s-1} = \sum_{m=0}^{\infty} (b_m - r)(2-s)^m$$

y converge en todo el plano.

Como se vio en el Teorema 3.1, si χ es un caracter no principal módulo q, se tiene que

$$L(s,\chi) = s\int_1^{\infty} \frac{R(x)}{x^{s+1}}dx,$$

donde $R(x) = \sum_{n\leqslant x} \chi(n) \leqslant q$. Por lo tanto, $L(s,\chi) \leqslant qs\int_1^{\infty} \frac{1}{x^{s+1}}dx$. Entonces existe una constante c tal que $|F(s)| < c(q_1q_2)^2$ sobre la circunferencia $|s-2| = \frac{3}{2}$, y $\frac{r}{s-1}$ es también acotado por $c(q_1q_2)^2$ en dicha circunferencia. Por las desigualdades de Cauchy para funciones holomorfas se deduce que

$$|b_m - r| < 2cq_1^2q_2^2\left(\frac{2}{3}\right)^m. \tag{3.13}$$

Proposición 3.37. *Si* $\frac{7}{8} < s < 1$ *se tiene que*

$$F(s) > \frac{1}{2} - \frac{cr}{1-s}(q_1q_2)^{8(1-s)}$$

para alguna constante $c > 0$.

Demostración. Por la ecuación (3.13) se tiene que, para cualquier M natural,

$$\sum_{m=M}^{\infty} |b_m - r|(2-s)^m \leqslant \sum_{m=M}^{\infty} 2cq_1^2q_2^2 \left(\frac{2}{3}(2-s)\right)^m$$

$$\leqslant 2cq_1^2q_2^2 \sum_{m=M}^{\infty} \left(\frac{3}{4}\right)^m < c_1q_1^2q_2^2 \left(\frac{3}{4}\right)^M < c_1q_1^2q_2^2e^{-\frac{M}{4}},$$

de donde

$$F(s) - \frac{r}{s-1} \geqslant 1 - r\sum_{m=0}^{M-1}(2-s)^m - c_1q_1^2q_2^2e^{-\frac{M}{4}} = 1 - r\frac{(2-s)^M - 1}{1-s} - c_1q_1^2q_2^2e^{-\frac{M}{4}}.$$

Escojiendo una M fija tal que $\frac{1}{2}e^{-\frac{1}{4}} < c_1q_1^2q_2^2e^{-\frac{M}{4}} < \frac{1}{2}$, se llega a la desigualdad

$$F(s) > \frac{1}{2} - r\frac{(2-s)^M}{1-s} + \frac{r}{1-s} > \frac{1}{2} - r\frac{(2-s)^M}{1-s},$$

para $s \in (\frac{7}{8}, 1)$, ya que $r = \lim_{s\to 1} \frac{F(s)}{\zeta(s)} = \lim_{s\to 1^+} \frac{F(s)}{\zeta(s)} > 0$. Como $\frac{1}{2}e^{-\frac{1}{4}} < c_1q_1^2q_2^2e^{-\frac{M}{4}}$ implica que $M \leqslant 8\log q_1q_2 + c_2$, se deduce que

$$(2-s)^M = e^{M\log(2-s)} < e^{M(1-s)} < c_3(q_1q_2)^{8(1-s)}.$$

Por lo tanto,

$$F(s) > \frac{1}{2} - c_3\frac{r}{1-s}(q_1q_2)^{8(1-s)}$$

para toda $s \in (-\frac{7}{8}, 1)$. ■

Teorema 3.38 (Siegel)**.** *Para cualquier* $\epsilon > 0$ *existen constantes positivas* $C_1(\epsilon)$ *y* $C_2(\epsilon)$ *tales que, si* χ *es un caracter real primitivo módulo* q*, entonces*

$$L(1,\chi) > C_1(\epsilon)q^{-\epsilon}$$

y, si $s > 1 - C_2(\epsilon)q^{-\epsilon}$*, entonces* $L(s,\chi) \neq 0$.

Demostración. Sea $\epsilon > 0$. Hay dos casos a considerar:

- Si existe un caracter real primitivo χ_1 tal que $L(\beta_1, \chi_1) = 0$ para algún $\beta_1 \in (1 - \frac{\epsilon}{16}, 1)$, entonces $F(\beta_1) = 0$ independientemente de χ_2,
- Si no existe algún caracter real primitivo con cero en $(1 - \frac{\epsilon}{16}, 1)$, entonces para cualquier $\beta_1 \in (1 - \frac{\epsilon}{16}, 1)$, se tiene que $F(\beta_1) < 0$, pues $L(s,\chi)$ es positivo en $s = 1$ y no cambia de signo

en $(1 - \frac{\epsilon}{16}, 1)$, y $\zeta(s)$ es negativo en $(0, 1)$.

En cualquiera de los casos se tiene que $F(\beta_1) \leqslant 0$. Aplicando esto en la Proposición 3.37 se tiene que

$$c_1 r > \frac{1}{2}(1-\beta_1)(q_1 q_2)^{-8(1-\beta_1)}.$$

Consideraremos ahora β_1, χ_1 fijos (ya sea como los del primer caso o elegidos al azar en el segundo caso). Por la Proposición 3.18 tenemos que, para cualquier caracter real primitivo χ_2 módulo $q_2 > q_1$, se cumple la estimación

$$r = L(1,\chi_1)L(1,\chi_2)L(1,\chi_1\chi_2) < c_2^2 \log q_1 \log q_1 q_2 L(1,\chi_2).$$

De las dos desigualdades se concluye que

$$L(1,\chi_2) > c_3 q_2^{-8(1-\beta_1)} \frac{1}{\log q_2} > c_3 q_2^{-\frac{\epsilon}{2}} \frac{1}{\log q_2} > c_3 q_2^{-\epsilon},$$

donde c_3 depende únicamente de χ_1 y, por lo tanto, depende únicamente de ϵ. La veracidad para cuando $q_2 \leqslant q_1$, se sigue de que podemos ajustar la constante c_3 a una constante $C_1(\epsilon)$ que sirva para estos casos finitos.

Ahora se demostrará la cota para los ceros. Sea $\epsilon > 0$ y q lo suficientemente grande para que se cumpla la desigualdad $1 - \frac{1}{\log q} \leqslant 1 - C_1\left(\frac{\epsilon}{2}\right) q^{-\epsilon}$. Se puede suponer que $C_1(\epsilon) > C_1\left(\frac{\epsilon}{2}\right)$, pues $L(1,\chi) > C_1\left(\frac{\epsilon}{2}\right) q^{-\frac{\epsilon}{2}} > C_1\left(\frac{\epsilon}{2}\right) q^{-\epsilon}$. Supongamos que existe un cero real σ de $L(s,\chi)$ con $1 - C_1\left(\frac{\epsilon}{2}\right) q^{-\epsilon} \leqslant \sigma \leqslant 1$. Por el Teorema del Valor Medio, existe $\sigma' \in (\sigma, 1)$ tal que

$$L(1,\chi) = L(1,\chi) - L(\sigma,\chi) = L'(\sigma',\chi)(1-\sigma).$$

Por la Proposición 3.18, existe una constante c tal que $L'(\sigma',\chi) < c\log^2 q$. Por lo tanto,

$$L(1,\chi) < c(1-\sigma)\log^2 q < cC_1\left(\frac{\epsilon}{2}\right) q^{-\epsilon}\log^2 q,$$

y para q suficientemente grande tal que $c\log^2 q < q^{\frac{\epsilon}{2}}$, se llegaría a que, $L(1,\chi) < C_1\left(\frac{\epsilon}{2}\right) q^{-\frac{\epsilon}{2}}$, teniendo una contradicción. De lo anterior se concluye la segunda parte del teorema. ■

Definición 3.39. Dado $x \geqslant 1$, y q, a enteros con $q > 0$, se define

$$\Psi(x;q,a) = \sum_{\substack{n \leqslant x \\ n \equiv a (\mathrm{mod}\ q)}} \Lambda(n).$$

Teorema 3.40 (Siegel-Walfisz)**.** *Para cada $M > 0$ existe $C_M > 0$ tal que*

$$\Psi(x;q,a) = \frac{x}{\varphi(q)} + O\left(xe^{-C_M\sqrt{\log x}}\right)$$

de manera uniforme siempre y cuando $q \leqslant (\log x)^M$.

Demostración. Por el Corolario 1.13 se tiene que $\Psi(x;q,a) = \dfrac{1}{\varphi(q)} \sum\limits_{\chi (\text{mod } q)} \overline{\chi(a)}\Psi(x,\chi)$. Por el Teorema 3.31 se sigue que

$$\Psi(x;q,a) = \frac{x}{\varphi(q)} + \frac{1}{\varphi(q)} \sum_{\substack{\chi (\text{mod } q) \\ \chi \neq \chi_0}} \overline{\chi(a)}\Psi(x,\chi) + O\left(\frac{1}{\varphi(q)}\left(xe^{-c\sqrt{\log x}} + \log^2 qx\right)\right).$$

Por el Corolario 3.36 sabemos que, para cualquier χ caracter no principal módulo q y $2 \leqslant T \leqslant x$, se tiene que

$$\Psi(x,\chi) = \varepsilon_\chi \frac{x^{\varrho_0}}{\varrho_0} + \sum_{\substack{n=1 \\ |\hat{\gamma}_n| < T}}^{\infty}{}^{\star} \frac{x^{\varrho_n}}{\varrho_n} + O\left(\frac{x\log^2 qx}{T} + x^{\frac{1}{4}}\log x\right),$$

donde ϱ_0 es el posible cero excepcional y $\varepsilon_\chi \in \{0,-1\}$. Por el Teorema de Siegel (Teorema 3.38) se tiene que, para cualquier $\epsilon > 0$, existe $C_2(\epsilon)$ tal que $\frac{1}{2} < \rho_0 < 1 - \frac{C_2(\epsilon)}{q^\epsilon}$, por lo cual

$$\frac{x^{\varrho_0}}{\varrho_0} \ll x^{1-\frac{C_2(\epsilon)}{q^\epsilon}}.$$

Como se hizo en la demostración del Teorema 3.31, pero aplicando el Teorema 3.12 y la estimación de $N(T,\chi)$, se deduce que

$$\sum_{\substack{n=1 \\ 1 \leqslant |\hat{\gamma}_n| < T}}^{\infty}{}^{\star} \frac{x^{\varrho_n}}{\varrho_n} \ll x^{1-\frac{c}{\log qT}}(\log qT)^2,$$

y

$$\sum_{\substack{n=1 \\ 0 \leqslant |\hat{\gamma}_n| < 1}}^{\infty}{}^{\star} \frac{x^{\varrho_n}}{\varrho_n} \ll x^{1-\frac{c}{\log q}}(\log q)^2.$$

Por lo tanto, para cualquier caracter χ no principal módulo q, se tiene que

$$\Psi(x,\chi) =\ll \frac{x\log^2 qx}{T} + x^{\frac{1}{4}}\log x + x^{1-\frac{C_2(\epsilon)}{q^\epsilon}} + x^{1-\frac{c}{\log qT}}(\log qT)^2 + x^{1-\frac{c}{\log q}}(\log q)^2.$$

Fijando $T = e^{\sqrt{\log x}}$ y $\epsilon = \frac{1}{2M}$ se tiene que

$$\Psi(x,\chi) \ll xe^{-c_M\sqrt{\log x}}.$$

Podemos entonces concluir que

$$\begin{aligned}\Psi(x;q,a) &= \frac{x}{\varphi(q)} + \frac{1}{\varphi(q)} \sum_{\substack{\chi (\text{mod } q) \\ \chi \neq \chi_0}} \overline{\chi(a)}\Psi(x,\chi) + O\left(\frac{1}{\varphi(q)}\left(xe^{-c\sqrt{\log x}} + \log^2 qx\right)\right) \\ &= \frac{x}{\varphi(q)} + O\left(xe^{-c'_M\sqrt{\log x}}\right)\end{aligned}$$

■

Definición 3.41. Para cualesquiera $x \geqslant 2$, $q, a \in \mathbb{N}$ y $(a,q) = 1$ se define

$$\pi(x;q,a) = \sum_{\substack{p\leqslant x \\ p \text{ primo} \\ p\equiv a (\text{mod } q)}} 1,$$

es decir, $\pi(x;q,a)$ es la función que cuenta a los primos menores o iguales que x que son congruentes con $a(\text{mod } q)$.

Definición 3.42. Para cualquier $x \geqslant 2$ se define la función $Li(x)$ como

$$Li(x) = \int_2^x \frac{1}{\log s} ds.$$

Teorema 3.43 (Siegel-Walfisz)**.** *Para cada $M > 0$ existe $C_M > 0$ tal que*

$$\pi(x;q,a) = \frac{Li(x)}{\varphi(q)} + O(xe^{-c\sqrt{\log x}})$$

de manera uniforme siempre y cuando $q \leqslant (\log x)^M$.

Demostración. Denotemos $\pi_1(x;q,a) = \sum_{\substack{n\leqslant x \\ n\equiv a(\text{mod } q)}} \frac{\Lambda(n)}{\log n}$. Se puede deducir fácilmente que

$$\pi_1(x;q,a) = \sum_{\substack{n\leqslant x \\ n\equiv a(\text{mod } q)}} \Lambda(n) \int_n^x \frac{1}{t\log^2 t} dt + \frac{1}{\log x} \sum_{\substack{n\leqslant x \\ n\equiv a(\text{mod } q)}} \Lambda(n) = \int_2^x \frac{\Psi(t;q,a)}{t\log^2 t} dt + \frac{\Psi(x;q,a)}{\log x}.$$

Aplicando ahora el Teorema 3.40 se tiene que

$$\begin{aligned}
\pi_1(x;q,a) &= \int_2^x \frac{1}{\varphi(q)\log^2 t} dt + \frac{x}{\varphi(q)\log x} + O\left(\int_2^x \frac{e^{-c\sqrt{\log t}}}{\log^2 t} dt + \frac{xe^{-c\sqrt{\log x}}}{\log x}\right) \\
&= \frac{1}{\varphi(q)} \int_2^x t\left(-\frac{1}{\log t}\right)' dt + \frac{x}{\varphi(q)\log x} + O\left(xe^{-c\sqrt{\log x}}\right) \\
&= \frac{1}{\varphi(q)} \int_2^x \frac{1}{\log t} dt - \left(\frac{t}{\varphi(q)\log t}\right)_{t=2}^x + \frac{x}{\varphi(q)\log x} + O\left(xe^{-c\sqrt{\log x}}\right) \\
&= \frac{Li(x)}{\varphi(q)} + O(xe^{-c\sqrt{\log x}}).
\end{aligned}$$

Finalmente, como

$$\pi_1(x;q,a) = \sum_{\substack{n\leqslant x \\ n\equiv a(\text{mod } q)}} \frac{\Lambda(n)}{\log n} = \sum_{m=1}^{\infty} \sum_{\substack{p\leqslant \sqrt[m]{x} \\ p \text{ primo} \\ p^m\equiv a(\text{mod } q)}} \frac{1}{m} = \pi(x;q,a) + O\left(\sum_{m=2}^{\infty} \frac{\pi(\sqrt[m]{x})}{m}\right),$$

y como $\displaystyle\sum_{m=2}^{\infty} \frac{\pi(\sqrt[m]{x})}{m} = O\left(x^{\frac{1}{2}} \log x\right)$, se concluye la demostración. ■

Capítulo 4

El Problema Ternario de Goldbach

En este capítulo se demostrará que el Problema Ternario de Goldbach tiene solución para cualquier N suficientemente grande. Este resultado fue demostrado por Vinogradov en 1937. Se denotará por $J(N)$ a la cantidad de formas distintas de representar a N como suma de tres números primos, contando las posibles permutaciones, es decir

$$J(N) = \#\{p_1 + p_2 + p_3 = N \ : \ p_1, p_2, p_3 \text{ son primos}\}.$$

Por la ecuación (1.2), se tiene la siguiente representación

$$\begin{aligned} J(N) &= \int_0^1 \left(\sum_{p_i \text{ primo}} e^{2\pi i\alpha(p_1+p_2+p_3-N)} \right) d\alpha = \int_0^1 \left(\sum_{\substack{p \leqslant N \\ p \text{ primo}}} e^{2\pi i\alpha p} \right)^3 e^{-2\pi i\alpha N} d\alpha \\ &= \int_{-R}^{1-R} \left(\sum_{\substack{p \leqslant N \\ p \text{ primo}}} e^{2\pi i\alpha p} \right)^3 e^{-2\pi i\alpha N} d\alpha \end{aligned} \tag{4.1}$$

Nótese que E_1 y E_2 dependen de N. Se usarán las constantes $A = 6$, $B = 8$, $\tau = \frac{N}{(\log N)^B}$, $Q = (\log N)^A$ y $R = \frac{1}{\tau}$. Se definen también los conjuntos

$$E_1 = \bigcup_{q \leqslant Q} \bigcup_{\substack{0 \leqslant a \leqslant q-1 \\ (a,q)=1}} \left[\frac{a}{q} - \frac{1}{q\tau}, \frac{a}{q} + \frac{1}{q\tau} \right],$$

$$E_2 = \left[-\frac{1}{\tau}, 1 - \frac{1}{\tau} \right] \backslash E_1.$$

Se denotará por $S(\alpha) = S_N(\alpha) = \sum\limits_{\substack{p \leqslant N \\ p \text{ primo}}} e^{2\pi i\alpha p}$. Entonces

$$J(N) = \int_{-\frac{1}{\tau}}^{1-\frac{1}{\tau}} S(\alpha)^3 e^{-2\pi i\alpha N} d\alpha.$$

Definiendo $J_i(N) := \int_{E_i} S(\alpha)^3 e^{-2\pi i\alpha N} d\alpha$, resulta que $J(N) = J_1(N) + J_2(N)$.

Se demostrará más adelante que, para N impar suficientemente grande, se cumplen las igualdades

$$J_1(N) = \frac{N^2}{(\log N)^3}\sigma(N) + O\left(\frac{N^2}{(\log N)^4}\right), \tag{4.2}$$

$$J_2(N) = O\left(\frac{N^2}{(\log N)^4}\right), \tag{4.3}$$

donde $\frac{12}{\pi^2} \leqslant \sigma(N) \leqslant \frac{\pi^2}{3}$. De estas igualdades se puede deducir el siguiente teorema.

Teorema 4.1 (Vinogradov). *Para N impar suficientemente grande, existen p_1, p_2, p_3 números primos tales que*

$$N = p_1 + p_2 + p_3.$$

El resto del capítulo consiste en demostrar las ecuaciones (4.2) y (4.3).

4.1. Estimación para $J_1(N)$

Proposición 4.2. *Para N suficientemente grande se tiene que*
i) los intervalos de E_1 son ajenos,
ii) la medida de Lebesgue de E_1 está acotada por $\frac{2Q}{\tau}$.

Demostración. Sea N suficientemente grande tal que se cumpla la desigualdad

$$2Q = 2(\log N)^A < \frac{N}{(\log N)^B} = \tau.$$

Tomemos todos los centros de los intervalos de la definición de E_1 y consideremos dos de ellos que sean consecutivos, digamos $\frac{a}{q_1} < \frac{b}{q_2}$. Veamos que los intervalos con dichos centros son ajenos, ya que

$$\frac{a}{q_1} + \frac{1}{q_1\tau} < \frac{b}{q_2} - \frac{1}{q_2\tau} \Leftrightarrow aq_2\tau + q_2 < bq_1\tau - q_1 \Leftrightarrow q_1 + q_2 < (bq_1 - aq_2)\tau.$$

Por fracciones de Farey sabemos que $bq_1 - aq_2 = 1$, concluyendo así que los intervales son ajenos pues

$$q_1 + q_2 \leqslant 2Q < \tau = (bq_1 - aq_2)\tau.$$

Para la cota de su medida de Lebesgue basta ver que

$$\mathcal{M}(E_1) = \sum_{q\leqslant Q} \sum_{\substack{0\leqslant a\leqslant q-1 \\ (a,q)=1}} \mathcal{M}\left(\left[\frac{a}{q} - \frac{1}{q\tau}, \frac{a}{q} + \frac{1}{q\tau}\right]\right) = \sum_{q\leqslant Q} \sum_{\substack{0\leqslant a\leqslant q-1 \\ (a,q)=1}} \frac{2}{q\tau} \leqslant \sum_{q\leqslant Q} \frac{2}{\tau} \leqslant \frac{2Q}{\tau}.$$

■

De aquí en adelante se considerará N suficientemente grande, tal que asegure que $2Q < \tau$.

Se denotará por $M(z)$ a la suma

$$M(z) = \sum_{n=3}^{N} \frac{e^{2\pi i z n}}{\log n}.$$

Lema 4.3. *Sea $\alpha = \frac{a}{q} + z \in E_1$, donde $0 \leqslant a < q \leqslant Q$ y $(a,q) = 1$ y $|z| \leqslant \frac{1}{q\tau}$. Entonces*

$$S(\alpha) = \frac{\mu(q)}{\varphi(q)} M(z) + O\left(N e^{-c\sqrt{\log N}}\right)$$

para toda N suficientemente grande.

Demostración. Se tiene que

$$S(\alpha) = S\left(\frac{a}{q} + z\right) = \sum_{\substack{p \leqslant N \\ p \text{ primo}}} e^{2\pi i (\frac{a}{q} + z)p} = \sum_{\substack{\sqrt{N} < p \leqslant N \\ p \text{ primo}}} e^{2\pi i \frac{a}{q} p} e^{2\pi i z p} + O(\sqrt{N}).$$

Como $q \leqslant Q = (\log N)^A < (\log N)^{\frac{A+B}{2}} < \sqrt{N}$, lo anterior se reescribe como

$$S(\alpha) = \sum_{\substack{l=1 \\ (l,q)=1}}^{q} \sum_{\substack{\sqrt{N} < p \leqslant N \\ p \text{ primo} \\ p \equiv l (\text{mod } q)}} e^{2\pi i \frac{a}{q} p} e^{2\pi i z p} + O(\sqrt{N}) = \sum_{\substack{l=1 \\ (l,q)=1}}^{q} \sum_{\substack{\sqrt{N} < p \leqslant N \\ p \text{ primo} \\ p \equiv l (\text{mod } q)}} e^{2\pi i \frac{al}{q}} e^{2\pi i z p} + O(\sqrt{N}).$$

de donde se obtiene la igualdad

$$S(\alpha) = \sum_{\substack{l=1 \\ (l,q)=1}}^{q} e^{2\pi i \frac{al}{q}} \left[\sum_{\substack{\sqrt{N} < p \leqslant N \\ p \text{ primo} \\ p \equiv l (\text{mod } q)}} e^{2\pi i z p} \right] + O(\sqrt{N}).$$

Denotemos

$$T(l) = T_q(l) = \sum_{\substack{\sqrt{N} < p \leqslant N \\ p \text{ primo} \\ p \equiv l (\text{mod } q)}} e^{2\pi i z p} = \sum_{\sqrt{N} < n \leqslant \sqrt{N}} \left(\Pi(n; q, l) - \Pi(n-1; q, l)\right) e^{2\pi i z n}.$$

Aplicando la Fórmula de Sumación de Abel (Teorema 1.3) para

$$c_n = \Pi(n; q, l) - \Pi(n-1; q, l), \qquad f(n) = e^{2\pi i z n},$$

$$\mathcal{C}(u) = \sum_{\sqrt{N} < n \leqslant u} c_n = \Pi(u; q, l) + O(\sqrt{N}),$$

y usando el Teorema de Siegel-Walfisz (Teorema 3.43) para $\mathcal{C}(u)$, se tiene que

$$T(l) = \sum_{\sqrt{N} < n \leqslant N} c_n f(n) = -\int_{\sqrt{N}}^{N} \mathcal{C}(u) f'(u) du + \mathcal{C}(N) f(N)$$

$$= -\int_{\sqrt{N}}^{N} \frac{Li(u)}{\varphi(q)} f'(u) + \frac{Li(N)}{\varphi(q)} f(N) + O\bigg(\int_{\sqrt{N}}^{N} \Big(ue^{-c\sqrt{\log u}} + \sqrt{u}\Big)\,|z|du\bigg) + O(Ne^{-c\sqrt{\log N}})$$

$$= -\int_{\sqrt{N}}^{N} \frac{Li(u)}{\varphi(q)} f'(u) + \frac{Li(N)}{\varphi(q)} f(N) + O(Ne^{-c_1}\sqrt{(}\log N))$$

$$= -\frac{Li(u)}{\varphi(q)} f(u)\bigg|_{u=\sqrt{N}}^{N} + \int_{\sqrt{N}}^{N} \frac{f(u)}{\varphi(q)\log u} du + \frac{Li(N)}{\varphi(q)} f(N) + O(Ne^{-c_1\sqrt{\log N}})$$

$$= \frac{Li(\sqrt{N})}{\varphi(q)} f(\sqrt{N}) + \int_{\sqrt{N}}^{N} \frac{f(u)}{\varphi(q)\log u} du + O(Ne^{-c_1\sqrt{\log N}})$$

$$= \int_{\sqrt{N}}^{N} \frac{f(u)}{\varphi(q)\log u} du + O(Ne^{-c_1\sqrt{\log N}}) = \int_{3}^{N} \frac{f(u)}{\varphi(q)\log u} du + O(Ne^{-c_1\sqrt{\log N}}).$$

Por lo tanto,

$$S\left(\frac{a}{q} + z\right) = \sum_{\substack{l=1\\(l,q)=1}}^{q} e^{2\pi i \frac{al}{q}} \left[\frac{1}{\varphi(q)} \int_3^N \frac{e^{2\pi i z u}}{\log u} du\right] + O\left(Ne^{-c_2\sqrt{\log N}}\right).$$

Veamos ahora que, si $u \in [n, n+1]$, se tiene que

$$\frac{1}{\log u} = \frac{1}{\log n} + O\left(\frac{1}{n\log^2 n}\right),$$

por lo que, haciendo uso del Teorema del Valor Medio,

$$\left|\int_n^{n+1} \frac{e^{2\pi i z u}}{\log u} du - \frac{e^{2\pi i z n}}{\log n}\right| = \left|\int_n^{n+1} \left(\frac{e^{2\pi i z u}}{\log u} - \frac{e^{2\pi i z n}}{\log n}\right) du\right| \leqslant \max_{u\in[n,n+1]} \left|\frac{e^{2\pi i z u}}{\log u} - \frac{e^{2\pi i z n}}{\log n}\right|$$

$$\leqslant \max_{x\in[n,n+1]} \left|\frac{d}{dx}\frac{e^{2\pi i z x}}{\log x}\right| \leqslant \max_{x} \left|\frac{2\pi i z e^{2\pi i z x}}{\log x} - \frac{e^{2\pi i z x}}{x\log^2 x}\right| \leqslant \frac{2\pi|z|}{\log n} + \frac{1}{n\log^2 n} \ll \frac{(\log N)^B}{N},$$

por lo que se puede deducir que

$$\int_3^N \frac{e^{2\pi i z u}}{\log u} du = \sum_{n=3}^{N} \frac{e^{2\pi i z n}}{\log n} + O\Big((\log N)^B\Big).$$

Con lo anterior y usando el Teorema 1.1 se puede concluir que

$$S\left(\frac{a}{q} + z\right) = \sum_{\substack{l=1\\(l,q)=1}}^{q} e^{2\pi i \frac{al}{q}} \left[\frac{1}{\varphi(q)} \int_3^N \frac{e^{2\pi i z u}}{\log u} du\right] + O\left(Ne^{-c_2\sqrt{\log N}}\right)$$

$$= \frac{1}{\varphi(q)}\Bigg(\sum_{\substack{l=1\\(l,q)=1}}^{q} e^{2\pi i \frac{al}{q}}\Bigg) M(z) + O\Big(Ne^{-c_3\sqrt{\log N}}\Big) = \frac{\mu(q)}{\varphi(q)} M(z) + O\Big(Ne^{-c_3\sqrt{\log N}}\Big).$$

■

Teorema 4.4. *Para N suficientemente grande se cumple la igualdad*

$$J_1(N) = \sigma\delta + O\Big(N^2(\log N)^{-A-1}\Big) + O\Big(N^2(\log N)^{2A-2B}\Big),$$

donde

$$\sigma = \sigma(N) = \sum_{q=1}^{\infty} \gamma(q), \qquad \gamma(q) = \gamma(q,N) = \frac{\mu(q)}{(\varphi(q))^3} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e^{-2\pi i \frac{a}{q} N},$$

$$\delta = \delta(N) = \int_{-\frac{1}{2}}^{\frac{1}{2}} M^3(z) e^{-2\pi i z N} dz.$$

Demostración. Notemos primero que

$$J_1(N) = \int_{E_1} S^3(\alpha) e^{-2\pi i \alpha N} d\alpha = \sum_{q \leqslant Q} \sum_{\substack{0 \leqslant a < q \\ (a,q)=1}} \int_{\frac{a}{q}-\frac{1}{q\tau}}^{\frac{a}{q}+\frac{1}{q\tau}} \Bigg(\sum_{\substack{p \leqslant N \\ p \text{ primo}}} e^{2\pi i \alpha p} \Bigg)^3 e^{-2\pi i \alpha N} d\alpha$$

$$= \sum_{q \leqslant Q} \sum_{\substack{0 \leqslant a < q \\ (a,q)=1}} \int_{-\frac{1}{q\tau}}^{\frac{1}{q\tau}} \left(\frac{\mu(q)}{\varphi(q)} M(z) + O\left(N e^{-c\sqrt{\log N}} \right) \right)^3 e^{-2\pi i (\frac{a}{q}+z)N} dz$$

$$= \sum_{q \leqslant Q} \sum_{\substack{0 \leqslant a < q \\ (a,q)=1}} \int_{-\frac{1}{q\tau}}^{\frac{1}{q\tau}} \left(\frac{\mu(q)}{\varphi^3(q)} M^3(z) + O\left(N^3 e^{-c\sqrt{\log N}} \right) \right) e^{-2\pi i (\frac{a}{q}+z)N} dz$$

$$= \sum_{q \leqslant Q} \sum_{\substack{0 \leqslant a < q \\ (a,q)=1}} \frac{\mu(q)}{\varphi^3(q)} e^{-2\pi i \frac{a}{q} N} \int_{-\frac{1}{q\tau}}^{\frac{1}{q\tau}} M^3(z) e^{-2\pi i z N} dz + O\left(\frac{Q}{\tau} N^3 e^{-c\sqrt{\log N}} \right)$$

$$= \sum_{q \leqslant Q} \sum_{\substack{0 \leqslant a < q \\ (a,q)=1}} \frac{\mu(q)}{\varphi^3(q)} e^{-2\pi i \frac{a}{q} N} \int_{-\frac{1}{q\tau}}^{\frac{1}{q\tau}} M^3(z) e^{-2\pi i z N} dz + O\left(N^2 e^{-c_1\sqrt{\log N}} \right).$$

Sea $s_n = \sum_{j=3}^{n} e^{2\pi i z k}$. Para $|z| \leqslant \frac{1}{2}$ se tiene la estimación

$$|s_n| = \left| \sum_{k=0}^{n-3} e^{2\pi i z k} \right| \leqslant \left| \frac{\operatorname{sen}(\pi z(n-2))}{\operatorname{sen}(\pi z)} \right| \leqslant \frac{1}{|z|},$$

por lo tanto,

$$|M(z)| = \left| \sum_{n=3}^{N} \frac{s_n - s_{n-1}}{\log n} \right| = \left| \frac{s_N}{\log N} - \frac{s_2}{\log 3} + \sum_{n=3}^{N-1} s_n \left(\frac{1}{\log n} - \frac{1}{\log(n+1)} \right) \right|$$

$$\leqslant \frac{1}{|z|} + \frac{1}{|z|} \sum_{n=3}^{N-1} \left(\frac{1}{\log n} - \frac{1}{\log(n+1)} \right) \ll \frac{1}{|z|}.$$

Así, tenemos que $J_1(N)$ es igual a

$$\sum_{q\leqslant Q}\sum_{\substack{0\leqslant a<q\\(a,q)=1}}\frac{\mu(q)}{\varphi^3(q)}e^{-2\pi i\frac{a}{q}N}\left(\delta-\int_{-\frac{1}{2}}^{-\frac{1}{q\tau}}M^3(z)e^{-2\pi izN}dz-\int_{\frac{1}{q\tau}}^{\frac{1}{2}}M^3(z)e^{-2\pi izN}dz\right)+O\left(N^2e^{-c_1\sqrt{\log N}}\right).$$

Por la estimación para $M(z)$, se tiene que

$$\left|\int_{-\frac{1}{2}}^{-\frac{1}{q\tau}}M^3(z)e^{-2\pi izN}dz\right|\leqslant\int_{-\frac{1}{2}}^{-\frac{1}{q\tau}}\frac{1}{|z|^3}dz\leqslant(q\tau)^2\leqslant(Q\tau)^2=N^2(\log N)^{2A-2B},$$

entonces

$$\begin{aligned}
J_1(N)&=\sum_{q\leqslant Q}\sum_{\substack{0\leqslant a<q\\(a,q)=1}}\frac{\mu(q)}{\varphi^3(q)}e^{-2\pi i\frac{a}{q}N}\left(\delta+O\left(N^2(\log N)^{2A-2B}\right)\right)+O\left(N^2e^{-c_1\sqrt{\log N}}\right)\\
&=\delta\sum_{q\leqslant Q}\sum_{\substack{0\leqslant a<q\\(a,q)=1}}\frac{\mu(q)}{\varphi^3(q)}e^{-2\pi i\frac{a}{q}N}+O\left(N^2(\log N)^{2A-2B}\right)+O\left(N^2e^{-c_1\sqrt{\log N}}\right)\\
&=\delta\sum_{q\leqslant Q}\frac{\mu(q)}{\varphi^3(q)}\sum_{\substack{0\leqslant a<q\\(a,q)=1}}e^{-2\pi i\frac{a}{q}N}+O\left(N^2(\log N)^{2A-2B}\right).
\end{aligned}$$

Usando la conocida estimación $\frac{n}{\varphi(n)}=O(\log\log n)$ (ver [3, pp. 267]) tenemos que

$$\begin{aligned}
\sum_{q\leqslant Q}\frac{\mu(q)}{\varphi^3(q)}\sum_{\substack{0\leqslant a<q\\(a,q)=1}}e^{-2\pi i\frac{a}{q}N}&=\sigma-\sum_{q>Q}\frac{\mu(q)}{\varphi^3(q)}\sum_{\substack{0\leqslant a<q\\(a,q)=1}}e^{-2\pi i\frac{a}{q}N}=\sigma+O\left(\sum_{q>Q}\frac{1}{\varphi^2(q)}\right)\\
&=\sigma+O\left(\sum_{q>Q}\frac{(\log\log q)^2}{q^2}\right)\leqslant\sigma+O\left((\log\log Q^4)^2\sum_{Q<q\leqslant Q^4}\frac{1}{q^2}+\sum_{q>Q^4}\frac{1}{q^{\frac{3}{2}}}\right)\\
&\leqslant\sigma+O\left(\frac{\log N}{Q}\right)=\sigma+O((\log N)^{-A+1}).
\end{aligned}$$

Entonces $J_1(N)=\delta\sigma+O(\delta(\log N)^{-A+1})+O(N^2(\log N)^{2A-2B})$. Como

$$\begin{aligned}
|\delta|=\left|\int_{-\frac{1}{2}}^{\frac{1}{2}}M^3(z)e^{-2\pi izN}dz\right|&\leqslant\int_{-\frac{1}{2}}^{\frac{1}{2}}|M(z)|^3dz\leqslant N\int_{-\frac{1}{2}}^{\frac{1}{2}}\sum_{n=3}^{N}\sum_{m=3}^{N}\frac{e^{2\pi iz(n-m)}}{\log n\log m}dz\\
&=N\sum_{n=3}^{N}\frac{1}{(\log n)^2}=O\left(\frac{N^2}{(\log N)^2}\right),
\end{aligned}$$

se tiene que

$$J_1(N)=\delta\sigma+O(N^2(\log N)^{-A-1})+O(N^2(\log N)^{2A-2B}).$$

■

Lema 4.5. *Para N grande se tiene la igualdad*

$$\delta = \frac{N^2}{2(\log N)^3} + O\left(\frac{N^2}{(\log N)^4}\right).$$

Demostración. Defínase $M_0(z) = \sum_{n=3}^{N} \frac{e^{2\pi i z n}}{\log N}$. Nótese que

$$|M(z) - M_0(z)| \leqslant \sum_{n=3}^{N} \left| \frac{e^{2\pi i z n}}{\log n} - \frac{e^{2\pi i z n}}{\log N} \right| = \sum_{n=3}^{N} \left(\frac{1}{\log n} - \frac{1}{\log N} \right) \leqslant \int_2^N \frac{1}{\log x} dx - \frac{N-2}{\log N}$$

$$= \frac{x}{\log x}\bigg|_{x=2}^{N} - \int_2^N x \left(\frac{1}{\log x}\right)' dx - \frac{N}{\log N} + \frac{2}{\log N} = \int_2^N \frac{1}{(\log x)^2} dx - \frac{2}{\log 2} + \frac{2}{\log N} \ll \frac{N}{(\log N)^2}.$$

Sea $\delta_0 = \int_{-\frac{1}{2}}^{\frac{1}{2}} (M_0(z))^3 e^{-2\pi i z N} dz$, entonces

$$|\delta - \delta_0| = \left| \int_{-\frac{1}{2}}^{\frac{1}{2}} \left(M^3(z) - M_0^3(z)\right) e^{-2\pi i z N} dz \right| \leqslant \int_{-\frac{1}{2}}^{\frac{1}{2}} |M(z) - M_0(z)||M^2(z) + 2M(z)M_0(z) + M_0^2(z)| dz$$

$$\ll \frac{N}{(\log N)^2} \int_{-\frac{1}{2}}^{\frac{1}{2}} |M^2(z) + M_0^2(z)| dz \ll \frac{N^2}{(\log N)^4}.$$

Esta última desigualdad se cumple ya que, por la ecuación (1.2), se tiene

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} |M^2(z)| dz = \int_{-\frac{1}{2}}^{\frac{1}{2}} \sum_{n_1=3}^{N} \sum_{n_2=3}^{N} \frac{e^{2\pi i (n_1 - n_2) z}}{\log n_1 \log n_2} dz = \sum_{n=3}^{N} \frac{1}{\log^2 n} \ll \sqrt{N} + \frac{N}{\log^2 N} \ll \frac{N}{\log^2 N}$$

y

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} |M_0^2(z)| dz = \int_{-\frac{1}{2}}^{\frac{1}{2}} \sum_{n_1=3}^{N} \sum_{n_2=3}^{N} \frac{e^{2\pi i (n_1 - n_2) z}}{\log^2 N} dz = \sum_{n=3}^{N} \frac{1}{\log^2 N} \ll \frac{N}{\log^2 N}$$

Como

$$\delta_0 = \int_{-\frac{1}{2}}^{\frac{1}{2}} \left(\sum_{n=3}^{N} \frac{e^{2\pi i z n}}{\log N} \right)^3 e^{-2\pi i z N} dz = \frac{1}{(\log N)^3} \sum_{\substack{3 \leqslant n_1, n_2, n_3 \leqslant N \\ n_1 + n_2 + n_3 = N}} 1 = \frac{1}{(\log N)^3} \sum_{n=3}^{N-6} (N - n - 5)$$

$$= \frac{1}{(\log N)^3} \left((N-5)(N-8) + 3 - \frac{(N-5)(N-6)}{2} \right) = \frac{N^2}{2(\log N)^3} + O\left(\frac{N}{(\log N)^3} \right),$$

se puede concluir que

$$\delta = \delta_0 + O\left(\frac{N^2}{(\log N)^4}\right) = \frac{N^2}{2(\log N)^3} + O\left(\frac{N}{(\log N)^3}\right) + O\left(\frac{N^2}{(\log N)^4}\right) = \frac{N^2}{2(\log N)^3} + O\left(\frac{N^2}{(\log N)^2}\right).$$

■

Lema 4.6. *Se cumple la igualdad*

$$\sigma = \sigma(N) = \prod_{\substack{p|N \\ p \text{ primo}}} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{\substack{p \nmid N \\ p \text{ primo}}} \left(1 + \frac{1}{(p-1)^3}\right)$$

y, existen $D_1, D_2 > 0$ tales que $D_1 < \sigma(N) < D_2$ para todo N impar.

Demostración. Denotemos por $R(q) = \sum_{\substack{0\leqslant a<q \\ (a,q)=1}} e^{-2\pi i \frac{a}{q} N}$. Veamos que $R(q)$ es multiplicativa ya que, si $(q_1, q_2) = 1$, se tiene que

$$R(q_1q_2) = \sum_{\substack{0\leqslant a<q_1q_2 \\ (a,q_1q_2)=1}} e^{-2\pi i \frac{a}{q_1q_2} N} = \sum_{\substack{0\leqslant x<q_2 \\ (x,q_2)=1}} \sum_{\substack{0\leqslant y<q_1 \\ (y,q_1)=1}} e^{-2\pi i \frac{q_1x+q_2y}{q_1q_2} N}$$

$$= \left(\sum_{\substack{0\leqslant x<q_2 \\ (x,q_2)=1}} e^{-2\pi i \frac{x}{q_2} N}\right)\left(\sum_{\substack{0\leqslant y<q_1 \\ (y,q_1)=1}} e^{-2\pi i \frac{y}{q_1} N}\right) = R(q_1)R(q_2).$$

Como $R(q)$, $\mu(q)$ y $\varphi(q)$ son multiplicativas, se tiene que $\gamma(q) = \frac{\mu(q)}{\varphi^3(q)} R(q)$ es multiplicativa. Notemos que $|\gamma(q)| \leqslant \frac{1}{\varphi^2(q)} \ll \frac{(\log\log q)^2}{q^2}$, por lo tanto, $\sum_{q=1}^{\infty} \gamma(q)$ converge. Además se tiene que

$$\sigma = \sum_{q=1}^{\infty} \gamma(q) = \lim_{x\to\infty} \left(\sum_{q\leqslant x} \gamma(q) + O\left(\sum_{q>x} \frac{(\log\log q)^2}{q^2}\right)\right)$$

$$= \lim_{x\to\infty} \prod_{\substack{p\leqslant x \\ p \text{ primo}}} \left(1 + \gamma(p) + \gamma(p^2) + \cdots\right) = \prod_{p \text{ primo}} \left(1 + \gamma(p) + \gamma(p^2) + \cdots\right),$$

y como para cualquier $k > 1$, $\gamma(p^k) = 0$ ya que $\mu(p^k) = 0$, se deduce que $\sigma = \prod_{p \text{ primo}} (1 + \gamma(p))$. Veamos ahora que, por el Teorema 1.1, se cumple que para todo primo p,

$$\gamma(p) = -\frac{1}{(p-1)^3} \sum_{a=1}^{p-1} e^{-2\pi i \frac{a}{p} N} = \begin{cases} -\frac{1}{(p-1)^2} & \text{si } p|N \\ \frac{1}{(p-1)^3} & \text{si } p \nmid N \end{cases}$$

concluyendo entonces que

$$\sigma = \sigma(N) = \prod_{\substack{p|N \\ p \text{ primo}}} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{\substack{p \nmid N \\ p \text{ primo}}} \left(1 + \frac{1}{(p-1)^3}\right).$$

Ahora, para ver que σ está acotado por abajo basta ver que, si N es impar, entonces

$$\sigma = \prod_{\substack{p|N \\ p \text{ primo}}} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{\substack{p \nmid N \\ p \text{ primo}}} \left(1 + \frac{1}{(p-1)^3}\right) \geqslant \left(1 + \frac{1}{(2-1)^3}\right) \prod_{\substack{p \text{ primo} \\ p\geqslant 3}} \left(1 - \frac{1}{(p-1)^2}\right)$$

$$> 2 \prod_{p \text{ primo}} \left(1 - \frac{1}{p^2}\right) = \frac{2}{\zeta(2)} = \frac{12}{\pi^2}.$$

Para ver que σ está acotado por arriba basta ver que

$$\sigma = \prod_{\substack{p|N \\ p \text{ primo}}} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{\substack{p\nmid N \\ p \text{ primo}}} \left(1 + \frac{1}{(p-1)^3}\right) \leqslant \prod_{p \text{ primo}} \left(1 + \frac{1}{(p-1)^3}\right)$$

$$= 2 \prod_{\substack{p \text{ primo} \\ p\geqslant 3}} \left(1 + \frac{1}{(p-1)^3}\right) \leqslant 2 \prod_{p \text{ primo}} \left(1 + \frac{1}{p^2}\right) = 2\zeta(2) = \frac{\pi^2}{3}.$$

■

Teorema 4.7. *Para todo N impar suficientemente grande se tiene que*

$$J_1(N) = \frac{N^2}{2(\log N)^3}\sigma + O\left(\frac{N^2}{(\log N)^4}\right).$$

Demostración. Partiendo del Teorema 4.4 y aplicando los Lemas 4.5 y 4.6 se tiene que

$$J_1(N) = \delta\sigma + O\left(N^2(\log N)^{-A-1}\right) + O(N^2(\log N)^{2A-2B})$$

$$= \frac{N^2}{2(\log N)^3}\sigma + \sigma O\left(\frac{N^2}{(\log N)^4}\right) + O\left(N^2(\log N)^{-A-1}\right) + O(N^2(\log N)^{2A-2B})$$

$$= \frac{N^2}{2(\log N)^3}\sigma + O\left(\frac{N^2}{(\log N)^4}\right).$$

■

4.2. Estimación para $J_2(N)$

Proposición 4.8. *Dado $\alpha \in E_2$, existen a, q enteros primos relativos entre sí con $Q < q \leqslant \tau$ y $0 \leqslant a < q$, tales que*

$$\left|\alpha - \frac{a}{q}\right| \leqslant \frac{1}{q^2}.$$

Demostración. Por el Teorema de aproximación de Dirichlet (Teorema 1.2) sabemos que existen a, q enteros primos relativos entre sí con $1 \leqslant q \leqslant \tau$ y $0 \leqslant a < q$ tales que

$$\left|\alpha - \frac{a}{q}\right| \leqslant \frac{1}{q\tau} \leqslant \frac{1}{q^2}.$$

Como $\alpha \notin E_1$, no existe $q \leqslant Q$ con las propiedades anteriores. Por lo tanto, $Q < q$, como se buscaba demostrar. ■

Se denotará por $\hat{S}(\alpha)$ a la suma

$$\hat{S}(\alpha) = \hat{S}_N(\alpha) = \sum_{n\leqslant N} \Lambda(n)e^{2\pi i\alpha n}.$$

Una relación entre $S(\alpha)$ y $\hat{S}(\alpha)$ que puede deducirse fácilmente con la Fórmula de Sumación de Abel se presenta en el siguiente lema.

Lema 4.9. *Se tiene la igualdad*

$$S(\alpha) = -\int_{1.9}^{N} \frac{\hat{S}(u)}{u\log^2 u}du + \frac{\hat{S}(N)}{\log N} + O(\sqrt{N}\log^2 N).$$

Demostración. Se aplicará la Fórmula de Sumación de Abel (Teorema 1.3) para $S(\alpha)$, con

$$c_n = \begin{cases} \log n\, e^{2\pi izn} & \text{si } n \text{ es primo,} \\ 0 & \text{en otro caso.} \end{cases}$$

$$\mathcal{C}(u) = \sum_{1.9<n\leqslant u} c_n.$$

Entonces

$$S(\alpha) = \sum_{1.9<n\leqslant N} (c_n e^{2\pi izn})\frac{1}{\log n} = -\int_{1.9}^{N} \mathcal{C}(u)\frac{1}{u\log^2 u}du + \mathcal{C}(N)\frac{1}{\log N}.$$

Nótese que

$$\mathcal{C}(u) = \hat{S}(u) - \sum_{n=2}^{\infty}\sum_{p^n\leqslant u} \log p\, e^{2\pi i\alpha p^n} = \hat{S}(u) + O\left(\log u \sum_{n=2}^{\log_2 u} \sqrt[n]{u}\right) = \hat{S}(u) + O(\sqrt{u}\log^2 u),$$

por lo que se concluye que

$$\begin{aligned} S(\alpha) &= -\int_{1.9}^{N} \mathcal{C}(u)\frac{1}{u\log^2 u}du + \mathcal{C}(N)\frac{1}{\log N} \\ &= -\int_{1.9}^{N} \frac{\hat{S}(u)}{u\log^2 u}du + \int_{1.9}^{N} O\left(\frac{1}{\sqrt{u}}\right)du + \frac{\hat{S}(N)}{\log N} + O(\sqrt{N}\log^2 N) \\ &= -\int_{1.9}^{N} \frac{\hat{S}(u)}{u\log^2 u}du + \frac{\hat{S}(N)}{\log N} + O(\sqrt{N}\log^2 N). \end{aligned}$$

■

Teorema 4.10. *Para cualquier $\alpha \in \mathbb{R}$, y U, V reales positivos se tiene que*

$$\sum_{n\leqslant N} \Lambda(n)e^{2\pi i\alpha n} \ll (W_1 + W_2 + W_3 + W_4)(\log N),$$

donde

$$W_1 = \left| \sum_{n \leqslant U} \Lambda(n) e^{2\pi i \alpha n} \right| \qquad W_3 = \sum_{n \leqslant V} \left| \sum_{m \leqslant \frac{N}{n}} \log m e^{2\pi i \alpha n m} \right|$$

$$W_2 = \sum_{n \leqslant UV} \left| \sum_{m \leqslant \frac{N}{n}} e^{2\pi i \alpha n m} \right| \qquad W_4 = \sum_{U < n \leqslant \frac{N}{V}} \Lambda(n) \left| \sum_{V < m \leqslant \frac{N}{n}} \omega_m e^{2\pi i \alpha n m} \right|,$$

con $\omega_m = \sum_{\substack{d|m \\ d \leqslant V}} \mu(d)$.

Demostración. Por la Identidad de Vaughan (Teorema 2.30) se tiene que

$$\sum_{n \leqslant N} \Lambda(n) e^{2\pi i \alpha n} = \sum_{n \leqslant N} \Lambda_1(n) e^{2\pi i \alpha n} + \sum_{n \leqslant N} \Lambda_2(n) e^{2\pi i \alpha n} + \sum_{n \leqslant N} \Lambda_3(n) e^{2\pi i \alpha n} + \sum_{n \leqslant N} \Lambda_4(n) e^{2\pi i \alpha n}.$$

Se concluirá acotando cada una de estas sumas como sigue

i] $$\left| \sum_{n \leqslant N} \Lambda_1(n) e^{2\pi i \alpha n} \right| = \left| \sum_{n \leqslant U} \Lambda(n) e^{2\pi i \alpha n} \right| = W_1,$$

ii] $$\left| \sum_{n \leqslant N} \Lambda_2(n) e^{2\pi i \alpha n} \right| = \left| \sum_{n \leqslant N} \sum_{\substack{mdr = n \\ m \leqslant U \\ d \leqslant V}} \Lambda(m) \mu(d) e^{2\pi i \alpha n} \right| = \left| \sum_{\substack{mdr \leqslant N \\ m \leqslant U \\ d \leqslant V}} \Lambda(m) \mu(d) e^{2\pi i \alpha m d r} \right|$$

$$\leqslant \sum_{\substack{m \leqslant U \\ d \leqslant V}} \log N \left| \sum_{r \leqslant \frac{N}{md}} e^{2\pi i \alpha m d r} \right| = \log N \sum_{n \leqslant UV} \left| \sum_{r \leqslant \frac{N}{md}} e^{2\pi i \alpha r n} \right| = W_2 \log N,$$

iii] $$\left| \sum_{n \leqslant N} \Lambda_3(n) e^{2\pi i \alpha n} \right| = \left| \sum_{n \leqslant N} \sum_{\substack{hd = n \\ d \leqslant V}} \mu(d) \log h e^{2\pi i \alpha n} \right| = \left| \sum_{\substack{hd \leqslant n \\ d \leqslant V}} \mu(d) \log h e^{2\pi i \alpha n} \right|$$

$$\leqslant \sum_{d \leqslant V} \left| \sum_{h \leqslant \frac{N}{d}} \log h e^{2\pi i \alpha h d} \right| = W_3,$$

iv] $$\left| \sum_{n \leqslant N} \Lambda_4(n) e^{2\pi i \alpha n} \right| = \left| \sum_{n \leqslant N} \sum_{\substack{mk = n \\ m > U \\ k > 1}} \Lambda(m) \left(\sum_{\substack{d|k \\ d \leqslant V}} \mu(d) \right) e^{2\pi i \alpha n} \right|$$

$$= \left| \sum_{\substack{mk \leqslant N \\ m > U \\ k > V}} \Lambda(m) \left(\sum_{\substack{d|k \\ d \leqslant V}} \mu(d) \right) e^{2\pi i \alpha m k} \right| = \left| \sum_{\substack{mk \leqslant N \\ m > U \\ k > V}} \Lambda(m) \omega_k e^{2\pi i \alpha m k} \right| = W_4.$$

■

Definición 4.11. Se definirá la función $|\cdot|_* : \mathbb{R} \to \left[0, \frac{1}{2}\right]$ como

$$|x|_* = \min\{\{x\}, 1 - \{x\}\}.$$

Lema 4.12. *Sean* $\alpha = \frac{a}{q} + \frac{\theta}{q^2}$, *donde* $(a, q) = 1$, $q \geqslant 1$ *y* $|\theta| \leqslant 1$. *Entonces, para cualquier*

$\beta \in \mathbb{R}, U > 0, P \geqslant 1$ se cumple la desigualdad

$$\sum_{x=1}^{P} \text{mín}\left\{U, \frac{1}{||\alpha x + \beta||}\right\} \leqslant 5\left(\frac{P}{q}+1\right)(U + q\log q).$$

Demostración. Es suficiente ver que para cualquier $k \in \mathbb{N}$ se cumple la desigualdad

$$\sum_{x=(k-1)q+1}^{kq} \text{mín}\left\{U, \frac{1}{|\alpha x + \beta|_*}\right\} = \sum_{x=1}^{q} \text{mín}\left\{U, \frac{1}{|\alpha x + \alpha(k-1)q + \beta|_*}\right\} \leqslant 5(U + q\log q).$$

Sea $\eta = \alpha\left((k-1)q + 1 + \left\lfloor \frac{q}{2} \right\rfloor\right) + \beta$. Se tiene que

$$\sum_{x=1}^{q} \text{mín}\left\{U, \frac{1}{|\alpha x + \alpha(k-1)q + \beta|_*}\right\} \leqslant \sum_{x=-\frac{q}{2}}^{\frac{q}{2}} \text{mín}\left\{U, \frac{1}{|\alpha x + \alpha(k-1)q + \beta|_*}\right\}.$$

Nótese que

$$\alpha x + \eta = \left(\frac{a}{q} + \frac{\theta}{q^2}\right)x + \eta = \frac{ax + \eta q}{q} + \frac{\theta x}{q^2} = \frac{ax + \lfloor \eta q \rfloor}{q} + \frac{\{\eta q\} + \frac{\theta x}{q}}{q}.$$

Como $\{\eta q\} + \frac{\theta x}{q} < 2$, y como cuando x recorre un sistema completo de residuos módulo q, también lo hace $ax + \lfloor \eta q \rfloor$, se concluye que

$$\sum_{x=-\frac{q}{2}}^{\frac{q}{2}} \text{mín}\left\{U, \frac{1}{|\alpha x + \alpha(k-1)q + \beta|_*}\right\} = \sum_{|y| \leqslant \frac{q}{2}} \text{mín}\left\{U, \frac{1}{\left|\frac{y}{q} + \frac{\theta(y)}{q}\right|_*}\right\}$$

$$\leqslant 5U + \sum_{3 \leqslant |y| \leqslant \frac{q}{2}} \frac{1}{\left|\frac{y}{q} + \frac{\theta(y)}{q}\right|_*} \leqslant 5U + \sum_{3 \leqslant |y| \leqslant \frac{q}{2}} \frac{1}{\frac{|y|-2}{q}} \leqslant 5(U + q\log q).$$

∎

Lema 4.13. *Sean $\alpha = \frac{a}{q} + \frac{\theta}{q^2}$, donde $(a,q) = 1$, $q \geqslant 1$ y $|\theta| \leqslant 1$. Para cualquier $C \geqslant 2$ y $N \geqslant 1$ se tiene que*

$$\sum_{t=1}^{T} \text{mín}\left\{\frac{N}{t}, \frac{1}{|\alpha t|_*}\right\} \ll \left(\frac{N}{q} + T + q\right)\log(2qT).$$

Demostración. Sean

$$R_1 = \sum_{t < \frac{q}{3}} \text{mín}\left\{\frac{N}{t}, \frac{1}{|\alpha t|_*}\right\} \qquad R_2 = \sum_{\frac{q}{3} \leqslant t \leqslant T} \text{mín}\left\{\frac{N}{t}, \frac{1}{|\alpha t|_*}\right\}.$$

Notemos que, si $t \leqslant \frac{q}{3}$, se puede escribir

$$\frac{1}{|\alpha t|_*} = \frac{1}{\left|\frac{at}{q} + \frac{\theta t}{q^2}\right|_*} = \frac{1}{\left|\frac{n}{q} + \frac{\theta(n)}{q}\right|_*}$$

donde $n = at$ y $|\theta(n)| \leqslant \frac{1}{3}$. Nótese que cuando t recorre los números $1, 2, \ldots, \frac{q}{3}$, los números at y $-at$ son todos distintos módulo q, entonces

$$R_1 \leqslant \sum_{t<\frac{q}{3}} \frac{1}{|\alpha t|_*} \leqslant \sum_{n\leqslant q-1} \frac{1}{\left|\frac{n}{q} + \frac{\theta(n)}{q}\right|_*} = \sum_{n\leqslant\frac{q}{2}} \frac{1}{\frac{n}{q} - \frac{1}{3q}} + \sum_{\frac{q}{2}<n\leqslant q-1} \frac{1}{1 - \frac{n}{q} - \frac{1}{3q}}$$

$$= \sum_{n\leqslant\frac{q}{2}} \frac{3q}{3n-1} + \sum_{\frac{q}{2}<n\leqslant q-1} \frac{3q}{3(q-n)-1} \ll q\log q,$$

$$R_2 \leqslant \sum_{\substack{k=0\\ L=2^k\frac{q}{3}}}^{\log_2\frac{3T}{q}} \sum_{t=L}^{2L-1} \text{mín}\left\{\frac{N}{L}, \frac{1}{|\alpha t|_*}\right\} \ll \sum_{\substack{k=0\\ L=2^k\frac{q}{3}}}^{\log_2\frac{3T}{q}} \left(\frac{L}{q}+1\right)\left(\frac{N}{L} + q\log q\right)$$

$$\ll \sum_{\substack{k=0\\ L=2^k\frac{q}{3}}}^{\log_2\frac{3T}{q}} \frac{L}{q}\left(\frac{N}{L} + q\log q\right) \ll \sum_{\substack{k=0\\ L=2^k\frac{q}{3}}}^{\log_2\frac{3T}{q}} \frac{N}{q} + L\log q$$

$$\ll \frac{N}{q}\log 2T + \frac{q}{3}(1+2+4+\cdots+2^{\lfloor\log_2\frac{3T}{q}\rfloor})\log q \ll \left(\frac{N}{q}+T\right)\log(2qT).$$

Por lo tanto

$$\sum_{t=1}^{T} \text{mín}\left\{\frac{N}{t}, \frac{1}{|\alpha t|_*}\right\} \ll \left(\frac{N}{q} + T + q\right)\log(2qT).$$

■

Teorema 4.14. *Sea $\alpha \in E_2$. Entonces se cumple la estimación*

$$\left|\sum_{n\leqslant N} \Lambda(n)e^{2\pi i\alpha n}\right| \ll \left(Nq^{-1/2} + N^{4/5} + N^{1/2}q^{1/2}\right)(\log N)^5.$$

Demostración. Sea $\alpha = \dfrac{a}{q} + \dfrac{\theta}{q^2}$, con $Q < q \leqslant \tau$, $0 \leqslant a < q$, $(a, q) = 1$ y $|\theta| < 1$. Se puede suponer que $N > q$, ya que en otro caso, la suma se estima trivialmente por $N\log N \ll N^{1/2}q^{1/2}\log N$. Usando el Teorema 4.10 y su notación, para $U, V = N^{2/5}$ se deducen las siguientes cotas

Cota para W_1: Es claro que $W_1 = \left|\sum_{n\leqslant U} \Lambda(n)e^{2\pi i\alpha n}\right| \leqslant \sum_{n\leqslant U} \log n \leqslant N^{2/5}\log N$.

Cota para W_2: Notemos primero que, trivialmente

$$\left|\sum_{m\leqslant P} e^{2\pi i\alpha nm}\right| \leqslant P$$

y

$$\left|\sum_{m\leqslant P} e^{2\pi i\alpha nm}\right| = \left|\frac{e^{2\pi i\alpha nP}-1}{e^{2\pi i\alpha n}-1}\right| = \left|\frac{\text{sen}(\pi\alpha nP)}{\text{sen}(\pi\alpha n)}\right| \leqslant \frac{1}{|\text{sen}(\pi\alpha n)|} \leqslant \frac{1}{|\alpha n|_*}.$$

Entonces, por el Lema 4.13 se tiene que

$$W_2 = \sum_{n\leqslant UV}\left|\sum_{m\leqslant \frac{N}{m}} e^{2\pi i\alpha nm}\right| \leqslant \sum_{n\leqslant N^{4/5}} \text{mín}\left\{\frac{N}{n}, \frac{1}{|\alpha n|_*}\right\} \ll \left(\frac{N}{q} + N^{4/5} + q\right)\log N.$$

Cota para W_3: Usando la Fórmula de Sumación de Abel (Teorema 1.3) para $c_k = e^{2\pi i\alpha nk}$ y $f(k) = \log k$ se tiene que

$$\left|\sum_{1<m\leqslant \frac{N}{n}} (\log m)e^{2\pi i\alpha nm}\right| = \left| -\int_1^{\frac{N}{n}} \left(\sum_{m\leqslant s} e^{2\pi i\alpha ns}\right)\frac{1}{s}ds + \left(\sum_{m\leqslant \frac{N}{n}} e^{2\pi i\alpha nm}\right)\log\frac{N}{n}\right|$$

$$\leqslant \int_1^{\frac{N}{n}} \text{mín}\left\{\frac{N}{n}, \frac{1}{|\alpha n|_*}\right\}\frac{1}{s}ds + \text{mín}\left\{\frac{N}{n}, \frac{1}{|\alpha n|_*}\right\}\log N \ll \text{mín}\left\{\frac{N}{n}, \frac{1}{|\alpha n|_*}\right\}\log N,$$

y nuevamente, por el Lema 4.13, se tiene que

$$W_3 = \sum_{n\leqslant V}\left|\sum_{m\leqslant \frac{N}{n}} \log m e^{2\pi i\alpha nm}\right| \ll \sum_{n\leqslant N^{2/5}} \text{mín}\left\{\frac{N}{n}, \frac{1}{|\alpha n|_*}\right\}\log N \ll \left(\frac{N}{q} + N^{2/5} + q\right)(\log N)^2.$$

Cota para W_4: Notemos primero que $|\omega_m| = \left|\sum_{\substack{d|m\\ d\leqslant V}} \mu(d)\right| \leqslant d(m)$, donde $d(m)$ denota el número de divisores de m (ver [4, pp. 233]). Usando la estimación del problema del número de divisores de Dirichlet que dice que $\sum_{n\leqslant x} d(n) \ll x\log x$, se deduce que

$$\sum_{m\leqslant k}|\omega_m|^2 \leqslant \sum_{m\leqslant k} d(m)^2 = \sum_{uv\leqslant k} d(uv) \leqslant \sum_{uv\leqslant k} d(u)d(v) \leqslant 2\sum_{u\leqslant k^{1/2}} d(u)\sum_{v\leqslant \frac{k}{u}} d(v)$$

$$\ll \sum_{u\leqslant k^{1/2}} d(u)\frac{k}{u}\log\frac{k}{u} \ll k\log k\sum_{u\leqslant k^{1/2}}\frac{d(u)}{u} \ll k\log k\left(2 + \sum_{1\leqslant k\leqslant \log_2 k^{1/2}}\ \sum_{u=2^k+1}^{2^{k+1}}\frac{u}{2^k}\right)$$

$$\ll k\log k\left(2 + 2(\log 4 + \log 8 + \cdots + \log 2^{\lceil \log_2(k^{1/2})\rceil})\right)$$

$$\ll k\log k(2 + 3 + 4 + \cdots + \log k) \ll k(\log k)^3.$$

Notemos también que, para j fijo, se tiene que

$$\sum_{\substack{k\neq j\\ 0<k\leqslant T}} \text{mín}\left(\frac{N}{k}, \frac{N}{j}, \frac{1}{|\alpha(k-j)|_*}\right) \ll \sum_{0<t\leqslant T} \text{mín}\left(\frac{N}{t}, \frac{1}{|\alpha t|_*}\right) \ll \left(\frac{N}{q} + T + q\right)\log(2qT).$$

Entonces

$$W_4 = \sum_{U<n\leqslant \frac{N}{V}} \Lambda(n)\left|\sum_{V<m\leqslant \frac{N}{n}} \omega_m e^{2\pi i\alpha nm}\right| \ll (\log N)^2\sum_{M<n\leqslant 2M}\left|\sum_{V<m\leqslant \frac{N}{n}} \omega_m e^{2\pi i\alpha nm}\right|,$$

por lo tanto

$$
\begin{aligned}
W_4^2 &\ll M(\log N)^4 \sum_{M<n\leqslant 2M} \left| \sum_{V<m\leqslant \frac{N}{n}} \omega_m e^{2\pi i\alpha nm} \right|^2 = M(\log N)^4 \sum_{\substack{M<n\leqslant 2M \\ V<m_1,m_2\leqslant \frac{N}{n}}} \omega_{m_1}\overline{\omega_{m_2}} e^{2\pi i\alpha n(m_1-m_2)} \\
&\leqslant M(\log N)^4 \sum_{V<m_1,m_2\leqslant \frac{N}{n}} |\omega_{m_1}\omega_{m_2}| \left| \sum_{M<n\leqslant \text{mín}\left\{2M, \frac{N}{m_1}, \frac{N}{m_2}\right\}} e^{2\pi i\alpha n(m_1-m_2)} \right| \\
&\ll M(\log N)^4 M\frac{N}{M}(\log N)^3 + M(\log N)^4 \sum_{\substack{V<m_1,m_2\leqslant \frac{N}{M} \\ m_1\neq m_2}} (\omega_{m_1}^2+\omega_{m_2}^2)\,\text{mín}\left\{M, \frac{1}{|\alpha(m_1-m_2)|_*}\right\} \\
&\ll N^{8/5}(\log N)^7 + M(\log N)^4 \sum_{\substack{V<m_1,m_2\leqslant \frac{N}{M} \\ m_1\neq m_2}} |\omega_{m_1}|^2\,\text{mín}\left\{M, \frac{1}{|\alpha(m_1-m_2)|_*}\right\} \\
&= N^{8/5}(\log N)^7 + M(\log N)^4 \sum_{V<m_1\leqslant \frac{N}{M}} \omega_{m_1}^2 \left(\sum_{\substack{V<m_2\leqslant \frac{N}{M} \\ m_2\neq m_1}} \text{mín}\left\{M, \frac{1}{|\alpha(m_1-m_2)|_*}\right\} \right) \\
&\leqslant N^{8/5}(\log N)^7 + M(\log N)^4 \sum_{V<m_1\leqslant \frac{N}{M}} \omega_{m_1}^2 \left(\sum_{\substack{V<m_2\leqslant \frac{N}{M} \\ m_2\neq m_1}} \text{mín}\left\{M, \frac{1}{|\alpha(m_1-m_2)|_*}\right\} \right) \\
&\leqslant N^{8/5}(\log N)^7 + M(\log N)^4 \sum_{V<m_1\leqslant \frac{N}{M}} \omega_{m_1}^2 \left(\sum_{\substack{V<m_2\leqslant \frac{N}{M} \\ m_2\neq m_1}} \text{mín}\left\{\frac{N}{m_1}, \frac{N}{m_2}, \frac{1}{|\alpha(m_1-m_2)|_*}\right\} \right) \\
&\ll N^{8/5}(\log N)^7 + M(\log N)^4 \left(\sum_{V<m_1\leqslant \frac{N}{M}} \omega_{m_1}^2 \right) \left(\frac{N}{q} + \frac{N}{M} + q \right) \log N \\
&\ll N^{8/5}(\log N)^7 + M\log N^5 \frac{N}{M} \left(\log\frac{N}{M}\right)^3 \left(\frac{N}{q} + N^{3/5} + q\right) \ll (\log N)^8 \left(\frac{N^2}{q} + N^{8/5} + Nq\right).
\end{aligned}
$$

Por lo tanto,

$$W_4 \ll \left(Nq^{-1/2} + N^{4/5} + N^{1/2}q^{1/2}\right)(\log N)^4.$$

Entonces se puede conluir que

$$\sum_{n=1}^{N} \Lambda(n)e^{2\pi i\alpha n} \ll (W_1+W_2+W_3+W_4)\log N \ll (Nq^{-1/2} + N^{4/5} + N^{1/2}q^{1/2})(\log N)^5.$$

■

Corolario 4.15. *Si* $\alpha \in E_2$, *con* $\alpha = \frac{a}{q} + \frac{\theta}{q^2}$ *y* $|\theta| \leqslant 1$, *entonces*

$$S(\alpha) = O\left(\frac{N}{(\log N)^3}\right)$$

Demostración. Por el Lema 4.9 y el Teorema 4.14 se deduce que

$$\begin{aligned} S(\alpha) &= -\int_{1.9}^{N} \frac{\hat{S}(u)}{u\log^2 u}du + \frac{\hat{S}(N)}{\log N} + O(\sqrt{N}\log^2 N) \\ &= -\int_{1.9}^{N} \frac{O((Nq^{-1/2} + N^{4/5} + N^{1/2}q^{1/2})(\log N)^5)}{u\log^2 u}du \\ &\quad + \frac{O((Nq^{-1/2} + N^{4/5} + N^{1/2}q^{1/2})(\log N)^5)}{\log N} + O(\sqrt{N}\log^2 N) \\ &= O\Big((Nq^{-1/2} + N^{4/5} + N^{1/2}q^{1/2})(\log N)^5\Big). \end{aligned}$$

Luego, como $q \leqslant \tau = \frac{N}{(\log N)^B}$ y $\frac{1}{q} \leqslant \frac{1}{(\log N)^A}$, se tiene que

$$S(\alpha) = O\left(\frac{N}{(\log N)^{A/2}} + N^{4/5} + \frac{N}{(\log N)^{B/2}}\right) = O\left(\frac{N}{(\log N)^3}\right)$$

■

Teorema 4.16. *Se cumple la estimación*

$$J_2(N) = O\left(\frac{N^2}{(\log N)^4}\right).$$

Demostración. Se sigue de que

$$\begin{aligned} J_2(N) &= \int_{E_2} S^3(\alpha)e^{-2\pi i\alpha N}d\alpha \leqslant \int_{E_2} |S^3(\alpha)|d\alpha \ll \frac{N}{(\log N)^3}\int_0^1 |S(\alpha)^2|d\alpha \\ &= \frac{N}{(\log N)^3}\sum_{\substack{p\leqslant N \\ p \text{ primo}}} 1 \ll \frac{N^2}{(\log N)^4}. \end{aligned}$$

■

Apéndice A

Productos infinitos

Definición A.1. Dada una sucesión de números complejos $\{u_n\}_{n\in\mathbb{N}}$, se define su producto infinito como

$$\prod_{n=1}^{\infty} u_n := \lim_{N\to\infty} \prod_{n=1}^{N} u_n$$

siempre y cuando exista $k \in \mathbb{N}$ tal que el siguiente límite existe y es distinto de 0

$$\lim_{N\to\infty} \prod_{n=k}^{N} u_n.$$

Teorema A.2. *Supóngase que $\{u_n\}_{n\in\mathbb{N}}$ es una sucesión de números complejos que, como serie, converge absolutamente. Entonces, el producto infinito $\prod_{n=1}^{\infty}(1+u_n)$ existe.*

Demostración. Para ver que la norma converge basta con observar que

$$\lim_{N\to\infty} \left| \prod_{n=1}^{N}(1+u_n) \right| \leqslant \lim_{N\to\infty} \prod_{n=1}^{N}(1+|u_n|)$$

$$\leqslant \lim_{N\to\infty} \prod_{n=1}^{N} e^{|u_n|} = \lim_{N\to\infty} \exp\left(\sum_{n=1}^{N}|u_n|\right) = \exp\left(\sum_{n=1}^{\infty}|u_n|\right).$$

Se necesita también que exista $k \in \mathbb{N}$ tal que $\lim_{N\to\infty} \prod_{n=k}^{N}(1+u_n) \neq 0$. Tomando $k \in \mathbb{N}$ tal que $\sum_{n=k}^{\infty}|u_n| < 1$, tenemos que

$$\left| \lim_{N\to\infty} \prod_{n=k}^{N}(1+u_n) \right| \geqslant \lim_{N\to\infty} \prod_{n=k}^{N}(1-|u_n|) \geqslant \lim_{N\to\infty} 1 - \sum_{n=k}^{N}|u_n| > 0,$$

por lo tanto, basta ver que el argumento converge.

Recordemos que $|\arctan(x)| \leqslant |x|$. Por la convergencia absoluta de $\{u_n\}_{n\in\mathbb{N}}$, existe $N \in \mathbb{N}$ tal que $|u_n| \leqslant \frac{1}{4}$ para cualquier $n \geqslant N$; y así se tiene que $\arg(1+u_n) \leqslant \arctan(2|u_n|) \leqslant 2|u_n|$, $\forall n \geqslant$

N. De aquí que

$$\begin{aligned}
\left|\arg\left(\prod_{n=1}^{\infty}(1+u_n)\right)\right| &= \lim_{M\to\infty}\left|\arg\left(\prod_{n=1}^{M}(1+u_n)\right)\right| \\
= \lim_{M\to\infty}\left|\sum_{n=1}^{M}\arg(1+u_n)\right| &= \left|\sum_{n=1}^{N}\arg(1+u_n) + \lim_{M\to\infty}\sum_{n=N+1}^{M}\arg(1+u_n)\right| \\
&\leqslant \left|\sum_{n=1}^{N}\arg(1+u_n)\right| + \lim_{M\to\infty}\sum_{n=N+1}^{M}|\arg(1+u_n)| \\
&\leqslant \left|\sum_{n=1}^{N}\arg(1+u_n)\right| + \lim_{M\to\infty}\sum_{n=N+1}^{M}|2u_n|
\end{aligned}$$

y por hipótesis, este límite existe. Entonces el argumento también converge. ■

Teorema A.3. *Supóngase que* $\{f_n\}_{n\in\mathbb{N}}$ *es una sucesión de funciones complejas acotadas en* $D\subset\mathbb{C}$*, tales que* $\sum_{n=1}^{\infty}|f_n(z)|$ *converge uniformemente en* D*. Entonces*

$$f(z) = \prod_{n=1}^{\infty}(1+f_n(z))$$

converge uniformemente en D*, y* $f(z_0)=0$ *sí y sólo sí* $f_n(z_0)=-1$ *para alguna cantidad finita de naturales* n*.*

Demostración. Como cada f_n es acotada en D y la serie converge uniformemente, se tiene que la suma $\sum_{n=1}^{\infty}|f_n(z)|$ es acotada en D.

Notemos que los productos parciales $F_N(z) = \prod_{n=1}^{N}(1+f_n(z))$ están acotados por e^C para cualesquiera $N\in\mathbb{N}$ y $z\in D$, donde C es la cota de $\sum_{n=1}^{\infty}|f_n(z)|$ (se puede ver claramente que esto sucede en la demostración del Teorema A.2). Entonces para todo $\epsilon>0$, existe $N_\epsilon\in\mathbb{N}$ tal que

$$\sum_{n=N_\epsilon}^{\infty}|f_n(z)| < \epsilon \qquad \forall z\in D$$

De aquí que

$$\begin{aligned}
|f(z)-F_{N_\epsilon}(z)| &= |F_{N_\epsilon}(z)|\left|\prod_{n=N_\epsilon+1}^{\infty}(1+f_n(z))-1\right| \\
&\leqslant |F_{N_\epsilon}(z)|(e^\epsilon-1) \leqslant 2\epsilon|F_{N_\epsilon}(z)| \leqslant 2C\epsilon
\end{aligned}$$

Por lo tanto converge uniformemente.

Notemos que si $f_n(z_0)=-1$ para alguna $z_0\in D$ y alguna $N_0\in\mathbb{N}$, entonces $F_N(z_0)=0$ para cualquier $N\geqslant N_0$, y en consecuencia $f(z_0)=0$.

Para el regreso, notemos que como la convergencia de la serie es uniforme, dada $0 < \epsilon < \frac{1}{2}$ se tiene que $\sum_{n=N_\epsilon}^{\infty} |f_n(z)| < \epsilon$ para cualquier $z \in D$. Supongamos que $f_n(z_0) \neq -1$ para toda $n \in \mathbb{N}$, como $|f(z) - F_{N_\epsilon}(z)| \leqslant 2\epsilon |F_{N_\epsilon}(z)|$ se tiene que $|f(z)| \geqslant (1-2\epsilon)|F_{N_\epsilon}(z)| > 0$. Observemos que se necesita que suceda para sólo una cantidad finita de naturales para que esté bien definido el producto. ■

Apéndice B

Funciones de orden 1

Definición B.1. Sea f una función entera. Se dice que f es de *orden finito* si

$$f(z) = O(e^{|z|^{\alpha}}) \qquad \text{cuando } |z| \to \infty$$

para algún $\alpha \geqslant 0$. En caso de tener orden finito, el *orden* de f se define como

$$\alpha_f = \text{ínf}\{\alpha \in \mathbb{R} : \alpha \text{ testifica que } f \text{ tiene orden finito}\}.$$

No es difícil ver que si f es de orden α entonces existen $A, B \geqslant 0$ tales que $|f(z)| \leqslant Ae^{B|z|^{\alpha}}$ para cualquier $z \in \mathbb{C}$. También se puede deducir, por el Teorema de Liuoville, que si f es de orden finito y no es una función constante, entonces $\alpha_f > 0$.

Proposición B.2. *Sea f holomorfa en Ω y que no se anula en esa región, con Ω simplemente conexo. Entonces, existe g holomorfa en Ω tal que $f(z) = e^{g(z)}$.*

Demostración. Sea $z_0 \in \Omega$ y para cualquier $z \in \Omega$ se define

$$g(z) := \int_{\gamma_z} \frac{f'(w)}{f(w)} dw + C,$$

donde γ_z es una trayectoria de z_0 a z dentro de Ω. Nótese que, por el Teorema de Cauchy, la definición de $g(z)$ no depende de la elección de γ_z. Se tiene entonces que g es holomorfa en Ω y $g'(z) = \frac{f'(z)}{f(z)}$. Como $\frac{d}{dz}(f(z)e^{-g(z)}) = 0$, se deduce que $f(z)e^{-g(z)}$ es constante. Eligiendo $C = \log f(z_0)$, tenemos que $f(z)e^{-g(z)} = f(z_0)e^{-g(z_0)} = 1$ para cualquier $z \in \Omega$. Por lo tanto, $f(z) = e^{g(z)}$. ∎

Teorema B.3. *Sea f una función entera, sin ceros y de orden finito. Entonces, existe polinomio $g(z)$ tal que $f(z) = e^{g(z)}$.*

Demostración. De la Proposición B.2, sabemos que $g(z) = \log f(z)$ para alguna rama del logaritmo. Sea α el orden de f, entonces existe c si $|z| = R$ y R suficientemente grande se tiene que

$$|\Re(g(z))| = \log|f(z)| < cR^{\alpha}.$$

Haciendo el desarrollo en serie de Taylor en el origen de $g(z)$, se tiene

$$g(z) = \sum_{n=0}^{\infty} (a_n + ib_n) z^n$$

por lo que, para $z = Re^{i\theta}$, se tiene la igualdad

$$\Re(g(z)) = \sum_{n=0}^{\infty} \big(a_n R^n \cos(n\theta)) - b_n R^n \operatorname{sen}(n\theta)\big).$$

Podemos suponer, sin pérdida de generalidad, que $g(0) = 0$. Entonces, para $n \geqslant 1$ se tiene que

$$\pi a_n R^n = \int_0^{2\pi} a_n R^n cos^2(n\theta) d\theta = \int_0^{2\pi} cos(n\theta) \Re(g(Re^{i\theta})).$$

Por lo tanto,

$$\pi |a_n| R^n \leqslant \int_0^{2\pi} |\Re(g(Re^{i\theta}))| d\theta \leqslant 2\pi c R^{\alpha}.$$

De lo anterior, se deduce que $|a_n| \leqslant 2cR^{\alpha-n}$ y, como R se puede elegir arbitrariamente grande concluimos que si $\alpha < n$, entonces $a_n = 0$. De manera similar se llega a que $b_n = 0$ cuando $\alpha < n$. Por lo tanto, $g(z)$ es un polinomio. ■

Observación B.4. Si $f(z) = e^{g(z)}$ donde $g(z)$ un polinomio de grado k, entonces $f(z)$ tiene orden k.

Proposición B.5. *Sea f una función de orden α que no se anula en $z = 0$, y sea $\beta > \alpha$. Para R suficientemente grande se tiene que*

$$\Upsilon(R) = O(R^{\beta})$$

donde $\Upsilon(R)$ es el número de ceros de $f(z)$ en $B_R(0)$.

Demostración. Sea $R_0 > 0$ tal que, si $|z| > R_0$, entonces $|f(z)| < e^{|z|^{\beta}}$. Sea $R \geqslant R_0$ y $z_1, z_2, \ldots, z_{\Upsilon(R)}$ los ceros de f en B_R. Sea

$$F(z) = f(z) \prod_{n=1}^{\Upsilon(R)} \frac{1}{z - z_n}.$$

Por el principio del máximo se tiene que $|F(0)| \leqslant \max\limits_{|z|=3R} |F(z)|$, por lo que

$$\frac{|f(0)|}{R^{\Upsilon(R)}} \leqslant \max_{|z|=3R} |f(z)| \prod_{n=1}^{\Upsilon(R)} \frac{1}{|z - z_n|} \leqslant e^{(3R)^{\beta}} \frac{1}{(2R)^{\Upsilon(R)}}$$

de donde se concluye que $\Upsilon(R) = O(R^{\beta})$. ■

Corolario B.6. *Sea f de orden α, con $f(0) \neq 0$ y con una cantidad infinita de ceros en $z_1, z_2, \ldots$ contados con multiplicidad. Entonces, para cualquier $\beta > \alpha$, la suma $\displaystyle\sum_{n=1}^{\infty} \frac{1}{|z_n|^\beta}$ converge.*

Demostración. Sea $\alpha < \delta < \beta$ y R_0 suficientemente grande. Para cualquier $R \geqslant R_0 \geqslant 1$ se tiene que $\Upsilon(R) = O(R^\delta)$. Entonces

$$\sum_{n=1}^{\infty} \frac{1}{|z_n|^\beta} = \sum_{|z_n|<R} \frac{1}{|z_n|^\beta} + \sum_{k=1}^{\infty} \sum_{R^k \leqslant |z_n| < R^{k+1}} \frac{1}{|z_n|^\beta} \leqslant C + \sum_{k=1}^{\infty} \frac{O((R^{k+1})^\delta)}{(R^k)^\beta}$$

$$\leqslant C + R^\delta O\left(\sum_{k=1}^{\infty} \frac{1}{(R^{\beta-\delta})^k}\right) < \infty.$$

∎

Teorema B.7. *Sea f una función de orden 1, con $f(0) \neq 0$ y con ceros en $z_1, z_2, \ldots$ contados con multiplicidad (podría ser una cantidad finita de ceros). Entonces, existen $A, B \in \mathbb{C}$ tales que*

$$f(z) = e^{A+Bz} \prod_{n=1}^{\infty} \left(1 - \frac{z}{z_n}\right) e^{\frac{z}{z_n}}.$$

Demostración. Para cada $z \in \mathbb{C}$ fijo, se tiene que

$$\left(1 - \frac{z}{z_n}\right) e^{\frac{z}{z_n}} = 1 + O\left(\frac{z^2}{z_n^2}\right)$$

donde la constante implícita no depende de n. Por el Corolario B.6 y el Teorema A.2, el producto

$$P(z) := \prod_{n=1}^{\infty} \left(1 - \frac{z}{z_n}\right) e^{\frac{z}{z_n}}$$

converge. Como la constante implícita está acotada en cada compacto de $\mathbb{C}$, $P(z)$ converge uniformemente en cada compacto de $\mathbb{C}$ y por el Teorema A.3, $P(z)$ es una función holomorfa.

Nótese que $F(z) = \frac{f(z)}{P(z)}$ es entera y no tiene ceros, pues $f(z)$ y $P(z)$ son enteras y tienen los mismos ceros con la misma multiplicidad. Por el Teorema B.3 sería suficiente demostrar que $F(z)$ es de orden 1.

Sea $r_n = |z_n|$. Por el Corolario B.6 se tiene que $\displaystyle\sum_{n=1}^{\infty} \frac{1}{r_n^2} < \infty$, lo que implica que existen $R \in \mathbb{R}^+$ tan grandes como se quieran tales que

$$R \notin U := \bigcup_{n=1}^{\infty} [r_n - r_n^2, r_n + r_n^2]$$

Por el Principio del Máximo, es suficiente demostrar que, para todo $R \in \mathbb{R}^+ \backslash U$, se cumple que $F(z) = O(e^{|z|^{1+\epsilon}})$ para cualquier $\epsilon > 0$.

Sean

$$P_1(z) = \prod_{|z_n|<\frac{R}{2}} \left(1 - \frac{z}{z_n}\right) e^{\frac{z}{z_n}}, \qquad P_2(z) = \prod_{\frac{R}{2}\leqslant|z_n|\leqslant 2R} \left(1 - \frac{z}{z_n}\right) e^{\frac{z}{z_n}},$$

$$P_3(z) = \prod_{2R<|z_n|} \left(1 - \frac{z}{z_n}\right) e^{\frac{z}{z_n}}.$$

De la misma forma que se demostró que $P(z)$ era una función holomorfa, se ve que cada $P_i(z)$ es entera. Sea $R \in \mathbb{R}^+ \setminus U$, entonces, para $|z| = R$ se tiene que

$$|P_1(z)| \geqslant \prod_{|z_n|<\frac{R}{2}} \left(\frac{|z|}{|z_n|} - 1\right) e^{-\frac{|z|}{|z_n|}} > \prod_{|z_n|<\frac{R}{2}} e^{-\frac{R}{|z_n|}} > \prod_{|z_n|<\frac{R}{2}} e^{-\left(\frac{R}{|z_n|}\right)^{1+\frac{\epsilon}{2}}} = e^{-c_1 R^{1+\frac{\epsilon}{2}}}$$

$$|P_2(z)| \geqslant \prod_{\frac{R}{2}\leqslant|z_n|\leqslant 2R} \frac{|z-z_n|}{|z_n|} e^{-\frac{|z|}{|z_n|}} \geqslant \prod_{\frac{R}{2}\leqslant|z_n|\leqslant 2R} e^{-2} \frac{1}{|z_n|^2 2R} \geqslant \prod_{\frac{R}{2}\leqslant|z_n|\leqslant 2R} e^{-2} \frac{1}{8R^3}$$

$$= \left(\frac{1}{8R^3e^2}\right)^{\Upsilon(2R)-\Upsilon(\frac{R}{2})} \geqslant \left(\frac{1}{8R^3e^2}\right)^{\Upsilon(2R)} \geqslant \left(\frac{1}{8R^3e^2}\right)^{c(2R)^{1+\frac{\epsilon}{4}}} \geqslant e^{-c_2 R^{1+\frac{\epsilon}{2}}}$$

$$|P_3(z)| \geqslant \prod_{2R<|z_n|} \left(1 - \frac{|z|}{|z_n|}\right) e^{-\frac{|z|}{|z_n|}} \geqslant \prod_{2R<|z_n|} e^{-c\left(\frac{R}{|z_n|}\right)^2} \geqslant e^{-cR^2(2R)^{-1+\frac{\epsilon}{2}}} \geqslant e^{c_3 R^{1+\frac{\epsilon}{2}}}.$$

Entonces $|P(z)| = |P_1(z)||P_2(z)||P_3(z)| > e^{-R^{1+\frac{3\epsilon}{4}}}$ para cualquier $|z| = R$ y $\epsilon > 0$, y como $f(z) = O\left(e^{|z|^{1+\frac{\epsilon}{2}}}\right)$, entonces

$$F(z) = \frac{f(z)}{P(z)} = O\left(e^{|z|^{1+\frac{\epsilon}{2}}} e^{|z|^{1+\frac{3\epsilon}{4}}}\right) = O\left(e^{|z|^{1+\epsilon}}\right)$$

con lo que queda demostrado. ■

Proposición B.8. *Sea f una función de orden 1 con $f(0) \neq 0$. Si $f(z) \neq O(e^{c|z|})$ cuando $|z| \to \infty$, entonces f tiene una infinidad de ceros.*

Demostración. Si f tuviera una cantidad finita de ceros en $z_1, z_2, \ldots, z_k$ contados con multiplicidad, se tendría que

$$|f(z)| = \left|e^{A+Bz} \prod_{n=1}^{k} \left(1 - \frac{z}{z_n}\right) e^{\frac{z}{z_n}}\right| \leqslant |e^{A+Bz}| \prod_{n=1}^{k} e^{2\frac{|z|}{|z_n|}} = O\left(e^{c|z|}\right)$$

para z suficientemente grande, llegando a una contradicción. ■

Proposición B.9. *Sea f una función de orden 1, y sean $z_1, z_2, \ldots$ sus ceros contados con multiplicidad. Si $\sum_{n=1}^{\infty} \frac{1}{|z_n|}$ converge, entonces $|f(z)| < e^{a+b|z|}$ para algunos a y b reales positivos.*

Demostración. Si la serie convergiera, se tendría que

$$|f(z)| = \left| e^{A+Bz} \prod_{n=1}^{\infty} \left(1 - \frac{z}{z_n}\right) e^{\frac{z}{z_n}} \right| \leqslant |e^{A+Bz}| \prod_{n=1}^{\infty} e^{2|z| \frac{1}{|z_n|}} \leqslant |e^{A+Bz}| e^{M|z|} \leqslant e^{A+(B+M)|z|}.$$

∎

Apéndice C

La función Γ

La función $\Gamma(s)$ se define, para $\Re(s) > 0$ como

$$\Gamma(s) := \int_0^\infty e^{-t} t^{s-1} dt.$$

Dicha función está bien definida, pues $e^{-t}t^{s-1}$ es continua en $[0, \infty)$ y $e^{-t}t^{s-1} = O\left(\frac{1}{t^2}\right)$. La función $e^{-t}t^{s-1}$ es holomorfa en $\Re(s) > 0$ para cada $t \in \mathbb{R}^+$ fija, y es continua sobre s y t, por lo tanto,

$$\Gamma_n(s) := \int_{\frac{1}{n}}^n e^{-t} t^{s-1} dt$$

es holomorfa en $0 < a < \Re(s) < b < \infty$. En la misma región se tiene que $\Gamma_n(s) \to \Gamma(s)$ uniformemente, ya que, tomando $s = \sigma + i\gamma$ con $a < \sigma < b$ se tiene que

$$|\Gamma(s) - \Gamma_n(s)| \leqslant \int_0^{\frac{1}{n}} e^{-t} t^{\sigma-1} dt + \int_n^\infty e^{-t} t^{\sigma-1} dt \leqslant \int_0^{\frac{1}{n}} e^{-t} t^{a-1} dt + \int_n^\infty e^{-t} t^{b-1} dt$$

$$\leqslant \frac{1}{n^a} + c \int_n^\infty e^{-\frac{t}{2}} dt \to 0$$

cuando $n \to \infty$. Por lo tanto, Γ es holomorfa en $\Re(s) > 0$.

Lema C.1. *Si $Re(s) > 0$, entonces $\Gamma(s+1) = s\Gamma(s)$.*

Demostración. Integrando por partes se tiene que si $\Re(s) > 0$, entonces

$$e^{-t} t^s \Big|_{t=\frac{1}{n}}^n = -\int_{\frac{1}{n}}^n e^{-t} t^s dt + s \int_{\frac{1}{n}}^n e^{-t} t^{s-1} dt$$

y haciendo $n \to \infty$ queda demostrado el Lema. ■

Nótese que $\Gamma(1) = \displaystyle\int_0^\infty e^{-t} dt = 1$. Usando el lema anterior se tiene el siguiente corolario.

Corolario C.2. *Para cualquier $n \in \mathbb{N}$ se tiene que $\Gamma(n+1) = n!$.*

Teorema C.3. *La función Γ se puede extender de manera meromorfa a todo el plano. Sus polos se localizan en $s \in \{0, -1, -2, \dots\}$ y el residuo de Γ en $s = -n$ es $\frac{(-1)^n}{n!}$.*

Demostración. Por el Lema C.1 se tiene que la función $\hat{\Gamma}_n(s) = \frac{\Gamma(s+m)}{s(s+1)\cdots(s+m-1)}$ coincide con $\Gamma(s)$ en $\Re(s) > 0$. Entonces $\hat{\Gamma}_n$ es extensión meromorfa de Γ en $\Re(s) > -n$. Por la unicidad de la extensión meromirfa se deduce que se puede extender a todo el plano complejo meromorfamente. Si $s = -k$ con $k \in \{0, 1, 2, \dots\}$ y $k < n$, entonces

$$\begin{aligned}
\mathrm{Res}_{s=-k}\hat{\Gamma}_m(s) &= \lim_{s\to -k} \frac{(s-k)\Gamma(s+n)}{s(s+1)\cdots(s+n-1)} = \frac{\Gamma(n-k)}{(n-1-k)!(-1)(-2)\cdots(-k)} \\
&= \frac{(n-k-1)!(-1)^k}{(n-k-1)!n!} = \frac{(-1)^n}{n!}.
\end{aligned}$$

■

Teorema C.4. *La relación* $s\Gamma(s) = \Gamma(s+1)$ *se extiende a* $\mathbb{C}\backslash\{0, -1, -2, \dots\}$.

Proposición C.5. *La función* Γ *se puede representar en todo el plano como*

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

Demostración. Usando la serie de Taylor de e^{-t} y el Teorema de la Convergencia Dominada de Lebesgue se tiene que, si $\Re(s) > 0$, se cumple la igualdad

$$\int_0^1 e^{-t}t^{s-1}dt = \int_0^1 \sum_{n=0}^{\infty} \frac{(-t)^n}{n!}t^{s-1}dt = \sum_{n=0}^{\infty} \int_0^1 \frac{(-1)^n t^{n+s-1}}{n!}dt = \sum_{n=0}^{\infty} \frac{(-1)^n}{n!(n+s)}.$$

Por lo tanto la proposición es cierta para $\Re(s) > 1$.

La función $\displaystyle\int_1^{\infty} e^{-t}t^{s-1}dt$ es entera, ya que $e^{-t}t^{s-1}$ es continua en $(s,t) \in \mathbb{C} \times (1, \infty)$ y; para cada $t \in (1, \infty)$ fijo, $e^{-t}t^{s-1}$ es holomorfa en s.

Sea $R > 0$. Veamos que $\displaystyle\sum_{n=0}^{\infty} \frac{(-1)^n}{n!(n+s)}$ es meromorfa en $B_R(0)$ pues, si $N > 2R$ se tiene que

$$\sum_{n=0}^{N} \frac{(-1)^N}{n!(n+s)}$$

es meromorfa en $B_R(0)$, y si $M \geqslant N$ se tiene que

$$\left| \sum_{n=M}^{\infty} \frac{(-1)^n}{n!(n+s)} \right| \leqslant \frac{1}{R} \sum_{n=M}^{\infty} \frac{1}{n!} \to 0$$

cuando $M \to \infty$, por lo que converge uniformemente en $B_R(0)$, por lo tanto $\displaystyle\sum_{n=N}^{\infty} \frac{(-1)^n}{n!(n+s)}$ es holomorfa. Entonces $\displaystyle\sum_{n=0}^{\infty} \frac{(-1)^n}{n!(n+s)}$ es meromorfa y la igualdad se da en todo el plano. ■

Lema C.6. *Si* $0 < a < 1$ *se tiene que*

$$\int_0^\infty \frac{\nu^{a-1}}{1+v} dv = \frac{\pi}{\operatorname{sen} \pi a}.$$

Demostración. Haciendo el cambio de variable $\nu \to e^x$ se tiene que

$$\int_0^\infty \frac{\nu^{a-1}}{1+\nu} d\nu = \int_{-\infty}^\infty \frac{e^{ax}}{1+e^x} dx.$$

Los polos del integrando son simples y se localizan en $z = (2k+1)\pi i$ para cualquier $k \in \mathbb{Z}$ y tienen residuo $\lim\limits_{s \to (2k+1)\pi i} \dfrac{(s-(2k+1)\pi i)e^{as}}{1+e^s} = -e^{a(2k+1)\pi i}$. Tomando ∂_R como la trayectoria conformada por la frontera del rectángulo con vértices en $-R, R, R+2\pi i - R + 2\pi i$ y aplicando el Teorema del Residuo se tiene que $\int_{\partial_R} \frac{e^{ax}}{1+e^x} dx = -2\pi i e^{a\pi i}$. Notemos que

$$\left| \int_R^{R+2\pi i} \frac{e^{az}}{1+e^z} dz \right| \leqslant 2\pi \frac{e^{aR}}{e^R - 1} \quad \text{y} \quad \left| \int_{-R+2\pi i}^{-R} \frac{e^{az}}{1+e^z} dz \right| \leqslant 2\pi \frac{e^{-aR}}{1-e^{-R}},$$

y cuando $R \to \infty$, ambas integrales se hacen 0. Por otro lado

$$\int_{R+2\pi i}^{-R+2\pi i} \frac{e^{az}}{1+e^z} dz = e^{2\pi i a} \int_R^{-R} \frac{e^{ax}}{1+e^x} dx$$

se deduce que

$$-2\pi i e^{a\pi i} = (1 - e^{2\pi i a}) \int_{-\infty}^\infty \frac{e^{ax}}{1+e^x} dx,$$

de donde se concluye

$$\int_{-\infty}^\infty \frac{e^{ax}}{1+e^x} dx = \frac{-2\pi i e^{a\pi i}}{1-e^{2\pi i a}} = \frac{\pi}{\operatorname{sen} \pi a}.$$

∎

Teorema C.7. *Para cualquier* $s \in \mathbb{C}$ *se tiene que* $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\operatorname{sen} \pi s}$.

Demostración. Se sigue del Teorema C.3 y el Corolario C.2 que los números enteros son todos los polos de $\Gamma(s)\Gamma(1-s)$, y son polos simples; al igual que la función $\frac{\pi}{\operatorname{sen} \pi s}$. Notemos que, si $0 < s < 1$ se cumple la igualdad

$$\Gamma(1-s) = \int_0^\infty e^{-u} u^{-s} du = t \int_0^\infty e^{-\nu t} (\nu t)^{-s} dv,$$

para cualquier $t > 0$. Entonces

$$\begin{aligned} \Gamma(1-s)\Gamma(s) &= \int_0^\infty e^{-t} t^{s-1} \Gamma(1-s) dt = \int_0^\infty e^{-t} t^{s-1} \left(t \int_0^\infty e^{-\nu t} (\nu t)^{-s} d\nu \right) dt \\ &= \int_0^\infty \int_0^\infty e^{-t(1+\nu)} \nu^{-s} dt d\nu = \int_0^\infty \frac{\nu^{-s}}{1+\nu} d\nu = \frac{\pi}{\operatorname{sen} \pi(1-s)} = \frac{\pi}{\operatorname{sen} \pi s}. \end{aligned}$$

Como la igualdad se da en un conjunto con puntos de acumulación, dicha igualdad es cierta en todo el plano. ∎

Corolario C.8. $\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$.

Teorema C.9 (Representación de Gauss para la función Γ)**.** *Para* $\Re(s) > 0$ *se da la igualdad*

$$\Gamma(s) = \lim_{n\to\infty}\left(\frac{n^s}{s}\prod_{k=1}^{n}\left(1+\frac{s}{k}\right)^{-1}\right).$$

Demostración. Se tiene que

$$\Gamma(s) = \int_0^\infty t^{s-1}\lim_{n\to\infty}\left(1-\frac{t}{n}\right)^n dt = \lim_{n\to\infty}\int_0^n t^{s-1}\left(1-\frac{t}{n}\right)^n dt.$$

Usando ahora integración por partes tenemos que

$$\int_0^n t^{s-1}\left(1-\frac{t}{n}\right)^n dt = \frac{1}{s}t^s\left(1-\frac{t}{n}\right)\Bigg|_{t=0}^{n} - \int_0^n \frac{1}{s}t^s n\left(1-\frac{t}{n}\right)^{n-1}\left(-\frac{1}{n}\right)dt$$

$$= \frac{n}{ns}\int_0^n t^s\left(1-\frac{t}{n}\right)^{n-1} dt.$$

Si se repite el proceso de integración por partes se llega a que

$$\int_0^n t^{s-1}\left(1-\frac{t}{n}\right)^n dt = \frac{n!}{n^n s(s+1)\cdots(s+n-1)}\int_0^n t^{s+n-1}dt = \frac{n!\cdot n^{s+n}}{n^n s(s+1)\cdots(s+n)}$$

Entonces

$$\Gamma(s) = \lim_{n\to\infty}\frac{n!\cdot n^s}{s(s+1)\cdots(s+n)} = \lim_{n\to\infty}\frac{n^s}{s}\prod_{k=1}^{n}\left(1-\frac{s}{k}\right)^{-1}.$$

∎

Definición C.10. Se define la constante γ de Euler como

$$\gamma = \lim_{n\to\infty}\left(\sum_{j=1}^{n}\frac{1}{j} - \log n\right).$$

Teorema C.11 (Producto de Weierstrass)**.** *Para cada* $s \in \mathbb{C}$ *se tiene la igualdad*

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

Demostración. Si $\Re(s) > 0$ se tiene que

$$\Gamma(s) = \lim_{n\to\infty}\frac{n^s}{s}\prod_{j=1}^{n}\left(1+\frac{s}{j}\right)^{-1} = \lim_{n\to\infty}\frac{e^{s\log n-\frac{s}{1}-\frac{s}{2}-\cdots-\frac{s}{n}}}{s}\prod_{j=1}^{n}\left(1+\frac{s}{i}\right)^{-1}e^{\frac{s}{j}}$$

$$= \frac{e^{-s\gamma}}{s} \lim_{n\to\infty} \prod_{j=1}^{n} \left(1+\frac{s}{j}\right)^{-1} e^{\frac{s}{j}}.$$

Por el Teorema A.3 el límite existe y es una función entera, pues $\left(1+\frac{s}{j}\right)^{-1} e^{\frac{s}{j}} = 1 + O\left(\frac{s^2}{j^2}\right)$ y $\sum_{j=1}^{\infty} \frac{s^2}{j^2}$ converge uniformemente en cualquier compacto de $\mathbb{C}$. Entonces se da la igualdad en $\Re(s) > 0$ y, por la unicidad de una extensión analítica, se concluye la demostración. ■

Corolario C.12. *La función* Γ *no tiene ceros en* $\mathbb{C}$.

Teorema C.13 (Fórmula de duplicación de Legendre)**.** *Para cualquier* $s \in \mathbb{C}$ *se tiene la igualdad*

$$\Gamma(s)\Gamma\left(s+\frac{1}{2}\right) = 2^{1-2s}\pi^{\frac{1}{2}}\Gamma(2s).$$

Demostración. No es difícil ver, ayudados del producto de Weierstrass, que

$$\frac{\partial}{\partial s}\frac{\Gamma'(s)}{\Gamma(s)} = \sum_{n=0}^{\infty} \frac{1}{(s+n)^2}.$$

Nótese que $\Gamma(s)\Gamma(s+\frac{1}{2})$ y $\Gamma(2s)$ tienen los mismos polos. Para cualquier $s \notin \{0, -\frac{1}{2}, -1, -\frac{3}{2}, \dots\}$ se tiene que

$$\frac{\partial}{\partial s}\frac{\Gamma'(s)}{\Gamma(s)} + \frac{\partial}{\partial s}\frac{\Gamma'(s+\frac{1}{2})}{\Gamma(s+\frac{1}{2})} = \sum_{n=0}^{\infty}\frac{1}{(s+n)^2} + \sum_{n=0}^{\infty}\frac{1}{(s+n+\frac{1}{2})^2} = 4\sum_{n=0}^{\infty}\frac{1}{(2s+n)^2} = 2\frac{\partial}{\partial s}\frac{\Gamma'(2s)}{\Gamma(2s)}.$$

Integrando lo anterior se tiene que, para algunas constantes a, b se cumple la igualdad

$$\Gamma(s)\Gamma(s+\frac{1}{2}) = e^{as+b}\Gamma(2s).$$

Evaluando en $s = 1$ y $s = \frac{1}{2}$, con ayuda del Teorema C.7 y el Corolario C.8 se puede concluir que $e^{as+b} = 2^{1-2s}\pi^{\frac{1}{2}}$. ■

La demostración de los siguientes famosos teoremas se encuentran en [1, pp 204].

Teorema C.14 (Fórmula de Stirling)**.** *Sea* $\delta > 0$. *Cuando* $|s| \to \infty$ *la función* Γ *cumple la aproximación*

$$\log\Gamma(s) = \left(s-\frac{1}{2}\right)\log s - s + \frac{1}{2}\log 2\pi + O(|s|^{-1})$$

en la región $-\pi + \delta < \arg s < \pi - \delta$.

Teorema C.15. *Sea* $\delta > 0$. *Cuando* $|s| \to \infty$ *la función* Γ *cumple la aproximación*

$$\frac{\Gamma'(s)}{\Gamma(s)} = \log s + O(|s|^{-1})$$

en la región $-\pi + \delta < \arg s < \pi - \delta$.

Apéndice D

Fórmula de sumación de Poisson

Se denotará por $\mathcal{F}_a$ al conjunto de funciones f tales que

- f es holomorfa en $S_a = \{z \in \mathbb{C} : |\Im(z)| < a\}$,
- existe $A > 0$ tal que $f(x+iy) \leqslant \frac{A}{1+x^2}$ siempre que $x \in \mathbb{R}$, $|y| < a$,

y se denotará por $\mathcal{F} = \bigcup\limits_{a \in \mathbb{R}^+} \mathcal{F}_a$.

Definición D.1. Para cada $f \in \mathcal{F}$ se define su *transformada de Fourier* como

$$\hat{f}(s) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i s x} dx.$$

Teorema D.2. *Si $f \in \mathcal{F}_a$ para alguna $a > 0$, entonces $|\hat{f}(s)| \leqslant Be^{-2\pi b|s|}$, para todo $0 \leqslant b < a$.*

Demostración. El caso $b = 0$ se sigue de que $\hat{f}$ es acotada, pues

$$|\hat{f}(s)| \leqslant \int_{-\infty}^{\infty} \left| \frac{f(x)}{e^{2\pi i x s}} \right| dx \leqslant A \int_{-\infty}^{\infty} \frac{1}{1+x^2} dx = A\pi.$$

En caso de que $s = 0$ se sigue de que

$$|\hat{f}(0)| \leqslant \int_{-\infty}^{\infty} |f(x)| dx \leqslant A \int_{-\infty}^{\infty} \frac{1}{1+x^2} = A\pi.$$

En caso de que $0 < b < a$ y $0 < s$ y usando el Teorema de Cauchy se tiene que

$$\hat{f}(s) = \lim_{R \to \infty} \int_{-R}^{R} f(x) e^{2\pi i x s} dx$$

$$= \lim_{R \to \infty} \left(\int_{-R}^{-R-ib} f(x) e^{2\pi i x s} dx + \int_{-R-ib}^{R-ib} f(x) e^{2\pi i x s} dx + \int_{R-ib}^{R} f(x) e^{2\pi i x s} dx \right).$$

Notemos que

$$\left| \int_{-R}^{-R-ib} f(x) e^{-2\pi i x s} dx \right| \leqslant \int_0^b |f(-R-it) e^{-2\pi i(-R-it)s}| dt \leqslant \int_0^b \frac{Ae^{-2\pi t s}}{1+R^2} dt \leqslant \int_0^b \frac{A}{R^2} dt = \frac{bA}{R^2}.$$

La misma cota se tiene para la integral de $R - ib$ a R. Finalmente

$$\left|\int_{-R-ib}^{R-ib} f(x)e^{-2\pi ixs}dx\right| \leqslant \int_{-\infty}^{\infty} |f(x-ib)e^{-2\pi i(x-ib)s}|dx \leqslant \int_{-\infty}^{\infty} \frac{Ae^{-2\pi bs}}{1+x^2}dx \leqslant A\pi e^{-2\pi bs}.$$

Haciendo tender R a infinito se concluye este caso.
Para el caso $0 < b < a$ y $s < 0$ se hace del mismo modo que el anterior, salvo que se considera la integral sobre el rectángulo con vértices en $-R, -R+ib, R+ib, R$. ■

Del Teorema anterior se deduce fácilmente que si $f \in \mathcal{F}$, entonces $\hat{f} \in \mathcal{F}$.

Teorema D.3 (Fórmula de Inversión de Fourier)**.** *Si $f \in \mathcal{F}$ entonces para cualquier $x \in \mathbb{R}$ se tiene que*

$$f(x) = \int_{-\infty}^{\infty} \hat{f}(s)e^{2\pi isx}ds.$$

Demostración. Usando el Teorema de Fubini-Tonelli se tiene que

$$\begin{aligned}\int_0^{\infty} \hat{f}(s)e^{2\pi ixs}ds &= \int_0^{\infty}\int_{-\infty}^{\infty} f(u-ib)e^{-2\pi i(u-ib)s}e^{2\pi ixs}duds \\ &= \int_{-\infty}^{\infty} f(u-ib)\int_0^{\infty} e^{-2\pi i(u-ib-x)s}dsdu \\ &= \int_{-\infty}^{\infty} f(u-ib)\frac{1}{2\pi b+2\pi i(u-x)}du = \frac{1}{2\pi i}\int_{-\infty}^{\infty}\frac{f(u-ib)}{u-ib-x}du.\end{aligned}$$

De manera similar se tiene que

$$\int_{-\infty}^{0} \hat{f}(s)e^{2\pi ixs}ds = -\frac{1}{2\pi i}\int_{-\infty}^{\infty}\frac{f(u+ib)}{u+ib-x}du.$$

Sea $R > |x|$. Por el Teorema de Cauchy, se tiene que

$$f(x) = \frac{1}{2\pi i}\int_{\partial C_R}\frac{f(z)}{z-x}dz,$$

donde C_R es el rectángulo que tiene por vértices a los puntos $R-ib, R+ib, -R+ib, -R-ib$. Como

$$\left|\int_{\pm R-ib}^{\pm R+ib}\frac{f(z)}{z-x}dz\right| \leqslant \int_{\pm R-ib}^{\pm R+ib}\frac{|f(z)|}{|z-x|}dz \leqslant \frac{A}{1+R^2}\int_{\pm R-ib}^{\pm R+ib}\frac{1}{|z-x|}dz$$

y esto último tiende a 0 cuando R tiende a ∞, concluyendo que

$$f(x) = \frac{1}{2\pi i}\left(\int_{-\infty}^{\infty}\frac{f(u-ib)}{u-ib-x}du + \int_{\infty}^{-\infty}\frac{f(u+ib)}{u+ib-x}du\right) = \int_{-\infty}^{\infty}\hat{f}(s)e^{2\pi isx}ds.$$

■

Teorema D.4 (Fórmula de sumación de Poisson)**.** *Si $f \in \mathcal{F}$, entonces* $\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}}\hat{f}(n)$.

Demostración. Notemos primero que la función $\frac{1}{e^{2\pi iz}-1}$ tiene polos simples para cada $z \in \mathbb{Z}$ con residuo $\frac{1}{2\pi i}$. Como f es holomorfa se tiene que $\frac{f(z)}{e^{2\pi iz}-1}$ tiene polos simples con residuo $\frac{f(z)}{2\pi i}$ para cada $z \in \mathbb{Z}$, a menos que f tenga un cero ahí. Sea $a > 0$ tal que $f \in \mathcal{F}_a$ y $0 < b < a$, y sea C_N el rectángulo con vértices en $N + \frac{1}{2} - ib, N + \frac{1}{2} + ib, -N - \frac{1}{2} + ib, -N - \frac{1}{2} - ib$. Por el Teorema de Cauchy se deduce que

$$\sum_{-N \leqslant n \leqslant N} f(n) = \int_{\partial C_N} \frac{f(z)}{e^{2\pi iz} - 1} dz.$$

Notemos también que

$$\lim_{N\to\infty} \left| \int_{\pm(N+\frac{1}{2})-ib}^{\pm(N+\frac{1}{2})+ib} \frac{f(z)}{e^{2\pi iz} - 1} dz \right| \leqslant \lim_{N\to\infty} \frac{A}{1 + (N + \frac{1}{2})^2} \int_{-b}^{b} \frac{1}{1 + e^{-2\pi x}} dx = 0.$$

Entonces concluimos que

$$\sum_{n\in\mathbb{Z}} f(n) = \lim_{N\to\infty} \left(\int_{-N-\frac{1}{2}-ib}^{N+\frac{1}{2}-ib} \frac{f(z)}{e^{2\pi iz} - 1} dz - \int_{-N-\frac{1}{2}+ib}^{N+\frac{1}{2}+ib} \frac{f(z)}{e^{2\pi iz} - 1} dz \right)$$

$$= \lim_{N\to\infty} \left(\int_{-N-\frac{1}{2}-ib}^{N+\frac{1}{2}-ib} f(z) e^{-2\pi iz} \sum_{n=0}^{\infty} e^{-2\pi inz} dz - \int_{-N-\frac{1}{2}+ib}^{N+\frac{1}{2}+ib} f(z) \sum_{n=0}^{\infty} e^{2\pi inz} dz \right)$$

$$= \sum_{n=0}^{\infty} \lim_{N\to\infty} \int_{-N-\frac{1}{2}-ib}^{N+\frac{1}{2}-ib} f(z) e^{-2\pi i(n+1)z} dz + \sum_{n=0}^{\infty} \lim_{N\to\infty} \int_{-N-\frac{1}{2}+ib}^{N+\frac{1}{2}+ib} f(z) e^{2\pi inz} dz$$

$$= \sum_{n=0}^{\infty} \int_{-\infty}^{\infty} f(z) e^{-2\pi i(n+1)z} dz + \sum_{n=0}^{\infty} \int_{-\infty}^{\infty} f(z) e^{2\pi inz} dz = \sum_{n\in\mathbb{Z}} \hat{f}(n).$$

■

Bibliografía

[1] Ahlfors, L.V., *Complex Analysis*, Segunda edición, McGrawHill, Estados Unidos de América, 1966.

[2] Stein, Elias M.; Shakarchi, R., *Complex Analysis*, Princeton, Estados Unidos de América, 2003.

[3] Hardy, G.H.; Wright, E.M., *An Introduction to the Theory of Numbers*, Quinta edición, Oxford University Press, Estados Unidos de América, 1979.

[4] Nathanson, M.B., *Elementary Methods in Number Theory*, Springer-Verlag, Estados Unidos de América, 2000.

[5] Apostol, Tom M., *Introducción a la Teoría Analítica de Números*, Reverté, España, 2002.

[6] Niven, I.; H.S. Zuckerman; H.L. Montgomery, *An Introduction to the Theory of Numbers*, Quinta edición, John Wiley & Sons, Estados Unidos de América, 1991.

[7] Davenport, H., *Multiplicative Number Theory*, Segunda edición, Springer-Verlag, Estados Unidos de América, 1980.

[8] G. H. Hardy y J. E. Littlewood, *Some problems of "Partitio Numerorum": III, On the expression of a number as a sum of primes*, Acta. Math. 44 (1923), 1-70.

[9] L. G. Schnirelmann, *On additive properties of numbers*, Ann. Inst. polytechn. Novočerkassk (1930), 14:3–28. JFM 56.0892.02.

[10] Tao, Terence, *Every odd number greater than 1 is the sum of at most five primes*, Math. Comp. 83 (2014), no. 286, 997–1038.

[11] I. M. Vinogradov, *Representation of an odd number as a sum of three primes*, Dokl. Akad. Nauk. SSR 15 (1937), 291–294.

[12] Walfisz, Arnold (1936). "Zur additiven Zahlentheorie. II"[On additive number theory. II]. Mathematische Zeitschrift (in German). 40 (1): 592–607.

[13] K. G. Borozdin, *On I. M. Vinogradov's constant*, Proc. 3rd All-Union Math. Conf., vol. 1 Izdat. Akad. Nauk SSSR, Moscow, 1956. (Russian) MR 20:6973a

[14] Liu, Ming-Chit; Wang, Tianze On the Vinogradov bound in the three primes Goldbach conjecture. Acta Arith. 105 (2002), no. 2, 133–175.

[15] Deshouillers, J.-M.; Effinger, G.; te Riele, H.; Zinoviev, D. *A complete Vinogradov 3-primes theorem under the Riemann hypothesis.* Electron. Res. Announc. Amer. Math. Soc. 3 (1997), 99–104.

[16] Helfgott, H. A., *Minor arcs for Goldbach's problem*, (2013) arXiv:1205.5252

[17] Helfgott, H. A., *Major arcs for Goldbach's problem*, (2013) arXiv:1305.2897

[18] Helfgott, H. A., *The ternary Goldbach conjecture is true*, (2013) arXiv:1312.7748

[19] Helfgott, H. A.; Platt, David J. *Numerical verification of the ternary Goldbach conjecture up to* $8.875 \cdot 10^{30}$. Exp. Math. 22 (2013), no. 4, 406–409. (Reviewer: Ping Ding)