"El saber de mis hijos hará mi grandeza"

UNIVERSIDAD DE SONORA

División de Ciencias Exactas y Naturales

Programa de Posgrado en Matemáticas

Enteros representables por formas binarias ciclotómicas

T E S I S

Que para obtener el título de:

Maestro en Ciencias (Matemáticas)

Presenta:

Omar Eduardo Hernández Andrade

Director de tesis: Dr. Genaro Hernández Mada

Hermosillo, Sonora, México, Septiembre 2019.

SINODALES

Dr. Genaro Hernández Mada
Universidad de Sonora, Hermosillo, México

Dr. Rafael Roberto Ramos Figueroa
Universidad de Sonora, Hermosillo, México

Dr. Jesús Francisco Espinoza Fierro
Universidad de Sonora, Hermosillo, México

REVISORA EXTERNA

Dra. Miriam Bocardo Gaspar
Universidad de Guadalajara, Guadalajara, México.

Agradecimientos

Le agradezco principalmente a mi director de tesis Dr. Genaro Hernández Mada porque durante la realización de este trabajo nos encontramos con muchas dificultades que nos costaron demasiado tiempo y esfuerzo.

Le agradezco a mis padres y a mi novia por el apoyo que siempre me han dado y por su compañia durante estos dos años.

Gracias a los doctores Rafael Roberto Ramos Figueroa y Jesús Francisco Espinoza Fierro por su trabajo como sinodales, y gracias a la Dra. Miriam Bocardo Gaspar por haber participado como revisora externa.

Por último, agradezco al Consejo Nacional de Ciencia y Tecnología por la beca que me permitió ser un estudiante de tiempo completo durante mis estudios de Maestría.

Índice general

Introducción

Para cada número natural n el n-ésimo polinomio ciclotómico $\phi_n(x)$ es el polinomio cuyas raíces son las raíces n-ésimas primitivas (complejas) de 1. El grado de cada polinomio ciclotómico está dado por la función φ de Euler y el coeficiente principal es 1, por lo que cada polinomio ciclotómico toma siempre valores positivos cuando $n \geq 3$. Los coeficientes de los polinomios ciclotómicos son enteros, consecuentemente al definir la función Φ_n mediante

$$\Phi_n(x, y) := y^{\varphi(n)} \phi_n \left(\frac{x}{y} \right),$$

obtenemos un polinomio en dos variables con coeficientes enteros que sólo toma valores positivos. El polinomio $\Phi_n(x, y)$ es llamado n-ésima forma binaria ciclotómica y para $m \in \mathbb{N}$ podemos estudiar la ecuación

$$\Phi_n(x, y) = m. \tag{1}$$

Si consideramos el caso $n = 4$, entonces $\Phi_4(x, y) = x^2 + y^2$ y la ecuación (1) toma la forma

$$\Phi_4(x, y) = x^2 + y^2 = m,$$

es decir, estamos en el clásico estudio de los números representables como suma de dos cuadrados, por lo que el estudiar la ecuación (1) puede entenderse como una generalización de este problema.

El matemático húngaro K. Győry obtuvo una cota para las soluciones de $\Phi_n(x, y) = m$ dada por

$$\text{máx}\{|x|, |y|\} \leq 2|m|^{\frac{1}{\varphi(n)}}. \tag{2}$$

É. Fouvry, C. Levesque y M. Waldschmidt (ver [1]) dieron algunos resultados sobre este tema, entre ellos, tres son particularmente importantes. El primero proporciona una mejora óptima a la cota (2) y también permite derivar una cota para n. Una consecuencia más, es que hará posible continuar el estudio de (1) con un enfoque diferente. Se define para cada par de números naturales n y N, el conjunto

$$\mathcal{A}(\Phi_n; N) := \{m \in \mathbb{N} \mid m \leq N, m = \Phi_n(x, y) \text{ para algún } (x, y) \in \mathbb{Z}^2, \text{máx}\{|x|, |y|\} \geq 2\},$$

y luego se considera la unión

$$\mathcal{A}(\Phi_{\{n\geq 3\}}; N) := \bigcup_{n\geq 3} \mathcal{A}(\Phi_n; N). \tag{3}$$

El estudio de este conjunto da lugar al segundo resultado, el cual demuestra la existencia de un par de sucesiones que determinan el comportamiento asintótico de la cardinalidad de $\mathcal{A}(\Phi_{\{n\geq 3\}}; N)$. Finalmente, el tercer resultado se enfoca en el número a_m de ternas (n, x, y) tales que $\Phi_n(x, y) = m$, es decir, la cantidad de representaciones por formas binarias ciclotómicas que m posee. Se demuestra que el valor promedio de la cantidad de representaciones a_m crece como $\sqrt{\log m}$.

Esta tesis contiene un desarrollo de estos resultados y para ello será necesario presentar contenido de dos ramas de la teoría de números. Por un lado tendremos una teoría algebraica y por otro una teoría analítica. La primera involucra el estudio de los anillos $\mathbb{Z}[i]$ y $\mathbb{Z}[j]$, conocidos como el anillo de enteros Gaussianos y el anillo de enteros de Eisenstein. Mientras que las series de Dirichlet y el método de Selberg-Delange representarán la parte analítica. Más importante aún, veremos cómo estas dos ramas se unen para poder demostrar el resultado sobre el conjunto $\mathcal{A}(\Phi_{\{n\geq 3\}}; N)$.

Vale la pena mencionar que las ideas y métodos tratados en este trabajo no son exclusivamente útiles para formas binarias ciclotómicas, es decir, podrían ser aplicados a otro tipo de formas binarias.

El Capítulo 1 está enfocado al estudio de los polinomios ciclotómicos y de las formas binarias ciclotómicas. Obtendremos una cota inferior para el valor mínimo de $\phi_n(x)$ y probaremos un lema sobre formas binarias. Esta teoría nos ayudará a demostrar el primer resultado importante en este trabajo.

En el Capítulo 2 estudiaremos la aritmética de los anillos $\mathbb{Z}[i]$ y $\mathbb{Z}[j]$. Probaremos que en estos dos conjuntos se satisface el Teorema Fundamental de la Aritmética, es decir, que cada elemento tiene una representación única como producto de primos. Esto nos permitirá determinar cómo son los números representables por las formas binarias $\Phi_3(x, y)$ y $\Phi_4(x, y)$. Caracterizar a los números representables por estas formas es un paso importante para entender el comportamiento de la cardinalidad de $\mathcal{A}(\Phi_{\{n\geq 3\}}; N)$.

El tercer capítulo está dedicado al estudio del método de Selberg-Delange, ya que nos proporciona una aproximación de las sumas parciales de un tipo de series de Dirichlet que serán de nuestro interés.

En el Capítulo 4 probaremos la mejora a la cota (2) dada por Győry y los resultados correspondientes a la cardinalidad de $\mathcal{A}(\Phi_{\{n\geq 3\}}; N)$ y la sucesión (a_m).

Capítulo 1

Formas binarias ciclotómicas

Las formas binarias ciclotómicas se definen a partir de los polinomios ciclotómicos, es por esto que la primera sección de este capítulo está dedicada principalmente a estas funciones. Veremos algunas fórmulas importantes para el obtención del n-ésimo polinomio ciclotómico $\phi_n(x)$ y algunas de sus propiedades. También incluiremos un importante resultado sobre formas binarias definidas positivamente.

La segunda sección se enfoca en el estudio de los valores mínimos de los polinomios ciclotómicos. Obtendremos algunas cotas inferiores que sólo dependerán de los divisores primos de n debido a la naturaleza de los polinomios ciclotómicos, así como una cota para la función φ de Euler. Estos resultados serán necesarios para probar el primer resultado importante de este trabajo, el cual nos permitirá estudiar el comportamiento asintótico de la cantidad de números representables por formas binarias ciclotómicas.

1.1. Polinomios ciclotómicos y formas binarias

Los polinomios ciclotómicos son muy sencillos de definir, primero necesitamos considerar al conjunto μ_n de raíces n-ésimas de la unidad en $\mathbb{C}$. Este conjunto contiene n elementos y está dado por

$$\mu_n = \left\{ e^{\frac{2\pi i}{n}k} \mid 1 \leq k \leq n \right\}.$$

Considerando a μ_n con el producto usual de números complejos, μ_n tiene estructura de grupo cíclico, de aquí que μ_n contiene generadores, los cuales son llamados raíces n-ésimas primitivas de la unidad. Denotaremos por E_n a este conjunto. No es difícil ver que E_n contiene $\varphi(n)$ elementos, los cuales son de la forma $e^{\frac{2\pi i m}{n}}$ con m primo relativo a n.

Definición 1.1. Sea $n \in \mathbb{N}$ y E_n el conjunto de raíces n-ésimas primitivas de la unidad. Definimos el n-ésimo polinomio ciclotómico $\phi_n(x)$ mediante

$$\phi_n(x) := \prod_{\zeta \in E_n} (x - \zeta).$$

Como las raíces del polinomio $x^n - 1$ son precisamente las raíces n-ésimas de la unidad, podemos escribir

$$x^n - 1 = \prod_{\zeta \in \mu_n} (x - \zeta). \tag{1.1}$$

Agrupando los factores $x - \zeta$, donde $\zeta \in \mu_n$ es un elemento de orden d, tenemos

$$x^n - 1 = \prod_{d|n} \prod_{\zeta \in E_d} (x - \zeta).$$

En la igualdad anterior el segundo producto es la definición de $\phi_d(x)$, así que obtuvimos la factorización

$$x^n - 1 = \prod_{d|n} \phi_d(x). \tag{1.2}$$

Esta identidad nos permite calcular $\phi_n(x)$ recursivamente para cualquier n.

Ejemplo 1.2. De la definición de polinomio ciclotómico vemos que

$$\phi_1(x) = x - 1 \qquad \text{y} \qquad \phi_2(x) = x + 1.$$

Usando (1.2) para calcular $\phi_3(x)$ obtenemos

$$x^3 - 1 = \phi_1(x)\phi_3(x) = (x - 1)\phi_3(x),$$

y despejando nos da

$$\phi_3(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1.$$

Similarmente

$$x^4 - 1 = \phi_1(x)\phi_2(x)\phi_4(x) = (x - 1)(x + 1)\phi_4(x),$$

de aquí que $\phi_4(x)$ esta dado por

$$\phi_4(x) = x^2 + 1.$$

Ejemplo 1.3. En el caso de $n = p$ un primo, la fórmula (1.2) nos permite obtener

$$\phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + ... + x + 1.$$

Podemos deducir de la definición que el polinomio ciclotómico $\phi_n(x)$ es mónico, de grado $\varphi(n)$ y además tiene coeficientes enteros.

El siguiente teorema nos permitirá obtener una expresión para $\phi_n(x)$ que involucra a la función de Möbius μ, (Definición A.1), la cual nos servirá para derivar más propiedades sobre los polinomios ciclotómicos.

Teorema 1.4 (Fórmula de Inversión de Möbius)**.** *Sea f una función aritmética y F definida mediante*

$$F(n) = \prod_{d|n} f(d),$$

entonces

$$f(n) = \prod_{d|n} F\left(\frac{n}{d}\right)^{\mu(d)}.$$

Demostración. La prueba es directa, sólo tenemos que hacer los cálculos necesarios. Para cada $n \in \mathbb{N}$,

$$\prod_{d|n} F\left(\frac{n}{d}\right)^{\mu(d)} = \prod_{d|n}\prod_{t|\frac{n}{d}} f(t)^{\mu(d)} = \prod_{t|n} f(t)^{\sum_{d|n,t|\frac{n}{d}}\mu(d)} = \prod_{t|n} f(t)^{\sum_{d|\frac{n}{t}}\mu(d)} = f(n).$$

En la última igualdad utilizamos la ecuación (A.2) del Apéndice. □

El Teorema 1.4 junto con la ecuación (1.2) nos permite obtener el siguiente resultado.

Corolario 1.5. *Sea $n \in \mathbb{N}$, entonces*

$$\phi_n(x) = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)}.$$

Esta última expresión para $\phi_n(x)$ nos ayudará a deducir algunas fórmulas muy útiles para calcular polinomios ciclotómicos.

Proposición 1.6. *Sea p un número primo y $n \in \mathbb{N}$. Entonces*

$$\phi_{np}(x) = \begin{cases} \phi_n(x^p) & si\ p|n, \\ \dfrac{\phi_n(x^p)}{\phi_n(x)} & si\ p \nmid n. \end{cases}$$

Demostración. Supongamos que $p|n$. Por el corolario anterior,

$$\phi_{np}(x) = \prod_{d|np} \left(x^{\frac{np}{d}} - 1\right)^{\mu(d)} = \prod_{d|n} \left(x^{\frac{np}{d}} - 1\right)^{\mu(d)} \prod_{\substack{d|np \\ d\nmid n}} \left(x^{\frac{np}{d}} - 1\right)^{\mu(d)} = \phi_n(x^p) \prod_{\substack{d|np \\ d\nmid n}} (x^{\frac{np}{d}} - 1)^{\mu(d)}$$

Si $d \mid np$ y $d \nmid n$, entonces $p^2 \mid d$ ya que $p|n$, consecuentemente d no es libre de cuadrados y así $\mu(d) = 0$, por lo tanto

$$\prod_{\substack{d|np \\ d\nmid n}} \left(x^{\frac{np}{d}} - 1\right)^{\mu(d)} = 1,$$

lo que implica que $\phi_{np}(x) = \phi_n(x^p)$.

Supongamos ahora que p es un primo tal que $p \nmid n$, entonces

$$\begin{aligned}\phi_{np}(x) &= \prod_{d|np} \left(x^{\frac{np}{d}} - 1\right)^{\mu(d)} = \prod_{d|n} \left(x^{\frac{np}{d}} - 1\right)^{\mu(d)} \prod_{d|n} \left(x^{\frac{np}{pd}} - 1\right)^{\mu(pd)} \\ &= \prod_{d|n} \left(x^{\frac{np}{d}} - 1\right)^{\mu(d)} \prod_{d|n} \left(x^{\frac{n}{d}} - 1\right)^{-\mu(d)} = \frac{\phi_n(x^p)}{\phi_n(x)}.\end{aligned}$$

□

Como una consecuencia inmediata tenemos el siguiente corolario que generaliza la proposición anterior.

Corolario 1.7. *Sea p un número primo y $n, k \in \mathbb{N}$. Entonces*

$$\phi_{np^k}(x) = \begin{cases} \phi_n(x^{p^k}) & \text{si } p|n, \\ \dfrac{\phi_n(x^{p^k})}{\phi_n(x^{p^{k-1}})} & \text{si } p \nmid n. \end{cases}$$

Demostración. De la proposición anterior tenemos,

$$\phi_{np^k}(x) = \phi_{np^{k-1}}(x^p) = \phi_{np^{k-2}}(x^{p^2}) = \ldots = \phi_{np}(x^{p^{k-1}}).$$

Realizando una iteración más de este proceso obtenemos,

$$\phi_{np^k}(x) = \begin{cases} \phi_n(x^{p^k}) & \text{si } p|n, \\ \dfrac{\phi_n(x^{p^k})}{\phi_n(x^{p^{k-1}})} & \text{si } p \nmid n. \end{cases}$$

□

Gracias a este corolario podemos derivar una propiedad muy interesante que reduce considerablemente los cálculos para obtener los polinomios $\phi_n(x)$. Esta propiedad nos dice que los polinomios ciclotómicos sólo dependen del radical de n[1].

[1]Recordemos que para $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, su radical R es definido como el producto $p_1 p_2 \cdots p_r$.

Teorema 1.8. *Sea $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ y R el radical de n. Entonces*

$$\phi_n(x) = \phi_R(x^{\frac{n}{R}}).$$

Demostración. La prueba es una aplicación del corolario anterior. Si escribimos n como el producto $n = (p_1 p_2^{e_2} \cdots p_r^{e_r}) \cdot p_1^{e_1 - 1}$, entonces

$$\phi_n(x) = \phi_{p_1 p_2^{e_2} \cdots p_r^{e_r}}(x^{p_1^{e_1 - 1}}).$$

Aplicando este método a cada primo en la expresión de n, obtenemos

$$\phi_n(x) = \phi_R(x^{\frac{n}{R}})$$

□

El Corolario 1.7 nos permite obtener una última propiedad en el caso en que $\phi_n(x)$ satisface que $n = 2m$ con m impar mayor que 1.

Teorema 1.9. *Sea $n = 2m$ con m impar y $m \geq 3$. Entonces*

$$\phi_n(x) = \phi_m(-x). \tag{1.3}$$

Demostración. Por el Corolario 1.7 tenemos que

$$\phi_{2m}(x) = \frac{\phi_m(x^2)}{\phi_m(x)} = \frac{\prod_{d|m}(x^{2d} - 1)^{\mu(\frac{m}{d})}}{\prod_{d|m}(x^d - 1)^{\mu(\frac{m}{d})}} = \frac{\prod_{d|m}\left((x^d - 1)(x^d + 1)\right)^{\mu(\frac{m}{d})}}{\prod_{d|m}(x^d - 1)^{\mu(\frac{m}{d})}} = \prod_{d|m}(x^d + 1)^{\mu(\frac{m}{d})},$$

podemos factorizar un -1 en el último término porque todos los divisores de m son impares, por lo que $(-x)^d = -x^d$, y así

$$\phi_{2m}(x) = \prod_{d|m}(-1)^{\mu(\frac{m}{d})}((-x)^d - 1)^{\mu(\frac{m}{d})} = (-1)^{\sum_{d|m}\mu(d)}\phi_m(-x).$$

Como $\sum_{d|m}\mu(d) = 0$, (ver Apéndice A), se sigue que

$$\phi_{2m} = \phi_m(-x).$$

□

Definición 1.10. Sea $P(x) = a_0 + a_1 x + ... + a_n x^n$ un polinomio. Diremos que $P^*(x)$ dado por

$$P^*(x) = a_n + a_{n-1} x + ... + a_0 x^n,$$

es el polinomio recíproco de $P(x)$. Si $P(x) = P^*(x)$ diremos que $P(x)$ es autorrecíproco.

Observemos que una forma de obtener $P^*(x)$ es mediante la fórmula $P^*(x) = x^n P(1/x)$, donde n es el grado de $P(x)$.

Proposición 1.11. *Los polinomios ciclotómicos $\phi_n(x)$ son autorrecíprocos para toda $n \geq 2$.*

Demostración. Es evidente que $\phi_2(x) = x + 1$ es autorrecíproco. Sea $n \geq 3$ y $\phi_n(x)$ el n-ésimo polinomio ciclotómico. Entonces

$$\phi_n^*(x) = x^{\varphi(n)} \prod_{\zeta \in E_n} \left(\frac{1}{x} - \zeta \right) = \prod_{\zeta \in E_n} (1 - x\zeta) = \prod_{\zeta \in E_n} \overline{\zeta}(1 - x\zeta). \tag{1.4}$$

La última igualdad de la ecuación se da porque si $\zeta \in E_n$ entonces $\overline{\zeta}$ también pertenece a E_n, lo que implica

$$\prod_{\zeta \in E_n} \zeta = 1 = \prod_{\zeta \in E_n} \overline{\zeta}.$$

Continuando la igualdad (1.4) y tomando en cuenta que hay una cantidad par de términos en el producto, tenemos

$$\phi_n^*(x) = \prod_{\zeta \in E_n} (\overline{\zeta} - x) = \prod_{\zeta \in E_n} (\zeta - x) = \prod_{\zeta \in E_n} (x - \zeta) = \phi_n(x).$$

□

Utilizaremos el término *forma binaria* para referirnos a cualquier polinomio homogéneo en dos variables. El siguiente lema es un resultado general sobre formas binarias asociadas a polinomios en una variable.

Lema 1.12. *Sea $f(x) \in \mathbb{Z}[x]$ un polinomio distinto de cero de grado d sin raíces reales. Sea $g(x) = x^d f(1/x)$ el polinomio recíproco de $f(x)$ y supongamos que el coeficiente del término de mayor grado de $f(x)$ es positivo, de modo que los siguientes números son positivos:*

$$\begin{cases} \gamma_1 = \inf\limits_{t \in \mathbb{R}} f(t), & \gamma_2 = \inf\limits_{t \in \mathbb{R}} g(t), \\ \gamma_1' = \inf\limits_{|t| \leq 1} f(t), & \gamma_2' = \inf\limits_{|t| \leq 1} g(t), \quad \gamma' = \min\{\gamma_1', \gamma_2'\}. \end{cases}$$

Sea $F(x, y)$ la forma binaria $y^d f(x/y)$ asociada a $f(x)$.
I. Entonces para cada $(x, y) \in \mathbb{Z}^2$ tenemos

$$F(x, y) \geq \gamma_1 |y|^d, \qquad F(x, y) \geq \gamma_2 |x|^d, \qquad F(x, y) \geq \gamma' \max\{|x|^d, |y|^d\}.$$

II. Más aun:

(i) Para cualquier número real c_1 *con* $c_1 > \gamma_1$*, existe una infinidad de parejas* $(x, y) \in \mathbb{Z}^2$ *con* $y > 0$ *y*

$$F(x, y) < c_1 y^d.$$

(ii) Además, para cualquier c_2 *con* $c_2 > \gamma_2$*, existe una infinidad de parejas* $(x, y) \in \mathbb{Z}^2$ *con* $x > 0$ *y*

$$F(x, y) < c_2 x^d.$$

(iii) También, para cualquier número real c *con* $c > \gamma'$*, existe una infinidad de parejas con* $(x, y) \in \mathbb{Z}^2$ *y*

$$F(x, y) < c \max\{|x|^d, |y|^d\}.$$

Demostración. La prueba de I es bastante sencilla:

$$F(x, y) = y^d f\Big(\frac{x}{y}\Big) = |y|^d f\Big(\frac{x}{y}\Big) \geq |y|^d \inf_{t\in\mathbb{R}} f(t) = |y|^d \gamma_1,$$

para todo $(x, y) \in \mathbb{Z}^2$. Análogamente para la desigualdad $F(x, y) \geq |x|^d \gamma_2$, teniendo en cuenta que $F(x, y) = x^d g(y/x)$. Luego, si $|x| \leq |y|$, entonces

$$F(x, y) \geq \gamma_1' |y|^d \geq \gamma' |y|^d$$

y

$$F(x, y) \geq \gamma_2' |x|^d \geq \gamma' |x|^d$$

si $|x| \geq |y|$, de donde es claro que

$$F(x, y) \geq \gamma' \max\{|x|^d, |y|^d\}.$$

Para la parte (i) de II, sea $t_0 \in \mathbb{R}$ tal que $f(t_0) = \gamma_1$. Sea $c_1 > \gamma_1$, entonces $c_1 = \gamma_1 + \varepsilon$. Como f' es continua, existe $\delta > 0$ donde para $t \in (t_0 - \delta, t_0 + \delta)$ tenemos

$$|f(t) - \gamma_1| = |f(t) - f(t_0)| < \varepsilon |t - t_0|,$$

ya que $f'(t_0) = 0$.

Para $y \in \mathbb{N}$, sea $x \in \mathbb{Z}$ tal que

$$\left|t_0 - \frac{x}{y}\right| \leq 1 \qquad \text{y} \qquad \left|t_0 - \frac{x}{y}\right| < \delta,$$

entonces

$$\left|f\Big(\frac{x}{y}\Big) - \gamma_1\right| < \varepsilon \left|\frac{x}{y} - t_0\right| \leq \varepsilon.$$

En otras palabras, nos estamos aproximando a t_0 con el racional x/y. Más aun, existe una infinidad de parejas (x, y) con las que podemos hacer esto. Luego,

$$\big|F(x, y) - y^d f(t_0)\big| = \left|y^d f\Big(\frac{x}{y}\Big) - y^d f(t_0)\right| < \varepsilon y^d.$$

Finalmente, como $F(x,y) - y^d f(t_0) \leq |F(x,y) - y^d f(t_0)|$, tenemos

$$F(x,y) < (\gamma_1 + \varepsilon)y^d = c_1 y^d.$$

La demostración es análoga para (ii).

La prueba de (iii) será por casos. Supongamos primero $c > \gamma' = \gamma_1'$ y sea t_0 tal que $f(t_0) = \gamma_1$. Si $\gamma_1' = \gamma_1$, podemos utilizar la prueba anterior para encontrar una infinidad de parejas (x,y) con $|x| \leq |y|$ (ya que $t_0 \leq 1$) y

$$F(x,y) < c|y|^d.$$

Como $y^d = \max\{|x|^d, |y|^d\}$ terminanos.

Supongamos ahora que $\gamma_1' > \gamma_1$. Entonces, $c > \gamma' = \gamma_1' > \gamma_1$, lo que implica que $t_0 \geq 1$ por lo que existe una infinidad de parejas (x,y) con $|x| \geq |y|$ tal que

$$F(x,y) < cy^d \leq cx^d = c\max\{|x|^d, |y|^d\}.$$

Es decir, en cualquier caso $F(x,y) > c\max\{|x|^d, |y|^d\}$. La prueba es análoga para el caso $c > \gamma_2' = \min\{\gamma_1', \gamma_2'\}$. □

Definición 1.13. La n-ésima forma binaria ciclotómica $\Phi_n(x,y)$ se define como

$$\Phi_n(x,y) := y^{\varphi(n)}\phi_n\Big(\frac{x}{y}\Big).$$

Como ejemplo tenemos a las formas $\Phi_3(x,y) = x^2 + xy + y^2$ y $\Phi_4(x,y) = x^2 + y^2$, las cuales serán muy importantes más adelante.

El Lema 1.12 nos permite obtener sencillamente un corolario al aplicarlo a formas binarias ciclotómicas. Notemos primero que como $\phi_n(x)$ es autorrecíproco, las constantes definidas en el lema son todas iguales. Sólo es necesario probar que

$$\inf_{t\in\mathbb{R}} \phi_n(t) = \inf_{|t|\leq 1} \phi_n(t).$$

En efecto, observemos que para $1 \leq |t|$ tenemos

$$\inf_{1\leq|t|} \phi_n(t) = \inf_{1\leq|t|} \phi_n^*(t) = \inf_{1\leq|t|} t^{\varphi(n)}\phi_n\left(\frac{1}{t}\right) \geq \inf_{1\leq|t|} \phi_n\left(\frac{1}{t}\right) = \inf_{|t|\leq 1} \phi_n(t).$$

Por lo tanto, tenemos el siguiente resultado.

Corolario 1.14. *Sea $n \geq 3$. Consideremos $\phi_n(x)$ el n-ésimo polinomio ciclotómico y $\gamma = \inf_{t\in\mathbb{R}} \phi_n(t)$. Entonces para cualquier $(x,y) \in \mathbb{Z}^2$ se tiene*

$$\Phi_n(x,y) \geq \gamma\max\{|x|, |y|\}^{\varphi(n)}.$$

1.2. Las constantes c_n

Para cada $n \geq 3$ definimos la constante c_n mediante $c_n := \text{ínf}_{x\in\mathbb{R}}\, \phi_n(x)$. Como vimos en la Sección 1.1, sabemos que

$$c_n = \inf_{|x|\leq 1} \phi_n(x)$$

y que c_n es positiva. La siguiente proposición nos da el valor de c_n para un caso especial de polinomios ciclotómicos y una cota inferior de c_n para el resto.

Proposición 1.15. *Sea n un número natural con $n \geq 3$.*

(1) Si $n = 2^{e_0}$ es una potencia de 2, entonces $c_n = 1$.

(2) Si $n = 2^{e_0} p_1^{e_1} \cdots p_r^{e_r}$, con $p_1, p_2, ..., p_r$ primos impares y $p_1 < p_2 < \cdots < p_r$, entonces

$$c_n = c_{p_1 \cdots p_r} \geq \frac{1}{p_1^{2^{r-2}}}.$$

Demostración. Para (1), como $\phi_n(x) = \phi_{2^{e_0}}(x)$, usando el Teorema 1.8 tenemos

$$\phi_{2^{e_0}}(x) = \phi_2(x^{2^{e_0-1}}) = x^{2^{e_0-1}} + 1,$$

lo que implica que $c_n = \phi_n(0) = 1$.

Para (2), utilizando el Teorema 1.8 de nuevo vemos que $c_n = c_{2p_1p_2\cdots p_r}$. Dado que el Teorema 1.9 nos dice que para m impar $c_{2m} = c_m$, concluimos que

$$c_n = c_{p_1p_2\cdots p_r}.$$

Esto significa que podemos suponer sin pérdida de generalidad que n es impar y libre de cuadrados. Es suficiente probar que

$$\phi_{p_1p_2\cdots p_r}(x) \geq \frac{1}{p_1^{2^{r-2}}}$$

para x con $|x| \leq 1$.

Empecemos con el caso $r = 1$, es decir, $n = p$ con p primo impar. Para $-1 \leq x \leq 0$, tenemos

$$1 \leq 1 - x^p \leq 1 - x \leq 2,$$

lo que implica

$$\frac{1}{2} \leq \frac{1 - x^p}{1 - x} \leq 1.$$

Como

$$\phi_p(x) = \frac{x^p - 1}{x - 1},$$

entonces $\phi_p(x)$ está acotado por $1/2 \leq \phi_p(x) \leq 1$ para $-1 \leq x \leq 0$. Ahora, si $0 \leq x \leq 1$ es claro que

$$1 \leq \phi_p(x) \leq p,$$

ya que $\phi_p(x) = 1 + x + x^2 + \cdots x^{p-1}$. Combinando las desigualdades obtenidas

$$\frac{1}{2} \leq \phi_p(x) \leq p$$

para $|x| \leq 1$. Obsérvese que para $p \geq 5$,

$$\frac{1}{p^{2^{-1}}} = \frac{1}{\sqrt{p}} \leq \frac{1}{2} \leq \phi_p(x),$$

es decir, si p es un primo impar mayor que 3 terminamos. Si $p = 3$, un cálculo directo nos da que $c_3 = 3/4 \geq \frac{1}{3^{2-1}}$. Esto concluye la prueba para el caso $r = 1$.

Supongamos ahora que $r \geq 2$, es decir, $n = p_1 \cdots p_r$. El número n tiene 2^r divisores, donde la mitad dividen a $p_2 \cdots p_r$ y la otra mitad son divisores de la forma $p_1 d$ donde $d | p_2 \cdots p_r$. Así, que podemos escribir

$$\begin{aligned}
\phi_n(x) &= \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})} \\
&= \prod_{d|p_2\cdots p_r} (x^d - 1)^{\mu(n/d)} \prod_{d|p_2\cdots p_r} (x^{p_1 d} - 1)^{\mu(n/p_1 d)} \\
&= \prod_{d|p_2\cdots p_r} (x^d - 1)^{\mu(p_1)\mu(\frac{p_2\cdots p_r}{d})} \prod_{d|p_2\cdots p_r} (x^{p_1 d} - 1)^{\mu(\frac{p_2\cdots p_r}{d})} \\
&= \prod_{d|p_2\cdots p_r} (x^d - 1)^{-\mu(\frac{p_2\cdots p_r}{d})} (x^{p_1 d} - 1)^{\mu(\frac{p_2\cdots p_r}{d})}.
\end{aligned}$$

Dado que $\phi_{p_1}(x^d) = (x^d - 1)^{-1}(x^{dp_1} - 1)$ vemos que cuando $\mu(p_2 \cdots p_r/d) = 1$ aparece 2^{r-2} veces el factor $\phi_{p_1}(x^d)$ en el producto anterior y cuando $\mu(p_2 \cdots p_r/d) = -1$ aparece $1/\phi_{p_1}(x^d)$ la misma cantidad de veces. Usando que para $-1 \leq x \leq 0$ teniamos que $1/2 \leq \phi_{p_1}(x) \leq 1$, entonces

$$\frac{1}{2} \leq \phi_{p_1}(x^d) \leq 1, \tag{1.5}$$

ya que d es impar por ser un divisor de $p_2 \cdots p_r$.

Sea $Q_1(x)$ el producto de los 2^{r-2} factores de la forma $\phi_{p_1}(x^d)$ y $Q_2(x)$ el producto de los factores $1/\phi_{p_1}(x^d)$. La ecuación (1.5) implica

$$\frac{1}{2^{2^{r-2}}} \leq Q_1(x) \leq 1 \qquad \text{y} \qquad 1 \leq Q_2(x) \leq 2^{2^{r-2}}.$$

Como $\phi_n(x) = Q_1(x)Q_2(x)$, tenemos que

$$\frac{1}{2^{2^{r-2}}} \leq \phi_{p_1 p_2 \cdots p_r}(x) \leq 2^{2^{r-2}}$$

para $-1 \leq x \leq 0$. Para $0 \leq x \leq 1$, sabemos que

$$1 \leq \phi_{p_1}(x^d) \leq p_1$$

y entonces

$$\frac{1}{p_1^{2^{r-2}}} \leq \phi_{p_1 p_2 \cdots p_r}(x) \leq p_1^{2^{r-2}}$$

para $|x| \leq 1$. Por lo tanto

$$c_n \geq \frac{1}{p_1^{2^{r-2}}}.$$

□

El siguiente lema es un resultado auxiliar que nos permitirá obtener una importante cota inferior para las constantes c_n en términos de la función φ de Euler.

Lema 1.16. *Para cualquier entero impar libre de cuadrados $n = p_1 \cdots p_r$ con $p_1 < p_2 < \ldots < p_r$ tal que $n \geq 11$ y $n \neq 15$, se tiene*

$$\varphi(n) > 2^{r+1} \log p_1.$$

Demostración. Si $r = 1$ entonces n es un primo mayor o igual que 11, entonces se cumple que

$$\varphi(n) = n - 1 > 2^2 \log n.$$

Si $r = 2$ y $n \geq 15$, entonces $p_2 \geq 7$, luego

$$\varphi(p_1 p_2) = (p_1 - 1)(p_2 - 2) \geq 6(p_1 - 1) > 2^2 \cdot 2 \log p_1 = 2^3 \log p_1.$$

Por último, si $r \geq 3$, entonces

$$\varphi(n) = (p_1 - 1) \cdots (p_r - 1) \geq (p_1 - 1)4^{r-1} = (p_1 - 1)2^{2(r-1)} \geq (p_1 - 1)2^{r+1} > 2^{r+1} \log p_1.$$

□

Proposición 1.17. *Para $n \geq 3$, se tiene que*

$$c_n \geq \left(\frac{\sqrt{3}}{2}\right)^{\varphi(n)}.$$

Demostración. Observemos que si $n = 2^e p_1^{e_1} \cdots p_r^{e_r}$ con $p_1, \ldots, p_r$ primos impares, entonces

$$\begin{aligned}
\varphi(n) &= \varphi(2^e)(p_1 - 1)(p_2 - 1) \cdots (p_r - 1) p_1^{e_1 - 1} p_2^{e_2 - 1} \cdots p_r^{e_r - 1} \\
&\geq (p_1 - 1)(p_2 - 1) \cdots (p_r - 1) \\
&= \varphi(p_1)\varphi(p_2) \cdots \varphi(p_r) \\
&= \varphi(p_1 p_2 \cdots p_r).
\end{aligned}$$

Además, como $\sqrt{3}/2 < 1$, entonces

$$\left(\frac{\sqrt{3}}{2}\right)^{\varphi(n)} \leq \left(\frac{\sqrt{3}}{2}\right)^{\varphi(p_1 p_2 \cdots p_r)}.$$

Por lo tanto, es suficiente probar el resultado para n impar y libre de cuadrados. Supongamos que n es de esta forma. Claramente el resultado es verdadero cuando $n = 3$, pues $c_3 = 3/4$. En los casos $n = 5, 7, 15$ se puede comprobar numéricamente que

$$c_5 > 0.6 > \left(\frac{\sqrt{3}}{2}\right)^4, \qquad c_7 > 0.6 > \left(\frac{\sqrt{3}}{2}\right)^6, \qquad c_{15} > 0.5 > \left(\frac{\sqrt{3}}{2}\right)^8.$$

Para $n \geq 11$, por la Proposición 1.15 y el Lema 1.16 tenemos

$$2^3 \log c_n \geq -2^3 2^{r-2} \log p_1 = -2^{r+1} \log p_1 \geq -\varphi(n),$$

de donde

$$\log c_n \geq \frac{-\varphi(n)}{8}.$$

Despejando c_n concluimos que

$$c_n \geq e^{-\varphi(n)/8} = (e^{-1/8})^{\varphi(n)} \geq \left(\frac{\sqrt{3}}{2}\right)^{\varphi(n)}.$$

□

La cota inferior anterior es la mejor posible, ya que para el caso $n = 3$ tenemos la igualdad:

$$c_3 = \frac{3}{4} = \left(\frac{\sqrt{3}}{2}\right)^2 = \left(\frac{\sqrt{3}}{4}\right)^{\varphi(3)}.$$

Además, como $c_6 = c_3$ y $\varphi(6) = 2$, la igualdad también se satisface en el caso $n = 6$.

Capítulo 2

Las ecuaciones $\Phi_3(x, y) = m$ y $\Phi_4(x, y) = m$

En el conjunto de los números naturales el algoritmo de Euclides nos permite encontrar el máximo común divisor entre dos números a y b. Este algoritmo es de nuestro interés porque nos permite generalizar el Teorema Fundamental de la Aritmética en ciertos anillos, y entre ellos, existen dos que son particularmente importantes para nosotros y son conocidos como el anillo de enteros Gaussianos y de enteros de Eisenstein. El estudio de la aritmética de estos conjuntos nos permitirá caracterizar a los números representables por las formas binarias $\Phi_3(x, y)$ y $\Phi_4(x, y)$.

2.1. Enteros Gaussianos

Definición 2.1. Un *entero Gaussiano* es un número complejo de la forma

$$a + bi,$$

donde $a, b \in \mathbb{Z}$. Denotamos al conjunto de enteros Gaussianos por $\mathbb{Z}[i]$.

En esta sección, usaremos el término *entero racional* para referirnos a un elemento de $\mathbb{Z}$ y utilizaremos exclusivamente letras griegas para denotar a los enteros Gaussianos.

Definición 2.2. Diremos que ξ es divisible por $\eta \neq 0$ si existe $\zeta \in \mathbb{Z}[i]$ tal que

$$\xi = \eta\zeta.$$

Llamamos a η un divisor de ξ y lo denotamos por $\eta|\xi$.

Es fácil ver que si $\gamma|\eta$ y $\eta|\zeta$, entonces $\gamma|\zeta$. También se satisface que si α divide a una cantidad finita de elementos $\gamma_1, \gamma_2, ..., \gamma_n$ entonces

$$\alpha|\beta_1\gamma_1 + ... + \beta_n\gamma_n,$$

para todo $\beta_i \in \mathbb{Z}[i]$.

Definición 2.3. Un entero Gaussiano ϵ es una unidad en $\mathbb{Z}[i]$ si ϵ divide a todo ξ en $\mathbb{Z}[i]$.

Utilizaremos la letra griega ϵ para denotar a una unidad. Una rápida observación nos permite obtener que $1, -1, i, -i$ son unidades en $\mathbb{Z}[i]$ ya que cualquier entero Gaussiano ξ tiene los 8 divisores "triviales"

$$1, \xi, -1, -\xi, i, i\xi, -i, -i\xi.$$

Definición 2.4. La *norma* de un entero $\xi = a + bi$ denotada por $N(\xi)$ se define por

$$N(\xi) = N(a + bi) = a^2 + b^2.$$

Como esta norma es el cuadrado de la definición usual de norma en $\mathbb{C}$, es fácil ver que

$$N(\xi) = \xi\overline{\xi} \quad \text{y} \quad N(\xi\eta) = N(\xi)N(\eta).$$

Teorema 2.5. *La norma de una unidad es 1, y cualquier entero Gaussiano cuya norma es 1 es una unidad.*

Demostración. Si ϵ es una unidad, entonces $\epsilon|1$, lo que implica que $1 = \epsilon\eta$ para algún $\eta \in \mathbb{Z}[i]$, y así

$$1 = N(\epsilon)N(\eta).$$

Esto significa que $N(\epsilon)|1$, por lo tanto $N(\epsilon) = 1$.
Suponamos ahora que $N(a + bi) = 1$, entonces

$$1 = a^2 + b^2 = (a + bi)(a - bi),$$

esto es, $a + bi$ divide a 1, consecuentemente $a + bi$ divide a todo elemento en $\mathbb{Z}[i]$, por lo tanto $a + bi$ es una unidad. □

Gracias a este teorema queda claro que las unidades en $\mathbb{Z}[i]$ son $1, i, -1, -i$, ya que las únicas soluciones a la ecuación $1 = a^2 + b^2 = (a + bi)(a - bi)$ son

$$a = \pm 1,\ b = 0; \qquad a = 0,\ b = \pm 1.$$

Definición 2.6. Sea ϵ una unidad y $\xi \in \mathbb{Z}[i]$, diremos que el entero $\epsilon\xi$ es un *asociado* de ξ.

De la definición anterior vemos que los asociados de ξ son por lo tanto

$$\xi, i\xi, -\xi, -i\xi.$$

Es importante mencionar este concepto ya que si η es divisible por ξ, entonces η es divisible por cualquier asociado de ξ.

En la siguiente definición hablaremos de los primos Gaussianos o primos en $\mathbb{Z}[i]$, para que no haya confusión, nos referiremos por *primos racionales* a los números primos definidos en $\mathbb{N}$.

Definición 2.7. Un *primo* en $\mathbb{Z}[i]$ es un entero Gaussiano distinto cero y de una unidad, cuyos divisores son únicamente sus asociados y las unidades.

Nótese que cualquier asociado de un primo es también un primo.

Teorema 2.8. *Cualquier entero Gaussiano distinto de 0 y de una unidad, es divisible por un primo en* $\mathbb{Z}[i]$.

Demostración. Sea $\gamma \neq 0$ un entero en $\mathbb{Z}[i]$ distinto de una unidad. Si γ es un primo el teorema es trivial. Supongamos que γ no es primo, entonces

$$\gamma = \alpha_1\beta_1$$

con $N(\alpha_1) > 1$, $N(\beta_1) > 1$ y $N(\gamma) = N(\alpha_1)N(\beta_1)$. Esto implica que

$$1 < N(\alpha_1) < N(\gamma).$$

Si α_1 no es un primo, entonces

$$\alpha_1 = \alpha_2\beta_2$$

con $N(\alpha_2) > 1$, $N(\beta_2) > 1$, $N(\alpha_1) = N(\alpha_2)N(\beta_2)$ y

$$1 < N(\alpha_2) < N(\alpha_1).$$

Podemos continuar este proceso siempre y cuando α_r no sea un primo. Como la sucesión

$$N(\gamma), N(\alpha_1), N(\alpha_2), ...$$

es estrictamente decreciente, este proceso no puede continuar indefinidamente, esto significa que existe r tal que α_r es primo. Si α_r es primo, entonces

$$\gamma = \beta_1\alpha_1 = \beta_1\beta_2\alpha_2 = ... = \beta_1\beta_2\beta_3\cdots\beta_r\alpha_r,$$

y así $\alpha_r|\gamma$. □

Teorema 2.9. *Cualquier entero en $\mathbb{Z}[i]$ distinto de cero y de una unidad, es un producto de primos Gaussianos.*

Demostración. Sea $\gamma \in \mathbb{Z}[i]$ distinto de cero y de una unidad. Por el teorema anterior γ es divisible por un primo π_1, entonces

$$\gamma = \pi_1\gamma_1, \qquad N(\gamma_1) < N(\gamma).$$

Si γ_1 no es una unidad, entonces

$$\gamma_1 = \pi_2\gamma_2, \qquad N(\gamma_2) < N(\gamma_1).$$

Continuando este proceso, obtenemos una sucesión estrictamente decreciente

$$N(\gamma), N(\gamma_1), N(\gamma_2), ...,$$

de enteros racionales positivos. Entonces $N(\gamma_r) = 1$ para algun r y γ_r es una unidad, por lo tanto

$$\gamma = \pi_1\pi_2 \cdots \pi_r\epsilon = \pi_1\pi_2 \cdots \pi_r',$$

donde π_r' es un primo asociado a π_r. □

Hemos demostrado que cualquier entero en $\mathbb{Z}[i]$ es un produto de primos, sin embargo, aun no hemos probado nada sobre la unicidad de esta representación.

Teorema 2.10. *Dados cualesquiera dos enteros Gaussianos γ y γ_1 con $\gamma_1 \neq 0$, existen enteros κ y γ_2 en $\mathbb{Z}[i]$ tales que*

$$\gamma = \kappa\gamma_1 + \gamma_2, \quad N(\gamma_2) < N(\gamma_1).$$

Demostración. Como $\gamma_1 \neq 0$, tenemos

$$\frac{\gamma}{\gamma_1} = R + Si,$$

donde R y S son reales. Podemos encontrar dos enteros racionales x y y tales que

$$|R - x| \leq \frac{1}{2}, \qquad |S - y| \leq \frac{1}{2},$$

y luego

$$\left|\frac{\gamma}{\gamma_1} - (x + iy)\right| = |(R - x) + i(S - y)| = \left\{(R - x)^2 + (S - y)^2\right\}^{\frac{1}{2}} \leq \frac{1}{\sqrt{2}}.$$

Si tomamos

$$\kappa = x + iy, \quad \text{y } \gamma_2 = \gamma - \kappa\gamma_1,$$

tenemos

$$|\gamma - \kappa\gamma_1| \leq \frac{|\gamma_1|}{\sqrt{2}}.$$

Elevando al cuadrado obtenemos

$$N(\gamma_2) = N(\gamma - \kappa\gamma_1) \leq \frac{1}{2}N(\gamma_1).$$

Esto completa la prueba, ya que

$$\gamma = \kappa\gamma_1 + \gamma_2 \quad \text{y} \quad N(\gamma_2) < N(\gamma_1).$$

□

Usando el teorema anterior podemos aplicar el algoritmo de Euclides en $\mathbb{Z}[i]$ a dos enteros γ y $\gamma_1 \neq 0$, lo que nos permite encontrar un entero ξ que divide a ambos y con la propiedad de que cualquier otro divisor común de γ y γ_1 divide a ξ.

Definición 2.11. Si ζ es un divisor común de γ y β, y cualquier divisor común de γ y β divide a ζ, diremos que ζ es un *máximo común divisor* de γ y β, y escribimos $\zeta = (\gamma, \beta)$.

Observemos que el máximo común divisor no es único, debido a que cualquiera de sus asociados es también un máximo común divisor. Si η y ζ son ambos máximo común divisores, por definición $\eta|\zeta$ y $\zeta|\eta$, y así

$$\zeta = \phi\eta \qquad \text{y} \qquad \eta = \theta\zeta,$$

combinando estas igualdades

$$\zeta = \phi\theta\zeta,$$

entonces $\theta\phi = 1$, es decir, ϕ y θ son unidades y entonces η es un asociado de ζ, por lo que *el máximo común divisor es único salvo asociados.*

Teorema 2.12. *Si $\gamma_1|\beta\gamma$ y $1 = (\gamma, \gamma_1)$, entonces $\gamma_1|\beta$.*

Demostración. Del algoritmo de Euclides vemos que

$$\beta\rho = (\beta\gamma, \beta\gamma_1),$$

donde ρ es un máximo común divisor de γ y γ_1 obtenido con el algoritmo. Como $1 = (\gamma, \gamma_1)$, entonces ρ es una unidad, y así

$$\beta = (\beta\gamma, \beta\gamma_1).$$

Sabemos por hipótesis que $\gamma_1|\beta\gamma$ y que $\gamma_1|\beta\gamma_1$, por la definición de máximo común divisor se sigue que

$$\gamma_1|(\beta\gamma, \beta\gamma_1),$$

es decir, $\gamma_1|\beta$. □

Si π es un primo y $(\pi, \gamma) = \mu$, entonces $\mu|\pi$ y $\mu|\gamma$, por lo que sucede uno de los dos siguientes casos:

(1) μ es una unidad y entonces $(\pi, \gamma) = 1$,

(2) μ es un asociado de π, y así $\pi|\gamma$.

Consecuentemente, si tomamos $\gamma_1 = \pi$ en el Teorema 2.12, obtenemos el siguiente resultado.

Teorema 2.13. *Si π es primo y $\pi|\beta\gamma$, entonces $\pi|\beta$ o $\pi|\gamma$.*

Ahora contamos con todo lo necesario para demostrar el Teorema Fundamental de la Aritmética para Enteros Gaussianos.

Teorema 2.14 (Teorema Fundamental de la Aritmética para Enteros Gaussianos)**.** *Cada entero distinto de cero y de la unidad, puede ser expresado de forma única como un producto de primos en $\mathbb{Z}[i]$, salvo por el orden de los primos, la presencia de unidades y primos asociados.*

Demostración. Sea γ un entero en $\mathbb{Z}[i]$ y supongamos que γ tiene dos representaciones diferentes como producto de primos, es decir,

$$\gamma = \pi_1^{a_1}\pi_2^{a_2}\cdots\pi_m^{a_m} = \eta_1^{b_1}\eta_2^{b_2}\cdots\eta_n^{b_n},$$

donde en cada representación ninguno de los factores primos son asociados. Por el teorema anterior (aplicado recursivamente) vemos que $\pi_1|\eta_1$ o $\pi_1|\eta_2$ o ... $\pi_1|\eta_n$, entonces $\pi_1 = \epsilon\eta_i$ para algún $1 \leq i \leq n$. Aplicando la misma observación en cada primo π_i en la primera representación para γ y en cada primo de la segunda representación, concluimos que $m = n$. Podemos reordenar las expresiones para γ de modo que $\pi_i = \epsilon_i\eta_i$ para cada $i = 1, 2, ..., n$. Resumiendo tenemos

$$\gamma = \pi_1^{a_1}\pi_2^{a_2}\cdots\pi_n^{a_n} = (\epsilon_1\eta_1)^{b_1}(\epsilon_2\eta_2)^{b_2}\cdots(\epsilon_n\eta_n)^{b_n}. \tag{2.1}$$

Supongamos que $a_i > b_i$ para algún i, dividiendo la ecuación (2.1) por $\pi_i^{b_i}$ obtenemos

$$\pi_1^{a_1}\cdots\pi_i^{a_i-b_i}\cdots\pi_n^{a_n} = (\epsilon_1\eta_1)^{b_1}\cdots(\epsilon_{i-1}\eta_{i-1})^{b_{i-1}}(\epsilon_{i+1}\eta_{i+1}^{b_{i+1}})\cdots(\epsilon_n\eta_n)^{b_n},$$

lo que significa que π_i no divide al entero de la derecha en la igualdad anterior y sí divide a la expresión de la izquierda, lo cual es una contradicción, ya que (2.1) nos dice que cualquier representación de un entero debe de contener los mismos divisores primos salvo asociados. Aplicando el mismo razonamiento para $b_i > a_i$ llegamos a la misma contradicción, por lo tanto $a_i = b_i$. Concluimos que la representación de un entero como producto de primos es única a excepción de las ambigüedades causadas por la presencia de unidades y primos asociados. □

Obsérvese que en cualquier anillo con división euclidiana podemos encontrar un resultado análogo al Teorema Fundamental de la Aritmética, ya que el Teorema 2.10 es la base de este teorema.

2.2. Caracterización de los primos en $\mathbb{Z}[i]$

Sea π un un primo en $\mathbb{Z}[i]$. Por la definición de norma tenemos

$$\pi | N(\pi) = \pi\overline{\pi},$$

lo que implica que existen enteros racionales positivos divisibles por π. Sea a un entero racional con estas características. Como a es un producto de primos racionales, π debe dividir a uno de ellos por el Teorema 2.13. Si dividiera a dos, digamos p y q, entonces

$$\pi | px - qy = 1$$

para apropiados x y y, lo cual no es posible. Esto prueba el siguiente resultado.

Teorema 2.15. *Cualquier primo π en $\mathbb{Z}[i]$ es divisor de sólo un primo racional.*

Al igual que en la sección anterior, usaremos los términos *entero racional* para referirnos a un elemento en $\mathbb{Z}$ y *entero* para referirnos a un entero Gaussiano.

Observemos que si p es un número primo racional tal que $\pi = a + bi | p$ y $p = \pi\lambda$, entonces

$$N(\pi)N(\lambda) = p^2.$$

Esto nos deja con dos posibilidades: $N(\lambda) = 1$, λ es una unidad y π un asociado de p; o bien, tenemos que

$$N(\pi) = a^2 + b^2 = (a + bi)(a - bi) = p. \tag{2.2}$$

Teorema 2.16. *Un entero cuya norma es un primo racional es un primo en $\mathbb{Z}[i]$.*

Demostración. Supongamos que $N(\xi) = p$ es un primo racional y que $\xi = \eta\zeta$, entonces

$$p = N(\eta)N(\zeta).$$

Esto implica que $N(\eta) = 1$ o que $N(\zeta) = 1$, es decir, η es una unidad y ζ un asociado de ξ o viceversa. En cualquier caso ξ tiene únicamente como divisores a sus asociados y las unidades, por lo tanto ξ es un primo. □

El teorema anterior implica que si π es un primo de este tipo, entonces $\overline{\pi}$ también es primo, ya que $N(\pi) = N(\overline{\pi})$.

Proposición 2.17. *Los primos en $\mathbb{Z}[i]$ son:*

(1) $1+i$ y sus asociados,

(2) los primos racionales de la forma $p = 4m+3$ y sus asociados,

(3) los factores $a+bi$ y $a-bi$ de los primos racionales de la forma $p = 4m+1$ y sus asociados.

Demostración. Como todo primo en $\mathbb{Z}[i]$ es un divisor de sólo un primo racional p, tenemos los siguientes tres casos:

(1) Si $p = 2$, entonces
$$p = 1^2 + 1^2 = (1+i)(1-i).$$
Esto implica que $1+i$, $1-i$, $-1+i$ y $-1-i$ son los únicos primos en $\mathbb{Z}[i]$ que dividen a 2.

(2) Si $p \equiv 3 \pmod 4$, entonces es imposible que p satisfaga la ecuación (2.2) ya que un cuadrado es congruente a 0 o 1 módulo 4, esto implica que la suma de dos cuadrados no es congruente a 3 módulo 4. Por lo que los únicos divisores de primos p son las unidades y sus asociados.

(3) Si $p = 4n+1$, de la ecuación (A.4) sabemos que -1 es un residuo cuadrático para primos de esta forma, lo que implica que existe x tal que $p|x^2+1$ y entonces
$$p|(x+i)(x-i).$$
Si p fuera un primo en $\mathbb{Z}[i]$ entonces dividiría a $x+i$ o $x-i$, pero esto es falso ya que los números
$$\frac{x}{p} \pm \frac{i}{p}$$
no son enteros. Se sigue que $p = \pi\lambda$ con $\pi = a+bi$ y $\lambda = a-bi$, salvo multiplicación por una unidad.

□

Teorema 2.18. *Un entero $n \geq 1$ es de la forma $n = x^2+y^2$ si y sólo si n se puede expresar como el producto*
$$n = 2^a p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m} q_1^{2b_1} q_2^{2b_2} \cdots q_n^{2b_n},$$
donde $p_i \equiv 1 \pmod 4$ para $i = 1, ..., m$ y $q_k \equiv 3 \pmod 4$ para $k = 1, ..., n$.

Demostración. Supongamos que n es representable. Entonces, existe γ en $\mathbb{Z}[i]$ tal que

$$n = N(\gamma)$$

y sabemos por el Teorema Fundamental de la Aritmética para Enteros Gaussianos que γ tiene la representación como producto de primos dada por

$$\gamma = (1+i)^a(x_1+y_1i)^{a_1}\cdots(x_m+y_mi)^{a_m}q_1^{b_1}\cdots q_n^{b_n}, \tag{2.3}$$

donde $(x_j + y_j i)$ es factor de un primo $p_j \equiv 1 \pmod 4$ para toda $j = 1, ..., m$ y q_k es de la forma $q_k \equiv 3 \pmod 4$, $k = 1, ..., n$. Como la norma en $\mathbb{Z}[i]$ es multiplicativa podemos ver que

$$\begin{aligned} n &= N(\gamma) \\ &= N\left[(1+i)^a(x_1+y_1i)^{a_1}\cdots(x_m+y_mi)^{a_m}q_1^{b_1}\cdots q_n^{b_n}\right] \\ &= [N(1+i)]^a[N(x_1+y_1i)]^{a_1}\cdots[N(x_m+y_mi)]^{a_m}[N(q_1)]^{b_1}\cdots[N(q_n)]^{b_n} \\ &= 2^a p_1^{a_1}\cdots p_m^{a_m}q_1^{2b_1}\cdots q_n^{2b_n} \end{aligned}$$

El resultado recíproco es inmediato ya que n es la norma del entero γ dado en (2.3). □

2.3. Enteros de Eisenstein

La teoría que vimos en la sección anterior sobre la aritmética en $\mathbb{Z}[i]$ no se tiene únicamente en este subconjunto de $\mathbb{C}$, recordemos que i es solución a la ecuación $\phi_4(x) = x^2 + 1 = 0$, veremos que podemos hacer un estudio análogo para la ecuación $\phi_3(x) = x^2 + x + 1 = 0$.

Definición 2.19. Definimos un entero de Eisenstein γ como el número complejo

$$\gamma = a + bj,$$

donde j es la solución a la ecuación $x^2 + x + 1 = 0$, dada por

$$j = \frac{-1+\sqrt{-3}}{2}.$$

Denotaremos a este conjunto de enteros mediante $\mathbb{Z}[j]$ y durante esta sección usaremos la palabra *entero* para referirnos de forma exclusiva a un elemento de este conjunto. Nótese que j satisface las siguientes dos identidades:

$$j + j^2 = -1 \quad \text{y} \quad j^3 = 1.$$

Definiremos los conceptos de *divisor*, *unidad*, *asociado* y *primo* igual que en $\mathbb{Z}[i]$.

Definición 2.20. La norma $N(\gamma)$ de un entero $\gamma = a + bj$ en $\mathbb{Z}[j]$ se define mediante

$$N(a + bj) = a^2 - ab + b^2$$

Podemos ver que la norma satisface la siguiente igualdad

$$N(a + bj) = \left(a - \frac{1}{2}b\right)^2 + \frac{3}{4}b^2 \tag{2.4}$$

lo que implica que $N(\gamma) > 0$ excepto cuando $\gamma = 0$. Como también

$$N(a + bj) = |a + bj|^2,$$

para dos enteros α y β en $\mathbb{Z}[j]$ se satisface

$$N(\alpha)N(\beta) = |\alpha|^2|\beta|^2 = |\alpha\beta|^2 = N(\alpha\beta).$$

Al igual que con los enteros Gaussianos tenemos los siguientes tres teoremas, cuyas pruebas son análogas a las versiones de $\mathbb{Z}[i]$.

Teorema 2.21. *La norma de una unidad es 1 y cualquier entero de Eisenstein cuya norma sea 1 es una unidad.*

Teorema 2.22. *Cualquier entero en $\mathbb{Z}[j]$ distinto de 0 y de una unidad es divisible por un primo.*

Teorema 2.23. *Cualquier entero en $\mathbb{Z}[j]$ distinto de cero y de una unidad es producto de primos.*

Las unidades son entonces las soluciones a la ecuación $a^2 - ab + b^2 = 1$, y con un análisis de la ecuación (2.4) vemos que las únicas soluciones están dadas por

(1) $a = \pm 1$, $b = 0$;

(2) $a = 0$, $b = \pm 1$;

(3) $a = 1$, $b = 1$;

(4) $a = -1$, $b = -1$.

Esto quiere decir que las unidades son

$$\pm 1, \pm j, \pm(1 + j)$$

y sus asociados. Recordemos que queremos probar que el Teorema Fundamental de la Aritmética es cierto en $\mathbb{Z}[j]$, para ello necesitamos el siguiente teorema.

Teorema 2.24. *Dados dos enteros γ y $\gamma_1 \neq 0$, existen enteros γ_2 y κ tales que*

$$\gamma = \kappa\gamma_1 + \gamma_2$$

con $N(\gamma_2) < N(\gamma_1)$.

Demostración. Escribamos $\gamma = a + bj$, $\gamma_1 = c + dj$ y observemos que

$$\frac{\gamma}{\gamma_1} = \frac{a+bj}{c+dj} = R + Sj,$$

donde R y S son números reales. Podemos encontrar dos enteros racionales x y y tales que

$$|R - x| \leq \frac{1}{2}, \quad |S - y| \leq \frac{1}{2}$$

y entonces

$$\left|\frac{\gamma}{\gamma_1} - (x + yj)\right|^2 = (R-x)^2 - (R-x)(S-y) + (S-y)^2 \leq \frac{3}{4}.$$

Por lo tanto, si $\kappa = x + yj$, $\gamma_2 = \gamma - \kappa\gamma_1$, tenemos

$$N(\gamma_2) = N(\gamma - \kappa\gamma_1) \leq \frac{3}{4}N(\gamma_1) < N(\gamma_1).$$

□

El teorema fundamental en $\mathbb{Z}[j]$ se sigue al usar el mismo argumento que en $\mathbb{Z}[i]$, ya que es el teorema anterior el que da lugar al algoritmo de Euclides y que además nos permite encontrar el máximo común divisor entre dos enteros, el cual es único salvo asociados.

Teorema 2.25. *Supongamos que π es un primo en $\mathbb{Z}[j]$ y π divide a $\gamma = \alpha\beta$, entonces $\pi|\alpha$ o $\pi|\beta$.*

Teorema 2.26 (Teorema Fundamental de la Aritmética para Enteros de Eisenstein)**.** *La expresión de un entero en $\mathbb{Z}[j]$ como producto de primos es única, salvo el orden de los primos, la presencia de unidades y primos asociados.*

2.4. Caracterización de los primos en $\mathbb{Z}[j]$

Los siguientes dos teoremas son muy importantes en la identificación de primos en $\mathbb{Z}[j]$, son idénticos a los teoremas 2.15 y 2.16, y la prueba es la misma. Recordemos que también en esta sección *entero racional* se refiere a un entero en $\mathbb{Z}$ y *entero* a un elemento de $\mathbb{Z}[j]$, los últimos denotados por letras griegas. De igual manera, *primo racional* y *primo* se refieren a un primo en $\mathbb{N}$ y a un primo de Eisenstein.

Teorema 2.27. *Cualquier primo π en $\mathbb{Z}[j]$ es un divisor de sólo un primo racional.*

Teorema 2.28. *Si $N(\gamma) = p$ con p un primo racional, entonces γ es un primo en $\mathbb{Z}[j]$.*

Al igual que en $\mathbb{Z}[i]$, vemos que si $\pi|p$ donde p es un primo racional y $\pi = a + bj$, entonces $p = \pi\lambda$ y luego

$$N(\pi)N(\lambda) = p^2$$

ya que $p = p + 0j$, lo que implica uno de los siguientes dos casos: $N(\lambda) = 1$ o $N(\pi) = 1$ y entonces π o λ es un asociado de p; o tenemos que

$$N(\pi) = a^2 - ab + b^2 = p.$$

Esto significa que si p tiene la representación $p = a^2 - ab + b^2$ entonces tiene como divisores a los primos $a + bj$ y $\overline{a + bj}$ junto con sus asociados adecuados.

Teorema 2.29. *Los primos en $\mathbb{Z}[j]$ son:*

(1) $1 - j$ *y sus asociados,*

(2) los primos racionales de la forma $3n + 2$ *y sus asociados,*

(3) los factores $a + bj$ *de los primos racionales de la forma* $3n + 1$.

Demostración. Como todo primo en $\mathbb{Z}[j]$ es divisor de un sólo primo racional tenemos los siguientes tres casos:

(1) Se sigue a partir del Teorema 2.28, ya que

$$3 = (1 - j)(1 - j^2) = (1 + j)(1 - j)^2 = -j^2(1 - j)^2.$$

(2) Si $p \equiv 2 \pmod 3$ es imposible que $N(\pi) = p$, ya que la norma de cualquier entero es congruente a 0 o 1 módulo 3, de aquí que p es divisible únicamente por asociados y unidades.

(3) Si $p \equiv 1 \pmod 3$ entonces

$$\left(\frac{-3}{p}\right) = 1$$

por la ecuación (A.4), esto significa que existe $x \in \mathbb{Z}$ tal que $p|x^2+3$. Como

$$x^2 + 3 = (x + 1 + 2j)(x - 1 - 2j),$$

si p fuera primo dividiría a $x + 1 + 2j$ o a $x - 1 - 2j$, sin embargo,

$$\pm\frac{2j}{p}$$

no es entero en $\mathbb{Z}[j]$. Se sigue que p es divisible por un primo $\pi = a + bj$ y que

$$p = N(\pi) = a^2 - ab + b^2.$$

□

Ahora nos encontramos listos para caracterizar a los primos que son representables por la forma binaria ciclotómica $\Phi_3(x, y) = x^2 + xy + y^2$.

Teorema 2.30. *Un entero $n \geq 1$ es de la forma*

$$n = x^2 + xy + y^2$$

si y sólo si n se puede expresar como el producto

$$n = 3^a p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m} q_1^{2b_1} q_2^{2b_2} \cdots q_n^{2b_n}, \tag{2.5}$$

donde $p_i \equiv 1 \pmod 3$ para $i = 1, ..., m$ y $q_k \equiv 2 \pmod 3$ para $k = 1, ..., n$.

Demostración. Supongamos que n es representable, entonces

$$n = N(x - yj) = x^2 + xy + y^2,$$

por el Teorema Fundamental de la Aritmética en $\mathbb{Z}[j]$ podemos escribir

$$x - yj = (1 - j)^a (x_1 + y_1 j)^{a_1} \cdots (x_m + y_m j)^{a_m} q_1^{b_1} \cdots q_n^{b_n}.$$

Usando la multiplicatividad de la norma obtenemos que

$$\begin{aligned} n &= N(x - yj) \\ &= N[(1 - j)^a (x_1 + y_1 j)^{a_1} \cdots (x_m + y_m j)^{a_m} q_1^{b_1} \cdots q_n^{b_n}] \\ &= [N(1 - j)]^a [N(x_1 + y_1 j)]^{a_1} \cdots [N(x_m + y_m j)]^{a_m} [N(q_1)]^{b_1} \cdots [N(q_n)]^{b_n} \\ &= 3^a p_1^{a_1} \cdots p_m^{a_m} q_1^{2b_1} \cdots q_n^{2b_n}. \end{aligned}$$

Recíprocamente, si n es de la forma (2.5), las ecuaciones anteriores nos muestran que n es la norma del entero $x - yj$ y así $n = x^2 + xy + y^2$. □

2.5. Enteros representables por las formas $\Phi_3(x,y)$ y $\Phi_4(x,y)$

El conjunto de enteros representables por la forma binaria $\Phi_3(x,y)$ y el conjunto de los enteros representables por $\Phi_4(x,y)$ poseen elementos en común y podemos derivar un resultado análogo a los teoremas 2.18 y 2.30 al combinar ambos resultados.

Denotaremos por $N_{a,q}$ a aquel número cuyos divisores primos p son congruentes con a módulo q. Es decir, si

$$p|N_{a,q} \implies p \equiv a \pmod{q}.$$

Esta notación nos permite expresar de una forma mas sencilla a los teoremas 2.18 y 2.30 mediante:

(1) Un entero n es representable por la forma binaria ciclotómica $\Phi_4(x,y)$ si y sólo si n se puede expresar como

$$n = 2^a N_{1,4} N_{3,4}^2,$$

para algún $a \geq 0$.

(2) Un entero n es representable por la forma binaria ciclotómica $\Phi_3(x,y)$ si y sólo si n se puede expresar como

$$n = 3^b N_{1,3} N_{2,3}^2,$$

para algún $b \geq 0$.

Con una aplicación directa del teorema chino del residuo podemos deducir el siguiente teorema de los dos resultados anteriores.

Teorema 2.31. *Un entero $n \geq 1$ es simultáneamente de las formas*

$$n = u^2 + uv + v^2 = x^2 + y^2$$

si y sólo si existen enteros $a, b \geq 0$, $N_{1,12}$, $N_{5,12}$, $N_{7,12}$, $N_{11,12}$ y $N_{1,12}$ tales que

$$n = \left(2^a 3^b N_{5,12} N_{7,12} N_{11,12}\right)^2 N_{1,12}.$$

Capítulo 3

Método de Selberg-Delange

Dada una serie de Dirichlet $F(s) = \sum_{n=1}^{\infty} a_n n^{-s}$, el método de Selberg-Delange proporciona un resultado sobre el comportamiento asintótico de la suma

$$\sum_{n \leq x} a_n,$$

siempre que $F(s)$ se "parezca" lo suficiente a una potencia de la función zeta de Riemann $\zeta(s)$, (Definición B.2), específicamente que $F(s) = G(s)\zeta(s)^z$, donde $G(s)$ satisface ciertas propiedades que veremos más adelante. El método de Selberg-Delange no es sencillo, sin embargo, su complejidad es justificada por su utilidad.

Utilizaremos la notación $s = \sigma + it$ para referirnos al número complejo complejo s y usaremos $f(s) = O(g(s))$ y $f(s) \ll g(s)$ de forma equivalente. Es decir, ambas notaciones significan que $|f(s)| \leq C|g(s)|$ para $|s|$ suficientemente grande. Diremos que C es la constante implicita y cuando C dependa de algun parámetro α, escribiremos $f(s) = O_\alpha(s)$ o $f(s) \ll_\alpha g(s)$.

3.1. Potencias de $\zeta(s)$

Definiendo el coeficiente binomial generalizado para $w \in \mathbb{C}$ y $\nu \in \mathbb{Z}_{\geq 0}$ por

$$\binom{w}{\nu} := \frac{1}{\nu!} \prod_{j=0}^{\nu-1} (w - j),$$

por el Teorema Generalizado del Binomio, podemos escribir para $|\xi| < 1$ y $z \in \mathbb{C}$,

$$(1 - \xi)^{-z} = \sum_{\nu=0}^{\infty} \binom{z + \nu - 1}{\nu} \xi^\nu.$$

Cuando z es un entero negativo la ecuación anterior se reduce a la fórmula clásica. Usando la Fórmula del Producto de Euler, vemos que para $\sigma > 1$,

$$\zeta(s)^z = \prod_p (1-p^{-s})^{-z} = \prod_p \left(1 + \sum_{\nu=1}^{\infty} \binom{z+\nu-1}{\nu} p^{-\nu s}\right).$$

Como la serie

$$\sum_p \sum_{\nu=1}^{\infty} \binom{z+\nu-1}{\nu} p^{-\nu s}$$

converge absolutamente para $\sigma > 1$, entonces por el Teorema I.2.4 de [3], la función $\zeta(s)^z$ es representable en ese semiplano como la serie de Dirichlet de la función multiplicativa $\tau_z(n)$, dada por

$$\tau_z(p^\nu) = \binom{z+\nu-1}{\nu}.$$

Veremos que la función $Z(s;z) = s^{-1}\{(s-1)\zeta(s)\}^z$ juega un papel particularmente importate. La función $Z(s;z)$ está definida en cualquier región que no incluya ceros de $\zeta(s)$, dado que la función no sería analítica en esos puntos. Podemos escoger la rama principal del logaritmo de modo que

$$Z(1;z) = 1.$$

La demostración del primer lema de esta sección hace uso de los conocidos polinomios de Bernoulli (Sección C del apéndice), como es usual denotamos por $B_n(x)$ a la n-ésima función de Bernoulli y por B_n al n-ésimo coeficiente.

Lema 3.1. *La función $\zeta(s)$ no se anula en la región $|s-1| < 1$.*

Demostración. El Teorema B.10 nos dice que para $\sigma > 0$ la función $\zeta(s)$ satisface

$$\zeta(s) = \sum_{n \le x} n^{-s} + \frac{x^{1-s}}{s-1} + \frac{\{x\}}{x^s} - s\int_x^\infty \{u\}u^{-s-1}du,$$

donde $\{u\}$ denota la parte fraccionaria de u. Particularmente para $x = 1$

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

Para continuar, integraremos por partes varias veces hasta obtener el resultado. En la primera iteración utilizamos que $dB_1(u) = d\{u\}$ y que $|u^s| = u^\sigma$ para concluir

$$-s\int_1^\infty u^{-s-1}\{u\}du = \{u\}u^{-s}\Big|_1^\infty - \int_1^\infty u^{-s}dB_1(u) = -\int_1^\infty u^{-s}dB_1(u).$$

Continuando el proceso:

$$-\int_1^\infty u^{-s}dB_1(u) = -B_1\left(u^{-s}\Big|_1^\infty\right) - \frac{1}{2}\int_1^\infty su^{-s-1}dB_2(u) = B_1 - \frac{1}{2}\int_1^\infty su^{-s-1}dB_2(u).$$

Sólo falta calcular la última integral:

$$\begin{aligned}\int_1^\infty su^{-s-1}dB_2(u) &= B_2\left(su^{-s-1}\big|_1^\infty\right) + s(s+1)\int_1^\infty u^{-s-2}B_2(u)du \\ &= -sB_2 + s(s+1)\int_1^\infty u^{-s-2}B_2(u)du.\end{aligned}$$

Combinando los cálculos anteriores llegamos a

$$\zeta(s) = \frac{1}{s-1} + \frac{1}{2} + \frac{s}{12} - \frac{s(s+1)}{2}\int_1^\infty u^{-s-2}B_2(u)du$$

Supongamos que $\zeta(\rho) = 0$ para algún $\rho = \beta + i\tau$, con $|\rho - 1| < 1$. Por la ecuación funcional para $\zeta(s)$ (Corolario B.15 en el apéndice B), podemos asumir que $\beta \geq \frac{1}{2}$. Como $|B_2(u)| \leq B_2 = \frac{1}{6}$ y $-(\beta+2) \leq \frac{-5}{2}$ tenemos que

$$\left|\int_1^\infty B_2(u)u^{-(\rho+2)}du\right| \leq \frac{1}{6}\int_1^\infty u^{-(\beta+2)}du \leq \frac{1}{6}\int_1^\infty u^{-5/2}du.$$

Sea v el complejo con el mismo argumento que $\int_1^\infty B_2(u)u^{-(\rho+2)}du$ y módulo

$$\frac{\left|\int_1^\infty B_2(u)u^{-(\rho+2)}du\right|}{\frac{1}{6}\int_1^\infty u^{-5/2}du}.$$

Entonces

$$0 = \zeta(\rho) = \frac{1}{\rho-1} + \frac{1}{2}\left(1 + \frac{\rho}{6} - \frac{1}{6}\rho(\rho+1)v\int_1^\infty u^{-5/2}du\right).$$

Multiplicando por $\rho - 1$ ambos lados de la ecuación y calculando el valor de la integral

$$0 = 1 + \frac{1}{2}(\rho-1)\left(1 + \frac{\rho}{6} - \frac{1}{9}\rho(\rho+1)v\right).$$

De esta última ecuación obtenemos al despejar que

$$\begin{aligned}1 &= \frac{1}{2}|\rho-1|\left|1 + \frac{1}{6}\rho - \frac{1}{9}\rho(\rho+1)v\right| < \frac{1}{2}\left(1 + \frac{1}{6}|\rho| + \frac{1}{9}|\rho(\rho+1)|\right) \\ &< \frac{1}{2}\left(1 + \frac{1}{3} + \frac{6}{9}\right) = 1,\end{aligned}$$

lo cual es una contradicción. Por lo tanto $\zeta(s)$ no se anula en $|s-1| < 1$. □

Como consecuencia del lema anterior, tenemos la siguiente propiedad de analiticidad para la función $Z(s;z)$.

Teorema 3.2. *La función $Z(s;z)$ es holomorfa en el disco $|s-1|<1$ y puede ser representada por la serie de Taylor*

$$Z(s;z)=\sum_{j=0}^{\infty}\frac{1}{j!}\gamma_j(z)(s-1)^j,$$

donde los coeficientes $\gamma_j(z)$ son funciones enteras de z que satisfacen para toda $A>0$ y $\varepsilon>0$ la cota superior

$$\frac{1}{j!}\gamma_j(z)\ll_{A,\varepsilon}(1+\varepsilon)^j \qquad (|z|\leq A).$$

Demostración. Observemos primero que $Z(s;z)$ es holomorfa en $|s-1|<1$, lo cual es una consecuencia de que $Z(s;z)$ sea el producto de las funciones s^{-1} y $(s-1)\zeta(s)^z$, ambas holomorfas en esa región. Podemos escribir entonces por el Teorema de Taylor,

$$Z(s;z)=\sum_{j=0}^{\infty}A_j(z)(s-1)^j.$$

Luego, para $r<1$, aplicando la fórmula de Cauchy,

$$A_j(z)=\frac{1}{j!}\gamma_j(z)=\frac{1}{2\pi}\int_{|s-1|=r}\frac{Z(s;z)}{(s-1)^{j+1}}ds=\frac{1}{2\pi}\int_{|s-1|=r}\frac{s^{-1}(s-1)^z\zeta(s)^z}{(s-1)^{j+1}}ds,$$

por lo que

$$|A_j(z)|\leq\frac{1}{2\pi}\int_{|s-1|=r}\frac{|(s-1)^z\zeta(s)^z|}{|s|r^{j+1}}|ds|\leq\max_{|s-1|=r}|(s-1)^z\zeta(s)^z|\frac{1}{(1-r)r^j}.$$

Como $r^{-1}=1+\varepsilon$, reescribiendo la ecuación anterior en términos de ε resulta en

$$\begin{aligned}|A_j(z)|&\leq\max_{|s-1|=r}|(s-1)^z\zeta(s)^z|\frac{(1+\varepsilon)^j(1+\varepsilon)}{\varepsilon}\\&\ll_{\varepsilon}\max_{|s-1|=r}|(s-1)^z\zeta(s)^z|(1+\varepsilon)^j\end{aligned}$$

Como $|z|\leq A$, el resultado se sigue. □

Sabemos que la región libre de ceros para $\zeta(s)$ es de la forma

$$\sigma \geq 1 - \frac{c}{(1 + \log^+ t)}, \tag{3.1}$$

donde $\log^+ t = \max\{0, \log t\}$. Denotaremos por $\mathcal{D}$ el conjunto simplemente conexo obtenido al eliminar el segmento $[1-c, 1]$ de la región libre de ceros de $\zeta(s)$. Tenemos entonces la continuación analítica

$$\zeta(s)^z = sZ(s; z)(s-1)^{-z} \qquad (s \in \mathcal{D}). \tag{3.2}$$

Usando la cota para $\log \zeta(s)$ (Teorema 16 del Capítulo II.3, [3]) dada por $|\log \zeta(s)| \leq \log\log|t| + O(1)$ y válida para $|t| > 3$ y $\sigma \geq 1 - c/\log|t|$, entonces

$$|\zeta(s)^z| = \left|e^{z \log \zeta(s)}\right| \leq e^{A(\log|\zeta(s)|+\pi)} \leq e^{A\pi} e^{A|\log \zeta(s)|} \ll e^{A\pi} e^{A(\log\log|t|+1)} = e^{A(\pi+1)} (\log|t| + 1)^A .$$

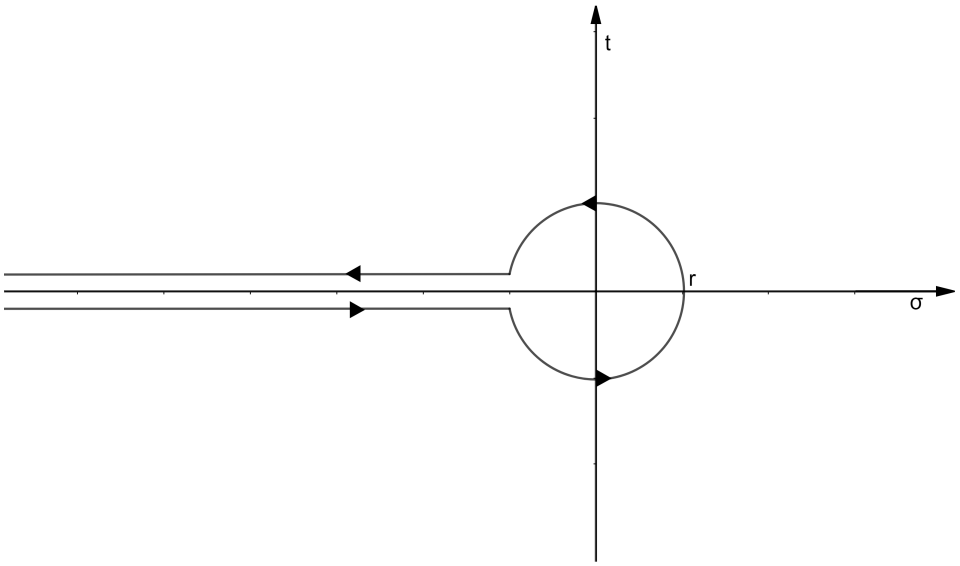
Podemos concluir que para $s \in \mathcal{D}$ con $|z| < A$ y $|s-1| \gg 1$

$$|\zeta(s)^z| \ll_A (\log|t| + 1)^A .$$

3.2. Fórmula de Hankel

En esta sección presentaremos un resultado clásico que involucra a la función gamma, el cual necesitaremos en nuestro estudio de las series de Dirichlet que se "parecen" a una potencia compleja de la función zeta de Riemann.

Definición 3.3. Dado $r > 0$, definimos el *contorno de Hankel* denotado por $\mathcal{H}$ como la curva por partes formada por el círculo $|s| = r$ excluyendo el punto $s = -r$, junto con la semirrecta $(-\infty, -r]$ trazada dos veces, con respectivos argumentos π y $-\pi$.



Denotaremos con ℓ_1 a la semirrecta que tiene como argumento $-\pi$ y de forma análogamos usamos ℓ_2 para denotar la otra semirrecta.

Teorema 3.4 (Fórmula de Hankel)**.** *Sea $\mathcal{H}$ un contorno de Hankel. Para cualquier complejo z se satisface*

$$\frac{1}{\Gamma(z)} = \frac{1}{2\pi i}\int_{\mathcal{H}} s^{-z}e^s ds$$

Demostración. Notemos que la integral converge absoluta y uniformemente. Primero,

$$\left|\int_{\ell_1} \frac{e^s}{s^z} ds\right| \leq \int_{-\infty}^{-r} \frac{e^\sigma}{s^{\operatorname{Re} z}} |ds| < \infty.$$

donde la convergencia se debe al ser $\sigma < 0$ y es uniforme. Análogamente para la integral sobre ℓ_2. En el caso de la integral sobre la curva $|s| = r$ tenemos

$$\left|\int_{|s|=r} \frac{e^s}{s^z} ds\right| \leq \int_{|s|=r} \frac{e^r}{r^{\operatorname{Re} z}} |ds| = 2\pi e^r r^{1-\operatorname{Re} z} < \infty \tag{3.3}$$

Observemos que esta integral tiende a cero cuando $r \to 0$ y $\operatorname{Re} z < 1$, por lo que el valor de la integral sobre $\mathcal{H}$ está determinado solamente por la integral sobre las semirrectas ℓ_1 y ℓ_2. Haciendo el cambio de variable $s = -\sigma$, tenemos

$$\begin{aligned}
\frac{1}{2\pi i}\int_{\ell_1} s^{-z}e^s ds + \frac{1}{2\pi i}\int_{\ell_2} s^{-z}e^s ds &= -\frac{1}{2\pi i}\int_{\infty}^{r} e^{z\pi i}\sigma^{-z}e^{-\sigma} d\sigma - \frac{1}{2\pi i}\int_{r}^{\infty} e^{-z\pi i}\sigma^{-z}e^{-s} d\sigma \\
&= \frac{1}{2\pi i}\int_{r}^{\infty} \left(e^{z\pi i} - e^{-z\pi i}\right)\sigma^{-z}e^{-\sigma} d\sigma \\
&= \frac{\operatorname{sen}(\pi z)}{\pi}\int_{r}^{\infty} \sigma^{-z}e^{-\sigma} d\sigma
\end{aligned}$$

Luego, haciendo $r \to 0$ en la última ecuación, podemos concluir

$$\frac{1}{2\pi i}\int_{\mathcal{H}} s^{-z}e^s ds = \frac{\operatorname{sen}(\pi z)}{\pi}\Gamma(1-z) = \frac{1}{\Gamma(z)\Gamma(1-z)}\Gamma(1-z) = \frac{1}{\Gamma(z)}.$$

Este resultado es válido para z con $\operatorname{Re} z < 1$ y se extiende a toda z por continuación analítica. □

Corolario 3.5. *Para cada $X > 1$, sea $\mathcal{H}(X)$ la parte del contorno de Hankel situada en el semiplano $\sigma > -X$. Se tiene uniformemente para $z \in \mathbb{C}$*

$$\frac{1}{2\pi i}\int_{\mathcal{H}(X)} s^{-z}e^s ds = \frac{1}{\Gamma(z)} + O\left(47^{|z|}\Gamma(1+|z|)e^{-\frac{X}{2}}\right).$$

Demostración. Notemos que para $s = \sigma e^{\pm i\pi}$ con $\sigma > 1$ tenemos

$$|s^{-z}e^s| = \sigma^{-\operatorname{Re} z}|e^{i\pi z}|e^{-\sigma} = \sigma^{-\operatorname{Re} z}e^{-\operatorname{Im} z\pi}e^{-\sigma} \leq (\sigma e^{\pi})^{|z|}e^{-\sigma}. \tag{3.4}$$

Por otro lado, queremos estimar

$$\begin{aligned}\frac{1}{2\pi i}\int_{\mathcal{H}(X)} s^{-z}e^s ds - \frac{1}{\Gamma(z)} &= \frac{1}{2\pi i}\int_{\mathcal{H}(X)} s^{-z}e^s ds - \frac{1}{2\pi i}\int_{\mathcal{H}} s^{-z}e^s ds \\ &= -\frac{1}{2\pi i}\int_{\ell_1(X)} s^{-z}e^s ds - \frac{1}{2\pi i}\int_{\ell_2(X)} s^{-z}e^s ds,\end{aligned}$$

donde $\ell_1(X)$ es la semirecta $(-\infty, -X]$ y $\ell_2(X)$ su análoga en sentido contrario. Haciendo el cambio de variable $s = -\sigma$ y utilizando la desigualdad (3.4) tenemos

$$\begin{aligned}\left|\frac{1}{2\pi i}\int_{\mathcal{H}(X)} s^{-z}e^s ds - \frac{1}{\Gamma(z)}\right| &\leq \frac{1}{2\pi}\int_X^{\infty}(e^{\pi}\sigma)^{|z|}e^{-\sigma}d\sigma + \frac{1}{2\pi}\int_X^{\infty}(e^{\pi}\sigma)^{|z|}e^{-\sigma}d\sigma \\ &= \frac{e^{\pi|z|}}{\pi}\int_X^{\infty}\sigma^{|z|}e^{-\sigma}d\sigma \leq \frac{e^{\pi|z|-\frac{X}{2}}}{\pi}\int_X^{\infty}\sigma^{|z|}e^{-\frac{\sigma}{2}}d\sigma\end{aligned}$$

Haciendo ahora $\sigma = 2t$ y como $X > 0$, obtenemos

$$\begin{aligned}\left|\frac{1}{2\pi i}\int_{\mathcal{H}(X)} s^{-z}e^s ds - \frac{1}{\Gamma(z)}\right| &\leq \frac{2}{\pi}(2e^{\pi})^{|z|}e^{-\frac{X}{2}}\int_0^{\infty}t^{|z|}e^{-t}dt \\ &= \frac{2}{\pi}(2e^{\pi})^{|z|}e^{-\frac{X}{2}}\Gamma(1+|z|) \\ &= O\left(47^{|z|}\Gamma(1+|z|)e^{-\frac{X}{2}}\right),\end{aligned}$$

ya que $2e^{\pi} < 47$. □

3.3. Método de Selberg-Delange

Nos encontramos casi listos para enunciar el teorema principal de este capítulo, sólo nos harán falta un par de definiciones más. Recordemos que el método de Selberg-Delange nos permite estimar las sumas parciales de los coeficientes a_n de una serie de Dirichlet $F(s) = \sum a_n n^{-s}$.

Definición 3.6. Sean $z \in \mathbb{C}$, $c_0 > 0$, $0 < \delta \leq 1$ y $M > 0$. Decimos que una serie de Dirichlet $F(s) = \sum a_n n^{-s}$ tiene la propiedad $\mathcal{P}(z; c_0, \delta, M)$ si la función

$$G(s; z) = F(s)\zeta(s)^{-z}$$

puede ser continuada analíticamente como una función holomorfa en el conjunto

$$\sigma \geq 1 - \frac{c_0}{1 + \log^+ |t|}$$

y además satisface en esta región la cota

$$|G(s; z)| \leq M(1 + |t|)^{1-\delta}.$$

Si $F(s)$ tiene la propiedad $\mathcal{P}(z; c_0, \delta, M)$ y también existe una sucesión de número reales positivos $(b_n)_{n=1}^{\infty}$ tal que $|a_n| \leq b_n$ para toda $n \in \mathbb{N}$ y la serie

$$\sum_{n=1}^{\infty} b_n n^{-s}$$

satisface la condición $\mathcal{P}(w; c_0, \delta, M)$ para algún complejo w, decimos entonces que $F(s)$ es de tipo $\mathcal{T}(z, w; c_0, \delta, M)$.

En el dominio donde $G(s; z)$ es holomorfa denotaremos su k-ésima derivada parcial respecto a s como

$$G^{(k)}(s; z)$$

y definimos

$$\lambda_k(z) := \frac{1}{\Gamma(z-k)} \sum_{h+j=k} \frac{1}{h!j!} G^{(h)}(1; z)\gamma_j(z),$$

donde $\gamma_j(z)$ son las funciones enteras que aparecen en el Teorema 3.2.

Teorema 3.7. *Sea $F(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ una serie de Dirichlet del tipo $\mathcal{T}(z, w; c_0, \delta, M)$. Entonces, para $x \geq 2$, $N \geq 0$, $A > 0$, $|z| \leq A$ y $|w| \leq A$, se tiene que*

$$\sum_{n \leq x} a_n = x(\log x)^{z-1} \left\{ \sum_{k=0}^{N} \frac{\lambda_k(z)}{(\log x)^k} + O(MR_N(x)) \right\},$$

con

$$R_N(x) := e^{-c_1\sqrt{\log x}} + \left(\frac{c_2 N + 1}{\log x}\right)^{N+1}.$$

Donde las constantes positivas c_1, c_2 y la constante implícita en $O(MR_N(x))$ dependen de a los más c_0, δ y M.

Demostración. Sea $c > 0$ una constante con $c < c_0$ y tal que $\zeta(s)$ no tenga ceros en la región

$$\sigma \geq 1 - \frac{c}{1 + \log^+ |t|}.$$

Entonces $F(s)$ es continuable a una función holomorfa en el dominio $\mathcal{D}$ definido previamente (ver desigualdad (3.1)), y tenemos que

$$F(s) = G(s; z)\zeta(s)^z \ll_A M(1 + \log^+ |t|)^A (1 + t)^{1-\delta} \tag{3.5}$$

uniformemente para $s \in \mathcal{D}$, $|s - 1| \gg 1$ y $|z| \leq A$. Notemos ahora que de forma general

$$(1 + \log^+ |t|)^A \ll_A (1 + |t|)^{\delta/2}$$

siempre que $\delta/2 > 0$, lo cual se tiene en nuestro caso ya que $0 < \delta \leq 1$. Concluimos que

$$M(1 + \log^+ |t|)^A (1 + |t|)^{1-\delta/2} \ll_A M(1 + |t|)^{1-\delta/2}, \tag{3.6}$$

es decir,

$$F(s) \ll_A M(1 + |t|)^{1-\delta/2}$$

uniformemente para $s \in \mathcal{D}$, $|s - 1| \gg 1$, $|z| \leq A$.

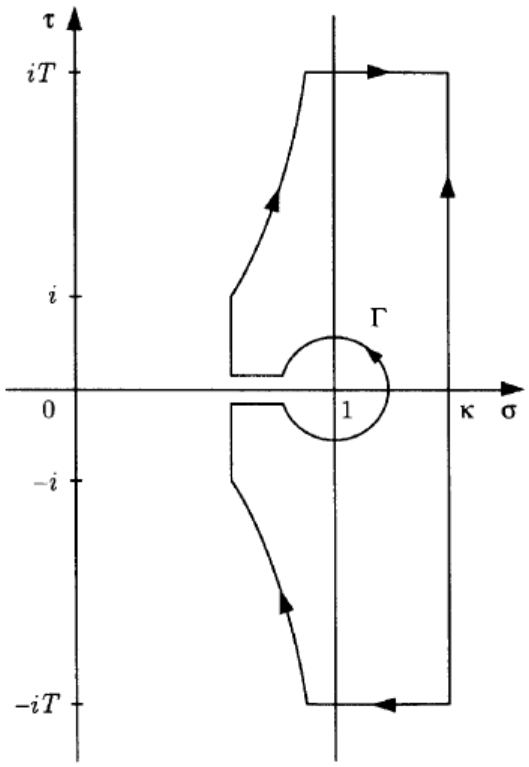
Denotemos por $A(x)$ la suma parcial que deseamos estimar:

$$A(x) = \sum_{n \leq x} a_n. \tag{3.7}$$

Utilizando la fórmula de Perron (Teo. 3 Capítulo II.2, [3]) podemos escribir,

$$\int_0^x A(x)dx = \frac{1}{2\pi i} \int_{\kappa - i\infty}^{\kappa + i\infty} F(s) x^{s+1} \frac{ds}{s(s+1)}$$

con $\kappa = 1 + 1/\log x$. Deformaremos el intervalo $[\kappa - iT, \kappa + iT]$ con $T > 1$ en un camino completamente contenido en $\mathcal{D}$. Para esto, consideremos la curva cerrada que se muestra en la siguiente figura.



Esta trayectoria es simétrica respecto al eje real y su parte superior está conformada por:

Γ: Contorno de Hankel truncado centrado en $s = 1$, con radio $r = \frac{1}{2\log x}$ y parte lineal uniendo $1 - r$ con $1 - \frac{c}{2}$.

Σ: La curva $\sigma(t)$ dada por

$$\sigma(t) = 1 - \frac{c}{2(1 + \log^+ t)}.$$

l: El segmento horizontal $[\sigma(T) + iT, \kappa + iT]$.

El valor de la integral sobre la curva que acabamos de definir es igual al valor de la integral sobre el segmento de recta original, ya que la curva cerrada formada por el segmento original y su deformación no contiene polos de la función que integraremos.

Estimemos ahora cada una de las secciones que forman el camino de integración. Iniciemos primero con las semirrectas $[\kappa \pm iT, \kappa \pm \infty]$. Haciendo el cambio de variable $s = \kappa + it$, tenemos

$$\frac{1}{2\pi i} \int_{\kappa+iT}^{\kappa+i\infty} F(s) x^{s+1} \frac{ds}{s(s+1)} ds = \frac{1}{2\pi} \int_T^{\infty} \frac{F(\kappa + it) x^{\kappa+1+it}}{(\kappa + it)(\kappa + 1 + it)} dt.$$

Entonces

$$\left|\frac{1}{2\pi i}\int_{\kappa+iT}^{\kappa+i\infty} F(s)x^{s+1}\frac{ds}{s(s+1)}\right| \leq \frac{1}{2\pi}\int_T^\infty \frac{|F(\kappa+it)||x^{\kappa+1+it}|}{|\kappa+it||\kappa+1+it|}|dt| \leq \frac{1}{2\pi}\int_T^\infty \frac{|F(\kappa+it)|x^{\kappa+1}}{t^2}dt$$
$$\ll_A Mx^2\int_T^\infty \frac{(1+t)^{1-\delta/2}}{t^2}dt \ll Mx^2\int_T^\infty t^{-1-\delta/2}dt$$
$$= \frac{Mx^2T^{-\delta/2}}{\delta} \ll_\delta Mx^2T^{-\delta/2}.$$

De forma análoga también tenemos que

$$\frac{1}{2\pi i}\int_{\kappa-iT}^{\kappa-i\infty} F(s)x^{s+1}\frac{ds}{s(s+1)} \ll_{A,\delta} Mx^2T^{-\delta/2}.$$

Estimemos ahora el valor de la integral sobre el intervalo $[\sigma(T)+iT, \kappa+iT]$. Haciendo el cambio de variable $s = r+iT$, tenemos

$$\left|\frac{1}{2\pi i}\int_{\sigma(T)+iT}^{\kappa+iT} F(s)x^{s+1}\frac{ds}{s(s+1)}\right| = \frac{1}{2\pi}\int_{\sigma(T)}^{\kappa}\left|\frac{F(r+iT)x^{r+1+iT}}{(r+iT)(r+1+iT)}\right||dr|$$
$$\leq \frac{x^{\kappa+1}}{2\pi}\int_{\sigma(T)}^{\kappa}\frac{|F(r+iT)|}{T^2}dr$$
$$\ll_A x^2\int_{\sigma(T)}^{\kappa}\frac{M(1+T)^{1-\delta/2}}{T^2}dr$$
$$\ll_\delta Mx^2T^{-\delta/2}.$$

Tenemos entonces el mismo comportamiento que la integral anterior. La curva Σ está definida por partes, estimaremos primero el segmento vertical de recta $[1-\frac{c}{2}, 1-\frac{c}{2}+i]$. Haciendo $s = 1-\frac{c}{2}+it$, tenemos

$$\left|\frac{1}{2\pi i}\int_{1-c/2}^{1-c/2+i} F(s)x^{s+1}\frac{ds}{s(s+1)}\right| \leq \frac{1}{2\pi}\int_0^1\left|\frac{F(1-c/2+it)x^{2-c/2+it}}{(1-c/2+it)(2-c/2+it)}\right||dt|$$
$$\leq \frac{x^{\sigma(T)+1}}{2\pi}\int_0^1 |F(1-c/2+it)|dt$$
$$\ll_A x^{\sigma(T)+1}\int_0^1 M(1+|t|)^{1-\delta/2}dt$$
$$\ll_\delta Mx^{\sigma(T)+1}.$$

Estimemos la parte faltante de la curva Σ, es decir, donde $1 \leq t \leq T$. Hagamos el cambio de variable natural

$$s = 1-\frac{c}{2(1+\log|t|)}+it,$$

de donde

$$ds = \frac{c}{2t(1+\log|t|)^2}+i.$$

Luego,

$$|ds|^2 = 1 + \frac{c^2}{4t^2(1+\log|t|)^2}.$$

Como $|\sigma(t)+1| \geq 1+t$, obtenemos que

$$\begin{aligned}\left|\frac{1}{2\pi i}\int_{\sigma(1)+i}^{\sigma(T)+iT} F(s)\frac{ds}{s(s+1)}\right| &\leq \frac{1}{2\pi}\int_1^T \left|\frac{F(\sigma(t)+it)x^{\sigma(t)+1}}{\sigma(t)(\sigma(t)+1)}\right| \left(1+\frac{c^2}{4t^2(1+\log|t|)^2}\right)^{1/2} dt \\ &\ll x^{\sigma(T)+1}\int_1^T \frac{|F(\sigma(t)+it)|}{(t+1)}\frac{1}{(1+t)}dt,\end{aligned}$$

ya que $t^2(1+\log t)^2 \gg (1+t)^2$. Continuando con los cálculos llegamos a que

$$\begin{aligned}\left|\frac{1}{2\pi i}\int_{\sigma(1)+i}^{\sigma(T)+iT} F(s)\frac{ds}{s(s+1)}\right| &\ll_A x^{\sigma(T)+1}\int_1^T M(1+t)^{-1-\delta/2}dt \\ &= \frac{2}{\delta}Mx^{\sigma(T)+1}\left(2^{-\delta/2}-(1+T)^{-\delta/2}\right) \\ &\ll_\delta Mx^{\sigma(T)+1}.\end{aligned}$$

Tomando $T = \exp(\sqrt{c/\delta\log x})$ de modo que $T > 1$, entonces

$$T^{-\delta/2} = \exp\left(-\frac{1}{2}\sqrt{c\delta\log x}\right).$$

Por lo que una de nuestras estimaciones es de la forma $x^2 M\exp(-\sqrt{c\delta\log x}/2)$ y la otra $Mx^{\sigma(T)+1}$, así que debemos estudiar el exponente $\sigma(T)+1$. Observemos

$$\sigma(T)+1 = 2 - \frac{c}{2(1+\log T)} = 2 - \frac{c}{2(1+\sqrt{c\delta^{-1}\log x})}.$$

Por otra parte, existe $K > 1$ constante positiva tal que

$$1+\sqrt{c\delta^{-1}\log x} \leq K\sqrt{c\delta^{-1}\log x} \qquad (x \geq 1+\varepsilon)$$

lo que implica que

$$-\frac{c}{2(1+\sqrt{c\delta^{-1}\log x})} \leq -\frac{c}{2K\sqrt{c\delta^{-1}\log x}} = -\frac{\sqrt{c\delta}}{2K\sqrt{\log x}}.$$

Entonces

$$x^{\sigma(T)+1} \leq x^2 x^{-\frac{\sqrt{c\delta}}{2K\sqrt{\log x}}}.$$

Tomando $x = e^{\log x}$ en el último factor, concluimos que

$$x^{\sigma(T)+1} \leq x^2\exp\left(-\frac{\sqrt{c\delta\log x}}{2K}\right).$$

Y como

$$-\frac{\sqrt{c\delta \log x}}{2} < -\frac{\sqrt{c\delta \log x}}{2K},$$

podemos elegir una sola estimación para así concluir

$$\int_0^x A(t)dt = \Phi(x) + O\left(Mx^2 e^{-c_3\sqrt{\log x}}\right) \tag{3.8}$$

donde $\Phi(x)$ es la función

$$\Phi(x) = \frac{1}{2\pi i}\int_\Gamma F(s)x^{s+1}\frac{ds}{s(s+1)}.$$

Como el integrando tiene derivadas parciales respecto a x continuas, podemos derivar para obtener que

$$\Phi'(x) = \frac{1}{2\pi i}\int_\Gamma \frac{F(s)x^s}{s}ds \qquad \text{y} \qquad \Phi''(x) = \frac{1}{2\pi i}\int_\Gamma F(s)x^{s-1}ds.$$

De aquí en adelante hacemos la convención de que todas las constantes implícitas o explícitas dependen de a los más c_0, δ y A.

Para $s \in \mathcal{D}$ tenemos

$$F(s) = sG(s;z)Z(s;z)(s-1)^{-z}, \tag{3.9}$$

y utilizando el Teorema 3.2, para $s \in \Gamma$

$$|F(s)| = |G(s;z)||s(s-1)^{-z}Z(s;z)| \ll M|s-1|^{-\operatorname{Re} z}\left|\sum_{j=0}^{\infty}\frac{\gamma_j(z)}{j!}(s-1)^j\right|.$$

Luego, existe $\varepsilon > 0$ tal que $|(1+\varepsilon)(s-1)| < 1$, y entonces

$$\left|\sum_{j=0}^{\infty}\frac{\gamma_j(z)}{j!}(s-1)^j\right| \le \sum_{j=0}^{\infty}|(1+\varepsilon)(s-1)|^j < \infty,$$

de donde

$$|F(s)| \ll M|s-1|^{-A}. \qquad (s \in \Gamma)$$

Por otra parte,

$$|\Phi''(x)| = \frac{1}{2\pi}\int_\Gamma |F(s)x^{s-1}||ds| \le \frac{1}{2\pi}\int_\Gamma |F(s)|x^r|ds| = \frac{e^{1/2}}{2\pi}\int_\Gamma |F(s)||ds| \ll M|s-1|^{-A},$$

y por lo tanto

$$\Phi''(x) \ll M|s-1|^{-A} \le Mr^{-A} \ll M(\log x)^A.$$

Además, para $s \in \Gamma$ tenemos que

$$\begin{aligned} G(s;z)Z(s;z) &= \left(\sum_{h=0}^{\infty} \frac{1}{h!} G^{(h)}(1;z)(s-1)^h\right)\left(\sum_{j=0}^{\infty} \frac{1}{j!}\gamma_j(z)(s-1)^j\right) \\ &= \sum_{k=0}^{\infty}\left(\sum_{h+j=k} \frac{1}{j!h!} G^{(h)}(1;z)\gamma_j(z)\right)(s-1)^k \\ &= \sum_{k=0}^{\infty}\frac{1}{k!}\left(\sum_{h+j=k} \frac{k!}{j!h!} G^{(h)}(1;z)\gamma_j(z)\right)(s-1)^k \\ &= \sum_{k=0}^{\infty}\frac{1}{k!}\left(\sum_{h+j=k} \binom{k}{j} G^{(h)}(1;z)\gamma_j(z)\right)(1-s)^k, \end{aligned}$$

es decir,

$$G(s;z)Z(s;z) = \sum_{k=0}^{\infty} g_k(z)(s-1)^k, \qquad g_k(z) := \frac{1}{k!}\sum_{h+j=k}\binom{k}{j} G^{(h)}(1;z)\gamma_j(z).$$

Por la definición previa al teorema, $g_k(z)$ cumple que

$$g_k(z) = \Gamma(z-k)\lambda_k(z).$$

Además, $G(s;z)Z(s;z)$ es holomorfa y $O(M)$ en el disco cerrado $|s-1| \leq c$ y como consecuencia de las fórmulas de Cauchy tenemos que

$$g_k(z) \ll Mc^{-k}.$$

Observemos que Γ está acotada en el disco $|s-1| \leq c/2$, así que para $s \in \Gamma$,

$$\begin{aligned} G(s;z)Z(s;z) &= \sum_{k=0}^{\infty} g_k(z)(s-1)^k = \sum_{k=0}^{N} g_k(z)(s-1)^k + \sum_{k=N+1}^{\infty} g_k(z)(s-1)^k \\ &= \sum_{k=0}^{N} g_k(z)(s-1)^k + O\left(\sum_{k=N+1}^{\infty} Mc^{-k}|s-1|^k\right) \\ &= \sum_{k=0}^{N} g_k(z)(s-1)^k + O\left(\frac{M|s-1|^{N+1}}{c^{N+1}}\right). \end{aligned}$$

Luego, de la ecuación (3.9) tenemos

$$\begin{aligned} \Phi'(x) &= \frac{1}{2\pi i}\int_{\Gamma} \frac{F(s)x^s ds}{s} = \frac{1}{2\pi i}\int_{\Gamma}\sum_{k=0}^{N} g_k(z)(s-1)^{k-z} + O\left(\frac{1}{2\pi i}\int_{\Gamma}\frac{M|s-1|^{N+1-\operatorname{Re} z}|x^s|}{C^{N+1}}|ds|\right) \\ &= \sum_{k=0}^{N}\frac{g_k(z)}{2\pi i}\int_{\Gamma}(s-1)^{k-z}x^s ds + O\left(Mc^{-N}\int_{\Gamma}|x^s||s-1|^{N+1-\operatorname{Re} z}|ds|\right). \end{aligned}$$

Refinando el último término,

$$\begin{aligned}\int_\Gamma |x^s||s-1|^{N+1-\operatorname{Re} z}|ds| &= \int_{1-c/2}^{1-r} x^\sigma (1-\sigma)^{N+1-\operatorname{Re} z} d\sigma + \int_{|s-1|=r} x^\sigma r^{N+1-\operatorname{Re} z}|ds| \\ &\ll \int_{1-c/2}^{1-r} x^\sigma (1-\sigma)^{N+1-\operatorname{Re} z} d\sigma + 2^{\operatorname{Re} z - N-2} x^{r+1} (\log x) r^{N+2-\operatorname{Re} z}.\end{aligned}$$

Con el cambio de variable

$$\sigma(t) = (1-r) + (r-c/2)e^{1/2-t}$$

se sigue que

$$\int_{1-c/2}^{1-r} x^\sigma (1-\sigma)^{N+1-\operatorname{Re} z} d\sigma = \int_{1/2}^{\infty} x^{1-r} x^{(r-c/2)e^{1/2-t}} (r+(c/2-r)e^{1/2-t})^{N+1-\operatorname{Re} z} (c/2-r) e^{1/2-t} dt. \tag{3.10}$$

Notemos que $x^{-r} = e^{-1/2}$, $x^{(r-c/2)e^{1/2-t}} < 1$, $r + (c/2-r)e^{1/2-t} \ll tr$ y que

$$\left| \left(\frac{c}{2} - r \right) e^{1/2-t} \right| = O\left(\left| r - \frac{c}{2} \right| e^{-t} \right) = O\left(re^{-t} \right).$$

Utilizando las observaciones anteriores en (3.10) se tiene que

$$\int_{1-c/2}^{1-r} x^\sigma (1-\sigma)^{N+1-\operatorname{Re} z} \ll x(\log x)^{\operatorname{Re} z - N-2} \int_{1/2}^{\infty} t^{N+1-\operatorname{Re} z} e^{-t} 2^{\operatorname{Re} z - N-2} dt,$$

por lo que

$$\int_\Gamma |x^s||s-1|^{N+1-\operatorname{Re} z}|ds| \ll x(\log x)^{\operatorname{Re} z - N-1} \left(\int_{1/2}^{\infty} t^{N+1-\operatorname{Re} z} e^{-t} dt + 1 \right).$$

Ahora, notemos que

$$\int_1^\infty t^{N+1-\operatorname{Re} z} e^{-t} dt \le \int_1^\infty t^{N+1+A} e^{-t} dt$$

y observemos que para t con $1/2 \le t \le 1$,

$$t^{N+1-\operatorname{Re} z} \le t^{N+1-A} = t^{N+1+A} t^{-2A} \le t^{N+1+A} 2^{2A},$$

lo que implica

$$\int_{1/2}^1 t^{N+1-\operatorname{Re} z} e^{-t} dt \le 2^{2A} \int_{1/2}^1 t^{N+1+A} e^{-t} dt.$$

Luego,

$$\int_{1/2}^\infty t^{N+1-\operatorname{Re} z} e^{-t} dt \le 2^{2A} \int_{1/2}^\infty t^{N+1+A} e^{-t} dt \le 2^{2A} \int_0^\infty t^{N+1+A} e^{-t} dt = 2^{2A} \Gamma(N+2+A),$$

de donde se concluye que

$$\int_\Gamma |x^s||s-1|^{N+1-\operatorname{Re} z}|ds| \ll x(\log x)^{\operatorname{Re} z-N-2}\Gamma(N+A+2) \ll x(\log x)^{z-1}\left(\frac{c_4N+1}{\log x}\right)^{N+1}.$$

La última estimación se debe a que

$$\Gamma(N+A+2) \leq (N+\lceil A\rceil+1)! \leq (N+\lceil A\rceil+1)^{N+\lceil A\rceil+1},$$

donde $\lceil A\rceil$ denota el menor entero mayor o igual que A. Al tomar c_4 tal que

$$c_4 > \frac{(N+\lceil A\rceil+1)^{\frac{N+\lceil A\rceil+1}{N+1}}-1}{N},$$

se tiene el resultado.

Con lo visto hasta este momento, tenemos para $\Phi'(x)$,

$$\Phi'(x) = \sum_{k=0}^{N} g_k(z)\frac{1}{2\pi i}\int_\Gamma (s-1)^{k-z}x^s ds + O\left(Mc^{-N}x(\log x)^{z-1}\left(\frac{c_4N+1}{\log x}\right)^{N+1}\right) \quad (3.11)$$

Para la integral $\int_\Gamma (s-1)^{k-z}x^s ds$, nos será útil el corolario a la fórmula de Hankel. Usando el cambio de variable $w=(s-1)\log x$, tenemos

$$\begin{aligned}
\frac{1}{2\pi i}\int_\Gamma x^s(s-1)^{k-z}ds &= \frac{1}{2\pi i}\int_{\mathcal{H}(\frac{c}{2}\log x)} x\cdot x^{w/\log x}\frac{w^{k-z}}{(\log x)^{k-z}}\frac{dw}{\log x}\\
&= x(\log x)^{z-1-k}\frac{1}{2\pi i}\int_{\mathcal{H}(\frac{c}{2}\log x)} e^w w^{k-z}dw\\
&= x(\log x)^{z-1-k}\left(\frac{1}{\Gamma(z-k)}+O\left(47^{|z-k|}\Gamma(1+z-k)x^{-c/4}\right)\right)\\
&= x(\log x)^{z-1-k}\left(\frac{1}{\Gamma(z-k)}+O\left(47^{k}\Gamma(1+k+A)x^{-c/4}\right)\right)\\
&= x(\log x)^{z-1-k}\left(\frac{1}{\Gamma(z-k)}+O\left((c_5k+1)^k x^{-c/4}\right)\right).
\end{aligned}$$

Entonces,

$$\sum_{k=1}^{N} g_k(z)\frac{1}{2\pi i}\int_\Gamma x^s(s-1)^{k-z}ds = \sum_{k=0}^{N} g_k(z)\left(x(\log x)^{z-1-k}\left\{\frac{1}{\Gamma(z-k)}+O\left((c_5k+1)^k x^{-c/4}\right)\right\}\right)$$

$$\begin{aligned}
&= x(x\log x)^{z-1}\left\{\sum_{k=0}^{N}\frac{g_k(z)}{\Gamma(z-k)}\frac{1}{(\log x)^k}+O\left(x^{-c/4}\sum_{k=0}^{N}|g_k(z)|\left(\frac{c_5k+1}{\log x}\right)^k\right)\right\}\\
&= x(\log x)^{z-1}\left\{\sum_{k=0}^{N}\frac{\lambda_k(z)}{(\log x)^k}+O\left(x^{-c/4}\sum_{k=0}^{N}|g_k(z)|\left(\frac{c_5k+1}{\log x}\right)^k\right)\right\}.
\end{aligned}$$

Trabajaremos ahora el término de error. Definimos por

$$E_N := \sum_{k=0}^{N} |g_k(z)| \left(\frac{c_5 k+1}{\log x}\right)^k \ll x^{-c/4} M \sum_{k=0}^{N} c^{-k} \left(\frac{c_5 k+1}{\log x}\right)^k,$$

y notamos ahora que

$$(c_5 k+1)^k = \sum_{j=0}^{k} \binom{k}{j} c_5^j k^j \leq k! c_6^N \left(\frac{1}{0!k!} + \frac{k}{1!(k-1)!} + \cdots \frac{k^k}{k!0!}\right),$$

donde $c_6 = \max\{c_5, c_5^{-1}\}$. Por otro lado,

$$5^k = e^{k \log 5} \geq 1 + k \log 5 + \frac{k^2 (\log 5)^2}{2!} + \cdots + \frac{k^k (\log 5)^k}{k!}.$$

Como $(\log 5)^j \geq 1/(k-j)!$ para $j \leq k$, tenemos

$$\begin{aligned}(c_5 k+1)^k &\leq k! c_6^N \left(1 + k \log 5 + \frac{k^2 (\log 5)^2}{2!} + \cdots + \frac{k^k (\log 5)^k}{k!}\right) \\ &\leq k! c_6^N 5^k.\end{aligned}$$

Por lo tanto

$$\begin{aligned}E_N &\ll c_6^N M x^{-c/4} \sum_{k=0}^{N} k! \left(\frac{5}{c \log x}\right)^k = M x^{-c/4} c_6^N \left(\frac{5}{c \log x}\right)^N \sum_{k=0}^{N} k! \left(\frac{c \log x}{5}\right)^{N-k} \\ &\leq M x^{-c/4} \left(\frac{5 c_6}{c \log x}\right)^N \sum_{k=0}^{N} \frac{N!}{(N-k)!} \left(\frac{c \log x}{5}\right)^{N-k} \\ &= M x^{-c/4} N! \left(\frac{5 c_6}{c \log x}\right)^N \sum_{k=0}^{N} \frac{(\log x^{c/5})^{N-k}}{(N-k)!} \\ &\leq M x^{-c/4} N! \left(\frac{5 c_6}{c \log x}\right)^N x^{c/5} = M x^{-c/20} N! \left(\frac{5 c_6}{c \log x}\right)^N.\end{aligned}$$

Veamos ahora que se satisface

$$x^{-c/20} N! \left(\frac{5 c_6}{c \log x}\right)^N \ll \left(\frac{c_7 N+1}{\log x}\right)^{N+1}.$$

Para ello, es claro que

$$N! \left(\frac{5 c_6}{c \log x}\right)^N \leq \left(\frac{5 c_6 N}{c \log x}\right)^N,$$

tomando $c_7 = 5c_6/\varepsilon c_0$, con ε tal que $\varepsilon c_0 < c$, se tiene

$$x^{-c/20}\left(\frac{5c_6N}{c\log x}\right)^N \leq x^{-c/20}\left(\frac{c_7N+1}{\log x}\right)^N \ll \left(\frac{c_7N+1}{\log x}\right)^{N+1},$$

ya que $x^{-c/20} \ll 1/\log x$. Podemos concluir entonces que

$$E_N \ll M\left(\frac{c_7N+1}{\log x}\right)^{N+1}.$$

Por lo tanto,

$$\Phi'(x) = x(\log x)^{z-1}\left\{\sum_{k=0}^{N}\frac{\lambda_k(z)}{(\log x)^k} + O\left(M\left(\frac{c_8N+1}{\log x}\right)^{N+1}\right)\right\}. \tag{3.12}$$

Usando (3.8) y que $\Phi''(x) \ll M(\log x)^A$, veremos que $\Phi'(x)$ es una buena aproximación para $A(x)$. Tomando el parámetro h, $0 < h < x/2$ y aplicándolo en (3.8) a x y $x+h$, tenemos

$$\begin{aligned}\int_x^{x+h} A(t)dt &= \int_0^{x+h} A(t)dt - \int_0^x A(t)dt \\ &= \Phi(x+h) + O\left(M(x+h)^2e^{-c_3\sqrt{\log(x+h)}}\right) - \Phi(x) + O\left(Mx^2e^{-c_3\sqrt{\log x}}\right) \\ &= \Phi(x+h) - \Phi(x) + O\left(Mx^2e^{-c_3\sqrt{\log x}}\right).\end{aligned}$$

Consideremos la siguiente igualdad obtenida mediante integración por partes:

$$\int_0^1 (1-t)\Phi''(x+th)dt = -\frac{1}{h}\Phi'(x) + \frac{\Phi(x+h)-\Phi(x)}{h^2}.$$

Despejando la diferencia $\Phi(x+h) - \Phi(x)$ obtenemos que

$$\begin{aligned}\Phi(x+h) - \Phi(x) &= h\Phi'(x) + h^2\int_0^1 (1-t)\Phi''(x)(x+th)dt \\ &\ll h\Phi'(x) + h^2\int_0^1 M(1-t)(\log(x+th))^A dt \\ &\ll h\Phi'(x) + h^2M(\log(3x/2))^A \\ &= h\Phi'(x) + h^2M(\log(3/2)+\log x)^A \\ &\ll h\Phi'(x) + h^2M(\log x)^A.\end{aligned}$$

Entonces

$$\int_x^{x+h} A(t)dt = h\Phi'(x) + O\left(Mh^2(\log x)^A + Mx^2e^{-c_3\sqrt{\log x}}\right).$$

Por otro lado,

$$\frac{1}{h}\int_x^{x+h} A(t)dt = \frac{1}{h}\int_x^{x+h}(A(t)-A(x))dt + A(x),$$

y despejando $A(x)$ obtenemos,

$$A(x) = \frac{1}{h}\int_x^{x+h} A(t)dt - \frac{1}{h}\int_x^{x+h}(A(t)-A(x))dt.$$

Es decir,

$$A(x) = \Phi'(x) + O\left(Mh(\log x)^A + Mx^2h^{-1}e^{-c_3\sqrt{\log x}} + h^{-1}L\right), \tag{3.13}$$

donde

$$L := \int_x^{x+h} |A(t)-A(x)|dt.$$

Ahora, como $F(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ es del tipo $\mathcal{T}(z,w;c_0,\delta,M)$, existe una sucesión de números reales positivos $(b_n)_{n=1}^{\infty}$ tal que $|a_n| \leq b_n$ para toda $n \in \mathbb{N}$ y la serie $\sum_{n=1}^{\infty} b_n n^{-s}$ tiene la propiedad $\mathcal{P}(w;c_0,\delta,M)$. Definimos para cada $t \geq 1$ la función $B(t)$ por $B(t) := \sum_{n\leq t} b_n$. Entonces,

$$L \leq \int_x^{x+h}(B(t)-B(x))dt \leq \int_x^{x+h} B(t)dt - \int_{x-h}^{x} B(t)dt.$$

La primera desigualdad se debe a que

$$|A(t)-A(x)| \leq \sum_{x<n\leq t} |a_n| \leq \sum_{x<n\leq t} b_n = B(t)-B(x).$$

Por nuestras hipótesis, existe una función infinitamente diferenciable $\Phi_1(x)$ que satisface

$$\Phi_1(x+h) - \Phi_1(x) = h\Phi_1'(x) + O\left(Mh^2(\log x)^A\right).$$

Por un procedimiento análogo llegamos a que

$$\Phi_1(x) - \Phi_1(x-h) = h\Phi_1'(x) + O\left(Mh^2(\log x)^A\right),$$

de modo que

$$\begin{aligned}\int_x^{x+h} B(t)dt &= \Phi_1(x+h) - \Phi_1(x) + O(Mx^2e^{-c_9\sqrt{\log x}}) \\ &= h\Phi_1'(x) + O\left(Mx^2e^{-c_9\sqrt{\log x}} + Mh^2(\log x)^A\right),\end{aligned}$$

y también

$$\int_{x-h}^{x} B(t)dt = h\Phi_1'(x) + O\left(Mx^2 e^{-c_9\sqrt{\log x}} + Mh^2(\log x)^A\right).$$

Concluimos que L satisface

$$L = O\left(Mx^2 e^{-c_9\sqrt{\log x}} + Mh^2(\log x)^A\right).$$

En otras palabras, salvo una modificación de la constante c_3, podemos suprimir el término $h^{-1}L$ en la ecuación (3.13), es decir,

$$A(x) = \Phi'(x) + O\left(Mx^2 h^{-1} e^{-c_3\sqrt{\log x}} + Mh(\log x)^A\right).$$

Eligiendo

$$h = xe^{-\frac{c_3}{2}\sqrt{\log x}},$$

tenemos

$$\begin{aligned} A(x) &= \Phi'(x) + O\left(Mxe^{-\frac{c_3}{2}\sqrt{\log x}} + Mxe^{-\frac{c_3}{2}\sqrt{\log x}}(\log x)^A\right) \\ &= \Phi'(x) + O\left(Mxe^{-\frac{c_3}{2}\sqrt{\log x}}\left(1 + (\log x)^A\right)\right). \end{aligned}$$

Haciendo el cambio de variable $x = e^{u^2}$, es claro que

$$e^{-\frac{c_3}{2}\sqrt{\log x}}\left(1 + (\log x)^A\right)) = e^{-c_3 u/2}(1 + u^{2A}) = O\left(e^{-c_{10}u}\right) = O\left(e^{-c_{10}\sqrt{\log x}}\right),$$

por lo que tenemos

$$A(x) = \Phi'(x) + O(Mxe^{-c_{10}\sqrt{\log x}}).$$

Combinando lo anterior con (3.12), se sigue que

$$A(x) = x(\log x)^{z-1}\left\{\sum_{k=0}^{N}\frac{\lambda_k(z)}{(\log x)^k} + O\left(M\left(\frac{c_8 N+1}{\log x}\right)^{N+1}\right)\right\} + O\left(Mxe^{-c_{10}\sqrt{\log x}}\right). \tag{3.14}$$

Como

$$e^{-c_{10}\sqrt{\log x}} = O\left((\log x)^{z-1}e^{-c_{11}\sqrt{\log x}}\right),$$

concluimos que

$$A(x) = x(\log x)^{z-1}\left\{\sum_{k=0}^{N}\frac{\lambda_k(z)}{(\log x)^k} + O\left(MR_N(x)\right)\right\},$$

con

$$R_N(x) = e^{-c_{11}\sqrt{\log x}} + \left(\frac{c_8 N+1}{\log x}\right)^{N+1}.$$

□

Corolario 3.8. *Sea $F(s) = \sum a_n n^{-s}$ una serie de Dirichlet con $a_n \geq 0$ para toda $n \in \mathbb{N}$ y que además existen $z \in \mathbb{C}$, $c_0 > 0$, $0 < \delta \leq 1$ y $M > 0$ tales que la función*

$$G(s) = F(s)\zeta(s)^{-z}$$

tiene una continuación holomorfa en el dominio $\mathcal{D}$ del plano complejo, definido por la desigualdad

$$\sigma \geq 1 - \frac{c_0}{1 + \log(1 + |t|)},$$

y satisface

$$|G(s)| \leq M(1 + |t|)^{1-\delta}$$

para toda $s \in \mathcal{D}$. Entonces existe una sucesión (λ_k) tal que para toda $N \geq 0$ se tiene la siguiente igualdad uniformemente para $x \geq 2$

$$\sum_{1 \leq n \leq x} a_n = x(\log x)^{z-1} \left\{ \sum_{0 \leq k \leq N} \frac{\lambda_k}{(\log x)^k} + O\left(\frac{1}{(\log x)^{N+1}} \right) \right\}.$$

En particular tenemos que

$$\lambda_0 = \frac{1}{\Gamma(z)} G(1).$$

Demostración. De acuerdo a las hipótesis, no es difícil ver que la serie de Dirichlet $F(s)$ es del tipo $\mathcal{T}(z, z; c_0, \delta, M)$. Por el método de Selberg-Delange vemos que existe una sucesión $(\lambda_k(z))$ que satisface la ecuación

$$\sum_{n \leq x} a_n = x(\log x)^{z-1} \left\{ \sum_{k=0}^{N} \frac{\lambda_k(z)}{(\log x)^k} + O(MR_N(x)) \right\},$$

con

$$R_N(x) := e^{-c_1\sqrt{\log x}} + \left(\frac{c_2 N + 1}{\log x} \right)^{N+1},$$

para toda $N \geq 0$ uniformemente para $x \geq 2$, por lo que el resultado se sigue al fijar z en $(\lambda_k(z))$ y al probar que

$$R_N(x) \ll \frac{1}{(\log x)^{N+1}}.$$

Lo cual es trivial debido a que

$$\lim_{x \to \infty} (\log x)^{N+1} R_N(x) = \lim_{x \to \infty} (\log x)^{N+1} e^{-c_1\sqrt{\log x}} < \infty.$$

□

Capítulo 4

Resultados

En la primera sección obtendremos una cota para las soluciones a $\Phi_n(x, y) = m$, la prueba es sencilla y únicamente utilizaremos la teoría del Capítulo 1. En la segunda sección estudiaremos el comportamiento asintótico de la cantidad de enteros representables por formas binarias ciclotómicas, para ello tendremos que presentar algunos resultados preliminares sobre series de Dirichlet y la función gamma. Finalmente, la última sección trata sobre la sucesión (a_m) dada por la cantidad de representaciones que el entero m tiene, donde entendemos por una representación de m a una terna (n, x, y) que satisface $\Phi_n(x, y) = m$.

4.1. Mejora a la cota para las soluciones de la ecuación $\Phi_n(x, y) = m$

Para $m \in \mathbb{N}$, estudiaremos las soluciones enteras a la ecuación

$$\Phi_n(x, y) = m \tag{4.1}$$

para $n \geq 3$, ya que las formas binarias ciclotómicas $\Phi_1(x, y) = x - y$ y $\Phi_2(x, y) = x + y$ son lineales, por lo que las soluciones de (4.1) son "triviales". Kálmán Győry en [2] da la cota para las soluciones a la ecuación $\Phi_n(x, y) = m$ dada por:

$$\text{máx}\{|x|, |y|\} \leq 2|m|^{\frac{1}{\varphi(n)}}. \tag{4.2}$$

El siguiente resultado es una mejora a esta estimación, ya que obtenemos una cota menor a la que se muestra en (4.2) y además acotaremos el valor de n.

Teorema 4.1. *Sea m un número natural y sean n, x, y enteros que satisfacen $n \geq 3$,* $\max\{|x|, |y|\} \geq 2$ *y* $\Phi_n(x, y) = m$. *Entonces*

$$\varphi(n) \leq \frac{2}{\log 3} \log m \qquad y \qquad \max\{|x|, |y|\} \leq \frac{2}{\sqrt{3}} m^{\frac{1}{\varphi(n)}}.$$

Demostración. Supongamos que $m = \Phi_n(x, y)$, $n \geq 3$ y $\max\{|x|, |y|\} \geq 2$. Recordemos que $\Phi_n(x, y) = y^{\varphi(n)} \phi_n(x/y)$. Utilizando el Corolario 1.14 con $\gamma = c_n$, se tiene que

$$\Phi_n(x, y) = m \geq c_n \max\{|x|^{\varphi(n)}, |y|^{\varphi(n)}\} = c_n \max\{|x|, |y|\}^{\varphi(n)}.$$

Usando ahora la Proposición 1.17 se sigue que

$$m \geq c_n \max\{|x|, |y|\}^{\varphi(n)} \geq \left(\frac{\sqrt{3}}{2} \max\{|x|, |y|\} \right)^{\varphi(n)}.$$

Despejando $\max\{|x|, |y|\}$, obtenemos

$$\max\{|x|, |y|\} \leq \frac{2}{\sqrt{3}} m^{1/\varphi(n)}.$$

Como $\max\{|x|, |y|\} \geq 2$, tenemos

$$m \geq \left(\frac{\sqrt{3}}{2} \max\{|x|, |y|\} \right)^{\varphi(n)} \geq \sqrt{3}^{\varphi(n)} = 3^{\varphi(n)/2}.$$

Luego,

$$\varphi(n) \leq \frac{2}{\log 3} \log m.$$

□

Usando la cota inferior para $\varphi(n)$ obtenida de [6] y dada por

$$\varphi(n) > \left(\frac{n}{2.685} \right)^{1/1.161}$$

junto con el teorema anterior, podemos ver que si m es representable por una forma binaria ciclotómica entonces

$$\left(\frac{n}{2.685} \right)^{1/1.161} < \frac{2}{\log 3} \log m.$$

Podemos despejar n para obtener la cota superior,

$$n < 5.383 (\log m)^{1.161}. \tag{4.3}$$

La cota para las soluciones dada en este teorema es óptima, ya que para $n=3$ y $l\in\mathbb{N}$, tomando $x=l$, $y=-2l$ obtenemos

$$\Phi_3(l,-2l)=3l^2,$$

y de acuerdo con el Teorema 4.1 tenemos que

$$\text{máx}\{|l|,|-2l|\}=2l=\frac{2}{\sqrt{3}}\left(3l^2\right)^{\frac{1}{\varphi(3)}}.$$

Diremos que la terna (n,x,y) es una *representación* de m si satisface que $\Phi_n(x,y)=m$. Este primer resultado nos muestra que el conjunto de representaciones de m dado por

$$\mathcal{S}_m:=\{(n,x,y)\in\mathbb{Z}^3\,|\,n\geq 3,\ m=\Phi_n(x,y),\ \text{máx}\{|x|,|y|\}\geq 2\}$$

es finito.

Corolario 4.2. *Si $d>2$, entonces el número de ternas (n,x,y) con $\varphi(n)\geq d$, $\text{máx}\{|x|,|y|\}\geq 2$ y $\Phi_n(x,y)<N$ está acotado por $CN^{2/d}$, donde la constante C depende de d.*

Demostración. Del teorema 4.1 deducimos que

$$\text{máx}\{|x|,|y|\}\leq\frac{2}{\sqrt{3}}m^{1/\varphi(n)}\leq\frac{2}{\sqrt{3}}m^{1/d}<\frac{2}{\sqrt{3}}N^{1/d},\tag{4.4}$$

de modo que para cada n con $\varphi(n)\geq d$ podemos acotar la cantidad de parejas solución (x,y) por $(16/3)N^{2/d}$. Como el conjunto $\{n_1,n_2,...,n_k\}$ que satisface $\varphi(n_j)=d$, $j=1,...,k$, es finito y depende de d, tenemos que la cantidad de ternas con $\varphi(n)=d$ está acotada por

$$k\frac{16}{3}N^{2/d}.$$

Para las n's restantes, es decir aquellas con $\varphi(n)\geq d+1$, podemos utilizar de nuevo (4.4) pero esta vez acotando con

$$\frac{2}{\sqrt{3}}N^{\frac{1}{d+1}}.$$

Lo anterior junto con la desigualdad (4.3) implican que la cantidad de ternas (n,x,y) con $\varphi(n)\geq d+1$ está acotada por

$$29(\log N)^{1.161}N^{\frac{2}{d+1}}.$$

Luego,

$$(\log N)^{1.161}N^{\frac{2}{d+1}}=(\log N)^{1.161}N^{\frac{2}{d+1}-\frac{2}{d}}N^{\frac{2}{d}}\leq MN^{\frac{2}{d}},$$

debido a que el factor

$$N^{\frac{2}{d+1}-\frac{2}{d}}$$

es una potencia negativa de N. Combinando las cotas para las ternas (n, x, y) con $\varphi(n) = d$ y $\varphi(n) \geq d+1$ obtenemos que la cantidad de ternas total está acotada por

$$\left(k\frac{16}{3} + M\right) N^{2/d}.$$

□

4.2. Comportamiento asintótico de la cantidad de enteros representables

Sea $\mathcal{A}(\Phi_n; N)$ el conjunto definido por

$$\mathcal{A}(\Phi_n; N) := \{m \in \mathbb{N} \,|\, m \leq N, m = \Phi_n(x, y), \text{ para algún } (x, y), \text{máx}\{|x|, |y|\} \geq 2\},$$

y consideremos la unión

$$\mathcal{A}(\Phi_{\{n\geq 3\}}; N) := \bigcup_{n\geq 3} \mathcal{A}(\Phi_n; N).$$

Este conjunto contiene a todos los elementos $m \leq N$ representables por cualquier forma binaria $\Phi_n(x, y)$ con $n \geq 3$. Nos interesa el comportamiento asintótico de la cardinalidad de $\mathcal{A}(\Phi_{\{n\geq 3\}}; N)$ y para ello haremos uso de el método de Selberg-Delange. Necesitaremos algunos resultados relacionados con series de Dirichlet, por lo que en esta sección demostraremos algunas propiedades de estas funciones.

El lema siguiente aunque no es una estimación muy buena para L-funciones nos será necesario porque nos permitirá utilizar el principio de convexidad de Phragmen-Lindelöf. Utilizaremos la notación usual $s = \sigma + it$ para denotar al número complejo s, usaremos χ para denotar a un caracter de Dirichlet, $L(s, \chi)$ denotará la serie de Dirichlet asociada al caracter χ y como es usual χ_0 denotará a un caracter principal.

Lema 4.3. *Sea χ un caracter primitivo módulo q, tal que $\chi \neq \chi_0$. Entonces, en regiones de la forma $a \leq \sigma \leq b$ tenemos*

$$L(s,\chi) \ll e^{|s|^A}$$

con $A > 1$.

Demostración. Obsérvese que como $\chi \neq \chi_0$, entonces $\chi^{-1} \neq \chi_0$, lo que implica que χ^{-1} tiene como abscisa de convergencia $\sigma_c = 0$, por el Teorema B.6 tenemos que para $0 < \varepsilon < \delta < 1$

$$L(1-s,\chi^{-1}) \ll (|t|+4)^{1-\delta+\varepsilon} \leq |t|+4 \tag{4.5}$$

uniformemente en $1-\sigma \geq \delta > 0$.

Por la ecuacion funcional para L-funciones, tenemos que para todo $s \in \mathbb{C}$

$$L(s,\chi) = \frac{G(\chi)}{i^\kappa \sqrt{q}} L(1-s,\chi^{-1}) 2^s \pi^{s-1} q^{\frac{1}{2}-s} \Gamma(1-s) \operatorname{sen} \frac{\pi}{2}(s+\kappa),$$

donde $\kappa = 0$ si χ es par, $\kappa = 1$ si es impar y $G(\chi)$ es la suma de Gauss de χ. De aquí que en módulo

$$|L(s,\chi)| = |L(1-s,\chi^{-1})| 2^\sigma \pi^{\sigma-1} q^{\frac{1}{2}-\sigma} |\Gamma(1-s)| |\operatorname{sen} \frac{\pi}{2}(s+\kappa)|.$$

La ecuación (4.5) implica que para $\sigma \leq 1-\delta < 1$,

$$|L(s,\chi)| \ll (|t|+4) q^{\frac{1}{2}-\sigma} |\Gamma(1-s)| |\operatorname{sen} \frac{\pi}{2}(s+\kappa)|.$$

Usando simplemente la definición de la función seno, vemos que

$$|\operatorname{sen} \frac{\pi}{2}(s+\kappa)| \leq \frac{e^{-\pi t/2} + e^{\pi t/2}}{2} \leq e^{|t|\pi/2} \leq e^{|s|\pi}$$

Luego, la fórmula de Stirling nos da

$$\begin{aligned} |\Gamma(1-s)| &\ll |(1-s)^{(1-s)-1/2}| e^{\sigma-1} \\ &\leq |1-s|^{1/2-\sigma} e^{|t|\pi} \\ &\ll e^{|s|} e^{|s|\pi} \\ &= e^{|s|(1+\pi)}. \end{aligned}$$

Estas estimaciones implican que para s con $\sigma \leq 1-\delta < 1$,

$$|L(s,\chi)| \ll (|t|+4) q^{1/2-\sigma} e^{|s|(1+2\pi)}.$$

Pero por el Teorema B.6 aplicado a χ tenemos que $|L(s,\chi)| \ll |t|+4$ para $\sigma \geq \delta > 0$. Por lo que la estimación

$$|L(s,\chi)| \ll (|t|+4)q^{|\sigma|}e^{|s|(1+2\pi)}$$

es válida de forma general. De aquí que cuando $a \leq \sigma \leq b$, el factor $q^{|\sigma|}$ está acotado y por lo tanto

$$|L(s,\chi)| \ll e^{2(1+\pi)|s|} \ll e^{|s|^A},$$

con $A > 1$. □

Necesitaremos estimar L-funciones de Dirichlet asociadas a caracteres cuadráticos primitivos en la banda $0 \leq \sigma \leq 1$, para ello utilizaremos la ecuación funcional para este tipo de funciones dada por:

$$L(s,\chi) = L(1-s,\chi)2^s\pi^{s-1}q^{\frac{1}{2}-s}\Gamma(1-s)\operatorname{sen}\left(\frac{\pi}{2}(s+\kappa)\right) \tag{4.6}$$

donde χ es un caracter primitivo módulo q, $\kappa = 0$ si χ es par y $\kappa = 1$ si χ es impar. Como la función $\Gamma(s)$ aparece en (4.6), tendremos que probar un par de resultados que la involucran.

Proposición 4.4. *Sea $s = \sigma + it \in \mathbb{C}$ con σ fijo. Entonces,*

$$\Gamma(s) \ll |s|^{\sigma-\frac{1}{2}}e^{-\sigma}e^{-\frac{\pi}{2}|s|}.$$

Demostración. De acuerdo a la fórmula de Stirling dada por el Teorema C.1, vemos que para $|s|$ suficientemente grande en la banda $a \leq \sigma \leq b$ se satisface

$$|\Gamma(s)| \leq |s^s||s|^{-\frac{1}{2}}e^{-\sigma}.$$

Observemos que

$$|s^s| = \left|e^{(\sigma+it)\log s}\right| = |s|^\sigma e^{-t\cdot\arg s},$$

por lo que tendremos el resultado deseado si probamos que

$$e^{-t\arg s} \ll e^{-\frac{\pi}{2}|s|},$$

o equivalentemente que

$$\frac{\pi}{2}|s| - t\arg s = O(1). \tag{4.7}$$

Denotemos por θ al argumento de s. Aprovechando que $t = \sigma\tan\theta$ y que

$$|s| = \frac{\sigma}{\cos\theta},$$

obtenemos

$$\left|\frac{\pi}{2}|s| - t\theta\right| = \left|\frac{\pi}{2}\frac{\sigma}{\cos\theta} - \theta\sigma\tan\theta\right| = |\sigma|\left|\frac{1}{\cos\theta}\left(\frac{\pi}{2} - \theta\,\mathrm{sen}\,\theta\right)\right|. \tag{4.8}$$

Para probar (4.7) necesitamos demostrar que $\frac{\pi}{2}|s| - t\theta$ es acotado cuando $|s|$ tiende a infinito, por la ecuación (4.8) esto es equivalente a probar que

$$h(\theta) := \left|\frac{1}{\cos\theta}\left(\frac{\pi}{2} - \theta\,\mathrm{sen}\,\theta\right)\right|$$

es acotada cuando θ tiende a $\frac{\pi}{2}$ o $-\frac{\pi}{2}$. Observemos que como $h(\theta)$ es una función par, el límite es el mismo en ambos casos. Usando la *regla de L'Hopital* vemos que

$$\lim_{\theta\to\frac{\pi}{2}} |h(\theta)| = 1,$$

lo que nos permite concluir que

$$\lim_{|s|\to\infty}\left|\frac{\pi}{2}|s| - t\arg s\right| = |\sigma|$$

Con esto hemos probado (4.7) y terminamos la demostración de la proposición. □

Corolario 4.5. *Sea $s = \sigma + it \in \mathbb{C}$ con σ fijo y a un número real. Entonces*

$$\frac{\Gamma(s+a)}{\Gamma(s)} \ll (s+a)^a.$$

Demostración. De la proposición anterior tenemos

$$\Gamma(s+a) \ll |s+a|^{\sigma+a-\frac{1}{2}} e^{-\sigma-a} e^{-\frac{\pi}{2}|s+a|}, \tag{4.9}$$

y también que

$$\frac{1}{\Gamma(s)} \ll |s|^{\frac{1}{2}-\sigma} e^{\sigma} e^{\frac{\pi}{2}|s|},$$

ya que $|s^{-s}| = |s|^{-\sigma} e^{t\arg s} \ll |s|^{-\sigma} e^{\frac{\pi}{2}|s|}$ por (4.7). Combinando estos dos resultados obtenemos

$$\frac{\Gamma(s+a)}{\Gamma(s)} \ll |s+a|^a e^{\frac{\pi}{2}(|s|-|s+a|)} \leq |s+a|^a e^{\frac{\pi}{2}} \leq |s+a|^a e^{\frac{\pi}{2}|a|}.$$

Lo que implica que

$$\frac{\Gamma(s+a)}{\Gamma(s)} \ll |s+a|^a.$$

□

El siguiente lema será de gran importancia para cumplir las hipótesis del método de Selberg-Delange, en nuestro estudio del comportamiento asintótico de la cantidad de enteros representables por formas binarias ciclotómicas no triviales, proporciona una buena estimación para caracteres cuadráticos primitivos en la región $0 \leq \sigma \leq 1$.

Lema 4.6. *Sea $\chi(n)$ un caracter cuadrático primitivo módulo q con $\chi \neq \chi_0$ y $\varepsilon > 0$. Entonces para $s = \sigma + it \in \mathbb{C}$ con $0 \leq \sigma \leq 1$, se tiene que*

$$|L(s,\chi)| \leq K(1+|t|)^{\frac{1-\sigma}{2}+\varepsilon}.$$

Demostración. Como χ es cuadrático, entonces $\chi = \chi^{-1}$, por lo que de la ecuación funcional tenemos que

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

Despejando a $L(s,\chi)$ en la ecuación anterior nos da

$$L(s,\chi) = \left(\frac{q}{\pi}\right)^{\frac{1}{2}-s} L(1-s,\chi) \frac{\Gamma(\frac{1-s+\kappa}{2})}{\Gamma(\frac{s+\kappa}{2})}. \tag{4.10}$$

Como usaremos el principio de convexidad de Phragmén-Lindelöf, nos interesa conocer una cota para los extremos de la región $0 \leq \sigma \leq 1$, sin embargo, consideraremos una región ligeramente mayor porque usaremos la convergencia absoluta de la serie $\sum \chi(n) n^{-s}$ para obtener una cota para $L(1-s,\chi)$, así que elegiremos la banda dada por las rectas $\sigma = -\alpha - i\tau$ y $\sigma = 1 + \alpha + i\tau$. Tomando $s = -\alpha - it$, tenemos que $1 - s = 1 + \alpha + it$, de donde $L(1-s,\chi)$ está uniformemente acotada por $\sum |\chi(n)| n^{-1-\alpha}$. Así, sólo basta acotar el cociente

$$\mathcal{B} := \frac{\Gamma\left(\frac{1-s+\kappa}{2}\right)}{\Gamma\left(\frac{s+\kappa}{2}\right)}.$$

Observemos que

$$\frac{\left|\Gamma\left(\frac{1+\alpha+it+\kappa}{2}\right)\right|}{\left|\Gamma\left(\frac{-\alpha-it+\kappa}{2}\right)\right|} = \frac{\left|\Gamma\left(\frac{1+\alpha-it+\kappa}{2}\right)\right|}{\left|\Gamma\left(\frac{-\alpha-it+\kappa}{2}\right)\right|} = \frac{\left|\Gamma\left(\frac{-\alpha-it+\kappa}{2}+\frac{1}{2}+\alpha\right)\right|}{\left|\Gamma\left(\frac{-\alpha-it+\kappa}{2}\right)\right|} \ll \left|\frac{-\alpha-it+\kappa}{2}\right|^{\frac{1}{2}+\alpha},$$

lo que implica que

$$\mathcal{B} \ll (1+|t|)^{\frac{1}{2}+\alpha}, \tag{4.11}$$

así que sustituyendo (4.11) en (4.10) obtenemos

$$L(s,\chi) \ll (1+|t|)^{\frac{1}{2}+\alpha}$$

en la recta $\sigma = -\alpha$. Esto significa por definición que

$$|L(s,\chi)| \leq Mq^{1/2}(1+|t|)^{\frac{1}{2}+\alpha}$$

para $t_0 \leq |t|$, aprovechando que $L(s,\chi)$ es una función entera, podemos extender la desigualdad anterior a toda la recta $\sigma = -\alpha$ eligiendo la constant $M_2 = \max\{M, M_1\}$, donde M_1 es una cota para $L(s,\chi)$ en el compacto $\{z = -\alpha + i\tau \in \mathbb{C} \,|\, -t_0 \leq \tau \leq t_0\}$, por lo tanto

$$|L(s,\chi)| \leq M_2(1+|t|)^{\frac{1}{2}+\alpha}$$

en la recta $\sigma = -\alpha$. Ahora usaremos el principio de convexidad de Phragmén-Lindelöf (pág. 150, [5]) en la región $0 \leq \sigma \leq 1$, ya que $L(s,\xi)$ satisface

1. $|L(-\alpha+it,\chi)| \leq M_2(1+|t|)^{\frac{1}{2}+\alpha}$,
2. $|L(1+\alpha,\chi)| \leq M_3(1+|t|)^0$,

y $L(s,\chi) \ll e^{|s|^A}$ en la región $-\alpha \leq \sigma \leq 1+\alpha$ por el Lema 4.3. El principio de convexidad nos dice que

$$|L(s,\chi)| \leq M_2^{\ell(\sigma)} M_3^{1-\ell(\sigma)}(1+|t|)^{\left(\frac{1}{2}+\alpha\right)\ell(\sigma)}, \tag{4.12}$$

para todo s en la región $-\alpha \leq \sigma \leq 1+\alpha$ y ℓ es la función lineal tal que $\ell(-\alpha) = 1$ y $\ell(1+\alpha) = 0$. Observemos que $\ell(\sigma)$ esta dada por

$$\ell(\sigma) = -\frac{\sigma}{1+2\alpha} + \frac{1+\alpha}{1+2\alpha},$$

esto nos permite calcular $\left(\frac{1}{2}+\alpha\right)\ell(\sigma)$ en (4.12):

$$\left(\frac{1}{2}+\alpha\right)\ell(\sigma) = \frac{1+2\alpha}{2}\left(\frac{1+\alpha-\sigma}{1+2\alpha}\right) = \frac{1-\sigma}{2} + \frac{\alpha}{2}.$$

Por lo tanto

$$|L(s,\chi)| \leq K(1+|t|)^{\frac{1-\sigma}{2}+\epsilon}$$

en $0 \leq \sigma \leq 1$ al elegir $\alpha = 2\epsilon$ y la constante K apropiada en (4.12). □

Ahora podemos continuar con nuestro estudio sobre el comportamiento asintótico de la cardinalidad de $\mathcal{A}(\Phi_{\{n\geq 3\}}; N)$.

Teorema 4.7. *Existen dos sucesiones (α_j) y (β_j) tal que para toda $M \geq 0$, la siguiente igualdad se satisface uniformemente para $N \geq 2$,*

$$|\mathcal{A}(\Phi_{\{n\geq 3\}}; N)| = \frac{N}{(\log N)^{1/2}}\left\{\sum_{j=0}^{M}\frac{1}{(\log N)^j}\left(\alpha_j - \frac{\beta_j}{(\log N)^{1/4}}\right) + O\left(\frac{1}{(\log N)^{M+1}}\right)\right\}$$

Haremos algunas observaciones y comentarios antes de presentar la prueba de este teorema. Observemos que

$$\Big||\mathcal{A}(\Phi_{\{n\geq 3\}};N)|-|\mathcal{A}(\Phi_3;N)\cup\mathcal{A}(\Phi_4;N)|\Big|\leq\left|\bigcup_{\varphi(n)\geq 4}\mathcal{A}(\Phi_n;N)\right|. \tag{4.13}$$

La relación anterior es una desigualdad porque si bien $2=\varphi(3)=\varphi(4)$, dependiendo de N puede suceder que

$$(\mathcal{A}(\Phi_3;N)\cup\mathcal{A}(\Phi_4;N))\bigcap\left(\bigcup_{\varphi(n)\geq 4}\mathcal{A}(\Phi_n;N)\right)\neq\emptyset.$$

Ahora, la ecuación (4.13) implica que

$$\Big||\mathcal{A}(\Phi_{\{n\geq 3\}};N)|-(|\mathcal{A}(\Phi_3;N)|+|\mathcal{A}(\Phi_4;N)|-|\mathcal{A}(\Phi_3;N)\cap\mathcal{A}(\Phi_4;N)|)\Big|\leq\left|\bigcup_{\varphi(n)\geq 4}\mathcal{A}(\Phi_n;N)\right|,$$

y esto significa que

$$|\mathcal{A}(\Phi_{\{n\geq 3\}},N)|=|\mathcal{A}(\Phi_3;N)|+|\mathcal{A}(\Phi_4;N)|-|\mathcal{A}(\Phi_3;N)\cap\mathcal{A}(\Phi_4;N)|+O(N^{1/2}), \tag{4.14}$$

por el corolario 4.2 pues,

$$\left|\bigcup_{\varphi(n)\geq 4}\mathcal{A}(\Phi_n;N)\right|\ll N^{1/2}.$$

Como en el Teorema 4.7 el término de error es $N(\log N)^{-3/2-M}$ y precisamente

$$\frac{N}{(\log N)^{3/2+M}}\gg N^{1/2},$$

nos enfocaremos a estudiar las cardinalidades de los conjuntos $\mathcal{A}(\Phi_3;N)$, $\mathcal{A}(\Phi_4;N)$ y $\mathcal{A}(\Phi_3;N)\cap\mathcal{A}(\Phi_4;N)$. Debido al método que utilizaremos para la prueba, requeriremos utilizar un par de conjuntos auxiliares dados por

$$\tilde{\mathcal{A}}(\Phi_k;N):=\{m\in\mathbb{N}|m\leq N, m=\Phi_k(x,y)\text{ para algún }(x,y)\neq(0,0)\},\qquad(k=3,4)$$

los cuales difieren de sus análogos a lo más en dos términos. El Teorema 4.7 será una consecuencia de la siguiente proposición.

Proposición 4.8. *Existen tres sucesiones* $(\alpha_j^{(3)})$, $(\alpha_j^{(4)})$ *y* (β_j) *tales que para toda* $M \geq 0$, *las siguientes desigualdades se satisfacen uniformemente para* $N \geq 2$,

$$|\tilde{\mathcal{A}}(\Phi_k; N)| = \frac{N}{(\log N)^{1/2}} \left\{ \sum_{j=0}^{M} \frac{\alpha_j^{(k)}}{(\log N)^j} + O\left(\frac{1}{(\log N)^{M+1}} \right) \right\} \qquad (k = 3, 4)$$

y

$$|\tilde{\mathcal{A}}(\Phi_3; N) \cap \tilde{\mathcal{A}}(\Phi_4; N)| = \frac{N}{(\log N)^{3/4}} \left\{ \sum_{j=0}^{M} \frac{\beta_j}{(\log N)^j} + O\left(\frac{1}{(\log N)^{M+1}} \right) \right\}.$$

Probaremos primero la proposición para el conjunto $\tilde{\mathcal{A}}(\Phi_3; N) \cap \tilde{\mathcal{A}}(\Phi_4; N)$, estas mismas ideas nos servirán para $\tilde{\mathcal{A}}(\Phi_3; N)$ y $\tilde{\mathcal{A}}(\Phi_3; N)$.

Demostración. Sea $\xi(n)$ la función característica del conjunto de enteros $n \geq 1$ que son simultáneamente representables por $\Phi_3(x, y)$ y $\Phi_4(x, y)$. Es claro que

$$|\tilde{\mathcal{A}}(\Phi_3; N) \cap \tilde{\mathcal{A}}(\Phi_4; N)| = \sum_{n \leq N} \xi(n).$$

Por el Teorema 2.31 es fácil ver que $\xi(n)$ es una función multiplicativa, ya que para m y n con $(m, n) = 1$ se satisface:

(1) Si m y n son representables, entonces mn es representable, es decir, $\xi(nm) = \xi(n)\xi(m)$,

(2) Si $\xi(m) = 1$ y $\xi(n) = 0$, entonces mn no es representable ya que el factor en n que no permite que sea representable se conserva en el producto, es decir, $\xi(mn) = 0$,

(3) Por la misma razón que en el caso anterior si m y n no son representables, entonces su producto tampoco lo es y así $0 = \xi(m) = \xi(n) = \xi(mn)$.

Sea

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

la serie de Dirichlet asociada. Como probamos que $\xi(n)$ es una función multiplicativa, $F(s)$ tiene una representación como producto de Euler dada por

$$F(s) = \prod_p \left(1 + \frac{\xi(p)}{p^s} + \frac{\xi(p^2)}{p^{2s}} + \cdots \right).$$

Por la definición de $\xi(n)$ y por el Teorema 2.31, $\xi(p^k) = 0$ para k impar en los primos $2, 3$ y los que son congruentes con 5, 7 u 11 módulo 12, lo que implica que $F(s)$ es el producto

$$F(s) = \left(\sum_{k=0}^{\infty} \frac{1}{4^s}\right)\left(\sum_{k=0}^{\infty} \frac{1}{9^s}\right) \prod_{p\equiv 5,7,11} \left(\sum_{k=0}^{\infty} \frac{1}{p^{2sk}}\right) \prod_{p\equiv 1} \left(\sum_{k=0}^{\infty} \frac{1}{p^{sk}}\right) \tag{4.15}$$

$$= \left(1 - \frac{1}{4^s}\right)^{-1}\left(1 - \frac{1}{9^s}\right)^{-1} \prod_{p\equiv 5,7,11} \left(1 - \frac{1}{p^{2s}}\right)^{-1} \prod_{p\equiv 1} \left(1 - \frac{1}{p^{s}}\right)^{-1}. \tag{4.16}$$

Llamemos $H(s)$ al producto

$$H(s) := \left(1 - \frac{1}{4^s}\right)^{-1}\left(1 - \frac{1}{9^s}\right)^{-1} \prod_{p\equiv 5,7,11} \left(1 - \frac{1}{p^{2s}}\right)^{-1}.$$

Ahora, utilizaremos el criterio para la convergencia absoluta de productos infinitos dado por el Teorema B.9. Notemos que el producto infinito

$$\prod_{p\equiv 5,7,11} \left(1 - \frac{1}{p^{2s}}\right)^{-1} = \prod_{p\equiv 5,7,11} \left(1 + \frac{1}{p^{2s} - 1}\right)$$

converge absolutamente para $\sigma > 1/2$, ya que

$$\sum_{p\equiv 5,7,11} \left|\frac{1}{p^{2s} - 1}\right| \leq \sum_{p\equiv 5,7,11} \frac{1}{p^{2\sigma} - 1} = \sum_{p\equiv 5,7,11} \frac{a_p}{p^{2\sigma}} \leq \frac{5}{4} \sum_{n=1}^{\infty} \frac{1}{n^{2\sigma}}. \tag{4.17}$$

Donde a_p es un término de la sucesión sucesión (a_p) dada por

$$a_p := \frac{p^{2\sigma}}{p^{2\sigma} - 1},$$

la cual es decreciente tanto en p como σ. Esta sucesión satisface para $p \geq 5$,

$$a_p \leq \frac{5^{2\sigma}}{5^{2\sigma} - 1} \leq \frac{5}{4}.$$

Se sigue que $H(s)$ es una función holomorfa en $\sigma > 1/2$ y uniformemente acotada en $\sigma \geq 3/4$.

Nuestro plan es usar los caracteres de Dirichlet adecuados para formar una L-función de Dirichlet que nos permita usar el método de Selberg-Delange. Es por ello que introduciremos una función auxiliar que nos permite detectar a los primos mayores o iguales que 5 congruentes con 1 módulo 12. Esta función está dada por

$$L(p) = \frac{1}{4}\left(1 + \left(\frac{-3}{p}\right) + \left(\frac{-4}{p}\right) + \left(\frac{12}{p}\right)\right) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod{12}, \\ 0 & \text{si } p \equiv 5, 7, 11 \pmod{12}. \end{cases}$$

Para probar que la función $L(p)$ toma precisamente esos valores, veremos qué sucede en cada caso. Todos los cálculos siguientes de los valores de los caracteres $(\frac{\bullet}{p})$ se deducen de las propiedades dadas en la sección sobre caracteres de Dirichlet del Apéndice A. Si $p \equiv 1 \pmod{12}$, entonces $p \equiv 1 \pmod 4$ y $p \equiv 1 \pmod 3$, lo que nos da

$$\left(\frac{12}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{4}{p}\right) = \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = 1,$$

$$\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{4}{p}\right) = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1,$$

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} = 1.$$

Por lo tanto $L(p) = 1$ si $p \equiv 1 \pmod{12}$. Supongamos ahora que $p \equiv 5 \pmod{12}$, entonces $p \equiv 1 \pmod 4$ y $p \equiv 2 \pmod 5$, lo que implica

$$\left(\frac{12}{p}\right) = -1,\ \left(\frac{-3}{p}\right) = -1,\ \left(\frac{-4}{p}\right) = 1.$$

Supongamos que $p \equiv 7 \pmod{12}$, entonces $p \equiv 3 \pmod 4$ y $p \equiv 1 \pmod 3$, se sigue

$$\left(\frac{12}{p}\right) = -1,\ \left(\frac{-3}{p}\right) = 1,\ \left(\frac{-4}{p}\right) = -1.$$

Si $p \equiv 11 \pmod{12}$, entonces $p \equiv 3 \pmod 4$ y $p \equiv 2 \pmod 3$, de aquí que

$$\left(\frac{12}{p}\right) = 1,\ \left(\frac{-3}{p}\right) = -1,\ \left(\frac{-4}{p}\right) = -1.$$

Sustituyendo los valores anteriores en la definición de $L(p)$ vemos que $L(p) = 0$ si $p \equiv 5, 7, 11 \pmod{12}$. Denotaremos a los caracteres $\left(\frac{-3}{n}\right)$, $\left(\frac{-4}{n}\right)$ y $\left(\frac{12}{n}\right)$ por $\chi_3(n)$, $\chi_4(n)$ y $\chi_{12}(n)$ respectivamente. Observemos que

$$\left\{\left(1-\frac{1}{p^s}\right)\left(1-\frac{\chi_3(p)}{p^s}\right)\left(1-\frac{\chi_4(p)}{p^s}\right)\left(1-\frac{\chi_{12}(p)}{p^s}\right)\right\} = \begin{cases} \left(1-\frac{1}{p^s}\right)^4 & \text{si } p \equiv 1 \pmod{12}, \\ \left(1-\frac{1}{p^{2s}}\right)^2 & \text{si } p \equiv 5, 7, 11 \pmod{12}. \end{cases}$$

La igualdad anterior implica que

$$\prod_{p\equiv 1}\left(1-\frac{1}{p^s}\right)^{-1} = \prod_{p\geq 5}\left\{\left(1-\frac{1}{p^s}\right)\left(1-\frac{\chi_3(p)}{p^s}\right)\left(1-\frac{\chi_4(p)}{p^s}\right)\left(1-\frac{\chi_{12}(p)}{p^s}\right)\right\}^{-1/4} \prod_{p\equiv 5,7,11}\left(1-\frac{1}{p^{2s}}\right)^{1/2}.$$

Ahora, observemos que si $n = 3$,

$$\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{\chi_3(3)}{3^s}\right)\left(1 - \frac{\chi_4(3)}{3^s}\right)\left(1 - \frac{\chi_{12}(3)}{3^s}\right) = \left(1 - \frac{1}{9^s}\right)$$

y que para $n = 2$

$$\left(1 - \frac{1}{2^s}\right)\left(1 - \frac{\chi_3(2)}{2^s}\right)\left(1 - \frac{\chi_4(2)}{2^s}\right)\left(1 - \frac{\chi_{12}(2)}{2^s}\right) = \left(1 - \frac{1}{4^s}\right)$$

Reuniendo todos estos cálculos obtenemos

$$\prod_{p\equiv 1}\left(1 - \frac{1}{p^s}\right)^{-1} = H_1(s)\zeta(s)^{1/4}L(s,\chi_3)^{1/4}L(s,\chi_4)^{1/4}L(s,\chi_{12})^{1/4}, \tag{4.18}$$

donde

$$H_1(s) = \left(1 - \frac{1}{4^s}\right)^{1/4}\left(1 - \frac{1}{9^s}\right)^{1/4}\prod_{p\equiv 5,7,11}\left(1 - \frac{1}{p^{2s}}\right)^{1/2}.$$

Sustituyendo (4.18) en la ecuación (4.16) para $F(s)$, nos da

$$F(s) = H_2(s)\zeta(s)^{1/4}L(s,\chi_3)^{1/4}L(s.\chi_4)^{1/4}L(s,\chi_{12})^{1/4}, \tag{4.19}$$

donde

$$H_2(s) = \left(1 - \frac{1}{4^s}\right)^{-3/4}\left(1 - \frac{1}{9^s}\right)^{-3/4}\prod_{p\equiv 5,7,11}\left(1 - \frac{1}{p^{2s}}\right)^{-1/2}.$$

Obsérvese que la función $H_2(s)$ es holomorfa en $\sigma > 1/2$ y uniformemente acotada en $\sigma \geq 3/4$. Por la región clásica libre de ceros para L-funciones de Dirichlet, existe $c_0 > 0$ tal que en el dominio

$$\mathcal{D} = \left\{\sigma + it \in \mathbb{C} \;\middle|\; \sigma > 1 - \frac{c_0}{1 + \log(1 + |t|)}\right\}$$

el producto

$$L(s,\chi_3)L(s,\chi_4)L(s,\chi_{12})$$

no se anula. Esto implica que la función

$$G(s) = F(s)\zeta(s)^{-1/4} = H_2(s)L(s,\chi_3)^{1/4}L(s,\chi_4)^{1/4}L(s,\chi_{12})^{1/4}$$

puede ser extendida a una función holomorfa en $\mathcal{D}$. Tomando c_0 tal que para $s = \sigma + it \in \mathcal{D}$ satisfaga que $\sigma > 3/4$, tenemos que H_2 es uniformemente acotada en $\mathcal{D}$. Luego, utilizando el Lema 4.6 vemos que existe K tal que

$$|G(s)| \leq K\left((1+|t|)^{1/8+\varepsilon}\right)^3 = K(1+|t|)^{1/2}$$

al tomar $\varepsilon = 1/24$. Se satisfacen todas las hipótesis del Corolario 3.8 con $z = 1/4$ y obtenemos que existe una sucesión (β_j) tal que para toda $M \geq 0$ se satisface uniformemente para $N \geq 2$ que

$$\sum_{n\leq N} \xi(n) = \frac{N}{(\log N)^{3/4}} \left\{ \sum_{j=0}^{M} \frac{\beta_j}{(\log N)^j} + O\left(\frac{1}{(\log N)^{M+1}}\right)\right\}.$$

Como $\sum_{n\leq N} \xi(n) = |\tilde{\mathcal{A}}(\Phi_3; N) \cap \tilde{\mathcal{A}}(\Phi_4; N)|$ terminamos este caso, continuemos a estimar $|\mathcal{A}(\Phi_{\{n\geq 3\}}; N)|$.

Sea $\xi_3(n)$ la función indicadora del conjunto de enteros $n \geq 1$ que son representables por $\Phi_3(x, y)$, entonces

$$|\tilde{\mathcal{A}}(\Phi_3; N)| = \sum_{n\leq N} \xi_3(n).$$

Sea $F(s)$ la serie de Dirichlet asociada a $\xi_3(n)$

$$F(s) = \sum_{n=1}^{\infty} \frac{\xi_3(n)}{n^s}.$$

Como $\xi_3(n)$ es una función multiplicativa tenemos que

$$F(s) = \prod_p \left(1 + \frac{\xi_3(p)}{p^s} + \frac{\xi_3(p^2)}{p^{2s}} + \cdots\right). \tag{4.20}$$

Por el Teorema 2.30, un número natural n es representable por $\Phi_3(x, y)$ si y sólo si $n = 3^b N_{2,3}^2 N_{1,3}$ con $b \geq 0$. Ordenando el producto infinito de $F(s)$ en clases de equivalencia módulo 3, se sigue que

$$F(s) = \left(1 - \frac{1}{3^s}\right)^{-1} \prod_{p\equiv 2} \left(1 - \frac{1}{p^{2s}}\right)^{-1} \prod_{p\equiv 1} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Usando que

$$\chi_3(p) = \left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod 3 \\ -1 & \text{si } p \equiv 2 \pmod 3, \end{cases}$$

tenemos que

$$\begin{aligned} \prod_{p\equiv 1} \left(1 - \frac{1}{p^s}\right)^{-1} &= \prod_p \left\{\left(1 - \frac{1}{p^s}\right)\left(1 - \frac{\chi_3(p)}{p^s}\right)\right\}^{-1/2} \prod_{p\equiv 2} \left(1 - \frac{1}{p^{2s}}\right)^{1/2} \left(1 - \frac{1}{3^s}\right)^{1/2} \\ &= \zeta(s)^{1/2} L(s, \chi_3)^{1/2} \prod_{p\equiv 2} \left(1 - \frac{1}{p^{2s}}\right)^{1/2} \left(1 - \frac{1}{3^s}\right)^{1/2}, \end{aligned}$$

lo que da

$$F(s) = \zeta(s)^{1/2} L(s, \chi_3)^{1/2} \prod_{p \equiv 2} \left(1 - \frac{1}{p^{2s}}\right)^{-1/2} \left(1 - \frac{1}{3^s}\right)^{-1/2}.$$

Es decir,

$$F(s) = \zeta(s)^{1/2} L(s, \chi_3)^{1/2} H(s),$$

donde $H(s)$ es una función holomorfa en $\sigma > 1/2$ y uniformemente acotada en $\sigma > 3/4$. De nuevo por la región clásica $\mathcal{D}$ adecuada libre de ceros, tenemos que la serie de Dirichlet

$$L(s, \chi_3)$$

es diferente de cero, lo que implica que la función

$$G(s) = F(s)\zeta(s)^{-1/4} = H(s)L(s, \chi)^{1/2}$$

puede ser continuada analíticamente a una función holomorfa en $\mathcal{D}$, donde

$$|G(s)| \leq K(|t| + 1)^{1/4+\varepsilon},$$

con $\varepsilon = 1/4$ tenemos $|G(s)| \leq K(|t| + 1)^{1/2}$ en $\mathcal{D}$. Se sigue del Corolario 3.8 con $z = 1/2$ que existe una sucesión $(\alpha_j^{(3)})$ tal que

$$|\tilde{\mathcal{A}}(\Phi_3; N)| = \frac{N}{(\log N)^{1/2}} \left\{ \sum_{j=0}^{M} \frac{\alpha_j^{(3)}}{(\log N)^j} + O\left(\frac{1}{(\log N)^{M+1}}\right) \right\}$$

para toda $M \geq 0$ y uniformemente para $N \geq 2$.

En cuanto a $\tilde{\mathcal{A}}(\Phi_4; N)$, sea $\xi_4(n) = 1$ si n es representable por $\Phi_4(x, y)$ y $\xi_4(n) = 0$ en otro caso. Sea $F(s) = \sum \xi_4(n) n^{-s}$ la serie de Dirichlet asociada a $\xi_4(n)$. Como $n = 2^a N_{3,4}^2 N_{1,4}$ si y sólo si n es representable por $\Phi_4(x, y)$, tenemos que $F(s)$ es el siguiente producto infinito sobre primos ordenados en clases de equivalencia módulo 4,

$$F(s) = \left(1 - \frac{1}{2^s}\right)^{-1} \prod_{p \equiv 3} \left(1 - \frac{1}{p^{2s}}\right)^{-1} \prod_{p \equiv 1} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Considerando que

$$\chi_4(p) = \left(\frac{-4}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod 4, \\ -1 & \text{si } p \equiv 3 \pmod 4, \end{cases}$$

obtenemos

$$\prod_{p\equiv 1}\left(1-\frac{1}{p^s}\right)^{-1} = \prod_{p}\left\{\left(1-\frac{1}{p^s}\right)\left(1-\frac{\xi_4(p)}{p^s}\right)\right\}^{-1/2}\prod_{p\equiv 3}\left(1-\frac{1}{p^{2s}}\right)^{1/2}\left(1-\frac{1}{2^s}\right)^{1/2}$$
$$= \zeta(s)^{1/2}L(s,\chi_4)^{1/2}\left(1-\frac{1}{2^s}\right)^{1/2}\prod_{p\equiv 3}\left(1-\frac{1}{p^{2s}}\right)^{1/2}.$$

Por lo que $F(s)$ satisface

$$F(s) = \zeta(s)^{1/2}L(s,\chi_4)^{1/2}\left(1-\frac{1}{2^s}\right)^{-1/2}\prod_{p\equiv 3}\left(1-\frac{1}{p^{2s}}\right)^{-1/2},$$

es decir,

$$F(s) = \zeta(s)^{1/2}L(s,\chi_4)^{1/2}H(s),$$

donde

$$H(s) = \left(1-\frac{1}{2^s}\right)^{-1/2}\prod_{p\equiv 3}\left(1-\frac{1}{p^{2s}}\right)^{-1/2}.$$

es holomorfa en $\sigma > 1/2$ y uniformemente acotada en $\sigma \geq 3/4$. Tomando $G(s)$ como

$$G(s) = F(s)\zeta(s)^{-1/2} = L(s,\chi_4)^{1/2}H(s),$$

vemos que $G(s)$ puede ser continuada analíticamente a una función holomorfa en la región clásica libre de ceros $\mathcal{D}$ y por el principio de convexidad de Phragmén-Lindelöf, $G(s)$ satisface

$$|G(s)| \leq K(|t|+1)^{1/2}$$

uniformemente para $s \in \mathcal{D}$. Por el Corolario 3.8 con $z = 1/2$ tenemos que existe una sucesión $(\alpha_j^{(4)})$ tal que para $M \geq 0$ y uniformemente para $N \geq 2$ se tiene

$$|\tilde{\mathcal{A}}(\Phi_4;N)| = \frac{N}{(\log N)^{1/2}}\left\{\sum_{j=0}^{M}\frac{\alpha_j^{(4)}}{(\log N)^j} + O\left(\frac{1}{(\log N)^{M+1}}\right)\right\}.$$

□

Continuaremos ahora con la demostración del Teorema 4.7. Recordemos que nuestro propósito es estimar las cardinalidades de $\mathcal{A}(\Phi_3;N)$, $\mathcal{A}(\Phi_4;N)$ y la de su intersección. De la proposición anterior podemos concluir que

$$|\mathcal{A}(\Phi_3;N)| + |\mathcal{A}(\Phi_4;N)| = \frac{N}{(\log N)^{1/2}}\left\{\sum_{j=0}^{M}\frac{\alpha_j^{(3)}+\alpha_j^{(4)}}{(\log N)^j} + O\left(\frac{1}{(\log N)^{M+1}}\right)\right\}$$

y también

$$|\mathcal{A}(\Phi_3;N)\cap\mathcal{A}(\Phi_4;N)| = \frac{N}{(\log N)^{3/4}}\left\{\sum_{j=0}^{M}\frac{\beta_j}{(\log N)^j} + O\left(\frac{1}{(\log N)^{M+1}}\right)\right\}.$$

Por lo que gracias a la ecuación (4.14) tenemos

$$|\mathcal{A}(\Phi_{\{n\geq 3\}};N)| = \frac{N}{(\log N)^{1/2}}\left\{\sum_{j=0}^{M}\frac{1}{(\log N)^j}\left(\alpha_j - \frac{\beta_j}{(\log N)^{1/4}}\right) + O\left(\frac{1}{(\log N)^{M+1}}\right)\right\},$$

donde $\alpha_j = \alpha_j^{(3)} + \alpha_j^{(4)}$. Con esto concluye la prueba del Teorema 4.7.

4.3. Un resultado sobre la densidad de las representaciones

Recordemos que en la Sección 4.1 vimos que el conjunto de ternas solución dado por

$$\mathcal{S}_m := \{(n,x,y)\in\mathbb{Z}^3 \,|\, n\geq 3,\ m=\Phi_n(x,y),\ \text{máx}\{|x|,|y|\}\geq 2\} \tag{4.21}$$

es finito. Sea a_m la cardinalidad de $\mathcal{S}_m$, a_m representa la cantidad de *representaciones* de m dadas por formas binarias ciclotómicas no triviales. Daremos un resultado sobre el crecimiento del valor promedio de a_m, las formas binarias $\Phi_3(x,y)$ y $\Phi_4(x,y)$ toman de nuevo un papel crítico para este resultado.

Lema 4.9. *Sea $r_2(n)$ el número de soluciones a la ecuación $x^2+y^2=n$. Entonces*

$$\sum_{1\leq n\leq N} r_2(n) \sim \pi N.$$

Demostración. Observemos que como $x^2+y^2=n$ traza un círculo, las soluciones a dicha ecuación son las parejas de enteros (x,y) que están sobre la circunferencia determinada por la ecuación. No es difícil ver que las soluciones que cuenta $r_2(1)+r_2(2)+\cdots+r_2(N)$ son las parejas sobre la circunferencia $x^2+y^2=N$ y las contenidas en su interior menos $(0,0)$, ya que $x^2+y^2=N$ traza un círculo de radio $\sqrt{N}$. Ahora, podemos asignar a cada una de las soluciones contenidas en el círculo de radio $\sqrt{N}$ un cuadrado de lado 1 que tiene como esquina inferior izquierda dicha solución, lo que implica que el área dada por el número total de cuadrados es la cantidad de soluciones.

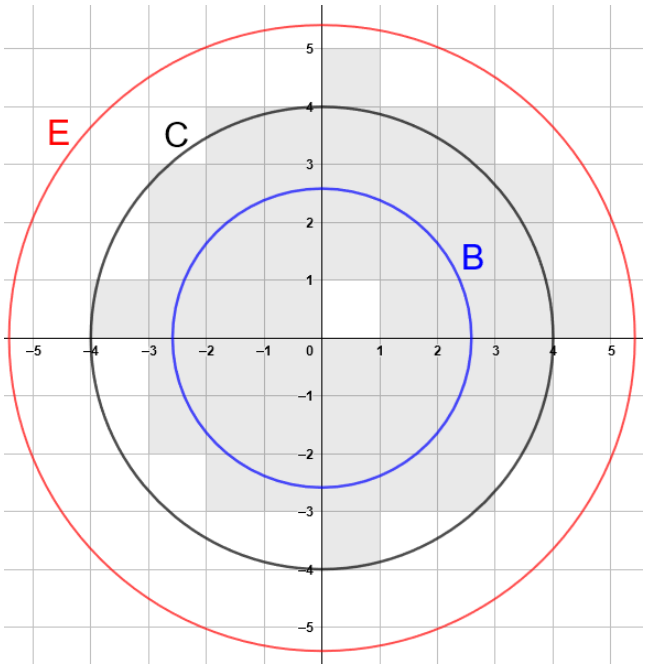


Figura 4.1: Ejemplo del caso $N = 16$. El área gris está determinada por las soluciones de $0 < x^2 + y^2 \leq N$. El círculo C tiene radio $\sqrt{N}$, mientras que los círculo E y B tienen radios $\sqrt{N} + \sqrt{2}$ y $\sqrt{N} - \sqrt{2}$ respectivamente.

Por último, observemos que dicha area está acotada superiormente por el área del círculo $x^2+y^2 = (\sqrt{N}+\sqrt{2})^2$ y acotada inferiormente por el área de $x^2+y^2 = (\sqrt{N}-\sqrt{2})^2$. Entonces

$$\pi(\sqrt{N} - \sqrt{2})^2 \leq \sum_{1\leq n\leq N} r_2(n) \leq \pi(\sqrt{N} + \sqrt{2})^2$$

Dividiendo por πN, tenemos

$$1 - \frac{2\sqrt{2}}{\sqrt{N}} + \frac{2}{N} \leq \frac{1}{\pi N} \sum_{1\leq n\leq N} r_2(n) \leq 1 + \frac{2\sqrt{2}}{\sqrt{N}} + \frac{2}{N},$$

haciendo N tender a infinito tenemos el resultado. □

El siguiente lema es la versión análoga del anterior para la forma binaria $\Phi_3(x, y)$.

Lema 4.10. *Sea $r_3(n)$ el número de soluciones a la ecuación $x^2 + xy + y^2 = n$. Entonces*

$$\sum_{1\leq n\leq N} r_3(n) \sim \frac{2\pi N}{\sqrt{3}}.$$

Demostración. La prueba es análoga a la prueba del lema anterior, solo que ahora, la ecuación $x^2 + xy + y^2 = n$ es la de una elipse cuyo semieje menor tiene una longitud de $\sqrt{2n/3}$ y eje mayor de $\sqrt{2n}$. Asignamos un cuadrado unitario a cada solución de $0 < x^2 + xy + y^2 \leq N$. Podemos acotar superiormente el área de los cuadrados con el área de una elipse cuyos ejes menor y mayor tienen una longitud de $\sqrt{2N/3} + \sqrt{2}$ y $\sqrt{2N} + \sqrt{2}$ respectivamente, y también podemos acotar inferiormente con la elipse cuyos ejes tiene longitudes $\sqrt{2N/3} - \sqrt{2}$ y $\sqrt{2N} - \sqrt{2}$.

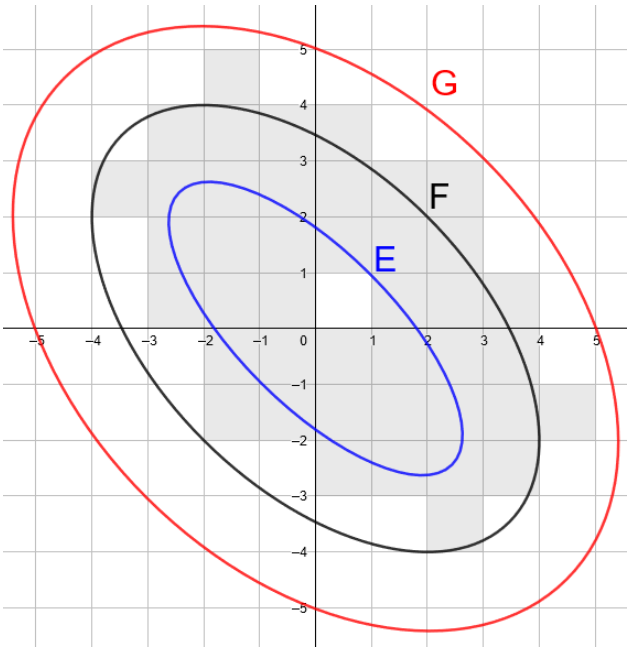


Figura 4.2: Ejemplo del caso $N = 12$. F es la elipse dada por $x^2 + xy + y^2 = 12$ y el área gris esta dada por las soluciones. El área de las elipse G acota superiormente el área de las soluciones y el área de la elipse E lo acota inferiormente.

El área de una elipse es el producto πab, donde a y b son las longitudes de los semiejes mayor y menor respectivamente, entonces

$$\pi\left(\sqrt{2N} - \sqrt{2}\right)\left(\sqrt{\frac{2N}{3}} - \sqrt{2}\right) \leq \sum_{1 \leq n \leq N} r_3(n) \leq \pi\left(\sqrt{2N} + \sqrt{2}\right)\left(\sqrt{\frac{2N}{3}} + \sqrt{2}\right).$$

Continuando los cálculos obtenemos que

$$\pi\left(\frac{2N}{\sqrt{3}} - 2\sqrt{N} - 2\sqrt{\frac{N}{3}} + 2\right) \leq \sum_{1 \leq n \leq N} r_3(n) \leq \pi\left(\frac{2N}{\sqrt{3}} + 2\sqrt{N} + 2\sqrt{\frac{2N}{3}} + 2\right).$$

Dividiendo ahora por $2\pi N/\sqrt{3}$ resulta en

$$1-\frac{\sqrt{3}}{\sqrt{N}}-\frac{1}{\sqrt{N}}+\frac{\sqrt{3}}{N}\leq\frac{\sqrt{3}}{2\pi N}\sum_{1\leq n\leq N}r_3(n)\leq 1+\frac{\sqrt{3}}{\sqrt{N}}+\frac{1}{\sqrt{N}}+\frac{\sqrt{3}}{N}.$$

Haciendo N tender a infinito concluimos que

$$\sum_{1\leq n\leq N}r_3(n)\sim\frac{2\pi N}{\sqrt{3}}.$$

□

Finalmente, el siguiente resultado nos muestra que el valor promedio del conjunto $\{a_1,a_2,...,a_N\}$ tomado sobre sus valores distintos de cero, crece como $\sqrt{\log N}$.

Teorema 4.11. *Para $N\geq 1$, definimos A_N y M_N como*

$$A_N=|\mathcal{A}(\Phi_{\{n\geq 3\}};N)|\qquad y\qquad M_N=\frac{1}{A_N}(a_1+a_2+\cdots+a_N).$$

Existe una constante positiva κ tal que

$$M_N\sim\kappa\sqrt{\log N}.$$

Demostración. Observemos que $a_1+a_2+\cdots+a_N$ cuenta el número de ternas (n,x,y) con $n\geq 3$, máx$\{|x|,|y|\}\geq 2$ y $\Phi_n(x,y)\leq N$. Denotaremos por $r_2(n)$ el número de representaciones con $\Phi_4(x,y)=n$, por $r_3(n)$ la cantidad de ternas que satisfacen $\Phi_3(x,y)=n$ y por T el número de ternas con $\varphi(n)>2$, entonces

$$\sum_{1\leq n\leq N}a_n=\sum_{1\leq n\leq N}r_2(n)+2\sum_{1\leq n\leq N}r_3(n)+T. \tag{4.22}$$

Obtendremos una equivalencia asíntotica para la suma del lado derecho de la ecuación; utilizando los lemas 4.9, 4.10 y 4.2 nos da

$$\lim_{N\to\infty}\frac{1}{N}\left(\sum_{1\leq n\leq N}r_2(n)+2\sum_{1\leq n\leq N}r_3(n)+T\right)=\pi+\frac{4\pi}{\sqrt{3}}+0.$$

En otras palabras,

$$\sum_{1\leq n\leq N}r_2(n)+2\sum_{1\leq n\leq N}r_3(n)+T\sim\left(1+\frac{4}{\sqrt{3}}\right)\pi N.$$

Del Teorema 4.7 con $M=0$ vemos que

$$A_N=|\mathcal{A}(\Phi_{\{n\geq 3\}};N)|=\frac{N}{(\log N)^{1/2}}\left(\alpha_0-\frac{\beta_0}{(\log N)^{1/4}}+O\left(\frac{1}{(\log N)}\right)\right),$$

de donde se sigue que

$$A_N \sim \frac{N}{(\log N)^{1/2}}\alpha_0.$$

Utilizando esta equivalencia asintótica en el cociente M_N,

$$M_N = \frac{1}{A_N}\sum_{1\leq n\leq N} a_n \sim \frac{(\log N)^{1/2}}{N\alpha_0}\left(1+\frac{4}{\sqrt{3}}\right)\pi N = \frac{\pi}{\alpha_0}\left(1+\frac{4}{\sqrt{3}}\right)\sqrt{\log N}.$$

□

Apéndice A

Caracteres de Dirichlet

Recordemos que una *función aritmética* es una función $f : \mathbb{N} \to \mathbb{C}$. Se dice que f es multiplicativa si $f(1) = 1$ y

$$f(mn) = f(n)f(m) \tag{A.1}$$

siempre que m y n sean primos relativos, es decir $(m, n) = 1$. Como ejemplo de una función multiplicativa tenemos a la función $\varphi : \mathbb{N} \to \mathbb{N}$ de Euler dada por

$$\varphi(n) = |\{m \in \mathbb{N} \,|\, m \leq n, (m, n) = 1\}|,$$

es decir, $\varphi(n)$ es la cantidad de primos relativos a n menores iguales a n. Otra función aritmética importante es la función de Möbius denotada por $\mu(n)$ y definida a continuación.

Definición A.1. La función de Möbius es la función aritmética dada por

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^r & \text{si } 1 = e_1 = e_2 = ... = e_r, \\ 0 & \text{en otro caso,} \end{cases}$$

donde para $n > 1$ escribimos n en su descomposición en primos, es decir $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$.

De la definición anterior se sigue que $\mu(n) = 0$ si n no es libre de cuadrados y que satisface:

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{si } n > 1. \end{cases} \tag{A.2}$$

Cuando $f(1) = 1$ y la ecuación (A.1) se satisface para todo m y n enteros, se dice que f es completamente multiplicativa. Para p un primo impar fijo, el símbolo de Legendre

denotado por $\left(\frac{a}{p}\right)$, es uno de los caracteres elementales de la teoría de números, y es definido mediante

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p|a, \\ 1 & \text{si } p \nmid a \text{ y } x^2 \equiv a \pmod{p} \text{ tiene solución}, \\ -1 & \text{si } p \nmid a \text{ y } x^2 \equiv a \pmod{p} \text{ no tiene solución}. \end{cases}$$

Además de ser completamente multiplicativo, el símbolo de Legendre satisface que

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p} \tag{A.3}$$

y $(\frac{a}{p}) = (\frac{b}{p})$ siempre que $a \equiv b \pmod{p}$, por lo que el símbolo de Legendre es una función periódica.

Existen resultados sobre el símbolo de Legendre que son de especial utilidad para calcular su valor, como los siguientes:

Teorema A.2 (Ley de Reciprocidad Cuadrática)**.** *Si p y q son dos primos impares distintos, entonces*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Luego, tenemos que

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } p \equiv 1 \pmod{4}, \\ -1 & \text{si } p \equiv 3 \pmod{4}, \end{cases} \tag{A.4}$$

y también,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{si } p \equiv 1 \text{ o } 7 \pmod{8}, \\ -1 & \text{si } p \equiv 3 \text{ o } 5 \pmod{8}. \end{cases} \tag{A.5}$$

Los caracteres de Dirichlet son una generalización del símbolo de Legendre.

Definición A.3. Sea $q \geq 1$ un entero. Un caracter de Dirichlet módulo q es una función $\chi : \mathbb{Z} \to \mathbb{C}$ que satisface

1) $\chi(n+q) = \chi(n)$ para todo $n \in \mathbb{Z}$,

2) $\chi(n) = 0$ si y sólo si $(n, q) > 1$,

3) $\chi(mn) = \chi(m)\chi(n)$ para todo $m, n \in \mathbb{Z}$.

De la definición anterior vemos que los caracteres de Dirichlet cumplen las siguientes propiedades:

a) $\chi(1) = 1$,

b) χ es completamente multiplicativo,

c) $\chi(a) = \chi(b)$ si $a \equiv b \pmod{q}$,

d) para todo a con $(a, q) = 1$, $\chi(a)$ es una raíz $\varphi(q)$-ésima de la unidad.

Para cada q, existe un único caracter (mód q) denotado por χ_0, que toma únicamente los valores $\{0, 1\}$, es llamado el caracter principal y se define mediante

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

El símbolo de Legendre en cambio, tiene como rango al conjunto $\{0, 1, -1\}$. Caracteres χ con esta propiedad son llamados caracteres cuadráticos, es decir, si $\chi^2 = \chi_0$.

Una consecuencia de la definición de caracter, es la siguiente igualdad.

Teorema A.4 (Primera relación de ortogonalidad)**.** *Si χ es un caracter de Dirichlet* (mód q) *y $k \in \mathbb{Z}$, entonces*

$$\sum_{n=1}^{kq} \chi(n) = \begin{cases} 0 & si\ \chi \neq \chi_0, \\ \varphi(q) & si\ \chi = \chi_0. \end{cases}$$

Ahora, supongamos que $d|q$ y que χ^* es un caracter (mód d) y sea

$$\chi(n) = \begin{cases} \chi^*(n) & \text{si } (n, q) = 1, \\ 0 & \text{en otro caso.} \end{cases}$$

Entonces $\chi(n)$ es un caracter de Dirichlet (mód q), en este caso decimos que χ^* induce a χ.

Definición A.5. Sea χ un caracter (mód q). Diremos que d es un cuasiperiodo de χ si $\chi(m) = \chi(n)$ siempre que $m \equiv n \pmod{d}$ y $(mn, q) = 1$.

El menor cuasiperiodo d de χ es llamado el *conductor de* χ y es un divisor de q. En el caso en que q sea igual a d, diremos que χ es un *caracter primitivo*, tales caracteres χ no son inducidos por ningún otro caracter con un conductor menor. Resumiendo, tenemos:

Teorema A.6. *Sea χ un caracter de Dirichlet módulo q y sea d el conductor de χ. Entonces $d|q$ y existe un único caracter primitivo χ^** (mód d) *que induce a χ.*

La siguiente tabla muestra todos los caracteres χ_i módulo 9. Como $\varphi(9) = 6$, existen 6 caracteres (mód 9) y los valores que toman son múltiplos de $\omega = e^{\frac{\pi i}{3}}$.

$\chi \setminus n$	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*
$\chi_0(n)$	0	1	1	0	1	1	0	1	1
$\chi_1(n)$	0	1	ω	0	ω^2	$-\omega^2$	0	$-\omega$	-1
$\chi_2(n)$	0	1	ω^2	0	$-\omega$	$-\omega$	0	ω^2	1
$\chi_3(n)$	0	1	-1	0	1	-1	0	1	-1
$\chi_4(n)$	0	1	$-\omega$	0	ω^2	ω^2	0	$-\omega$	1
$\chi_5(n)$	0	1	$-\omega^2$	0	$-\omega$	ω	0	ω^2	-1

El símbolo de Legendre $(\frac{\bullet}{p})$ es un caracter primitivo módulo p que sólo está definido para primos p impares, existe una generalización que no se limita a estos números y es conocida como el símbolo de Kronecker.

Definición A.7. Decimos que d es un discriminante cuadrático si algunas de las siguientes dos propiedades se satisfacen

a) $d \equiv 1 \pmod 4$ y d es libre de cuadrados,

b) $4|d$, $d/4 \equiv 2$ o $3 \pmod 4$ y $d/4$ es libre de cuadrados.

Para cada discriminante d, definimos el símbolo de Kronecker $\left(\frac{d}{n}\right)_K$ por:

i) $\left(\frac{d}{p}\right)_K = 0$ cuando $p|d$,

ii) $\left(\frac{d}{2}\right)_K = \begin{cases} 1 & \text{cuando } d \equiv 1 \pmod 8, \\ -1 & \text{cuando } d \equiv 5 \pmod 8, \end{cases}$

iii) $\left(\frac{d}{p}\right)_K = \left(\frac{d}{p}\right)$, el símbolo de Legendre cuando p es primo y $p > 2$,

iv) $\left(\frac{d}{-1}\right)_K = \begin{cases} 1 & \text{cuando } d > 0, \\ -1 & \text{cuando } d < 0, \end{cases}$

v) $\left(\frac{d}{n}\right)_K$ es una función completamente multiplicativa de n.

Es importante señalar que el símbolo de Kronecker es un caracter cuadrático primitivo módulo $|d|$.

Definición A.8. Dado un caracter χ módulo q, definimos la suma de Gauss $G(\chi)$ de χ como

$$G(\chi) = \sum_{a=1}^{q} \chi(a) e(a/q),$$

donde $e(x) = e^{2\pi i x}$.

Aunque la suma de Gauss $G(\chi)$ tiene muchas propiedades interesantes y útiles, para nosotros sólo será necesario el siguiente teorema.

Teorema A.9. *Supongamos que χ es un caracter primitivo módulo q. Entonces*

$$|G(\chi)| = \sqrt{q}.$$

El lector interesado puede consultar [8] para obtener más información sobre los caracteres de Dirichlet.

Apéndice B

L-funciones de Dirichlet

El siguiente concepto es fundamental en la teoría analítica de números y es uno que permite de cierta forma relacionar todos lo conceptos anteriores puramente numéricos con la teoría de funciones analíticas de variable compleja. Como es de costumbre utilizaremos la notación $s = \sigma + it$ para denotar al número complejo s.

Definición B.1. Una serie de Dirichlet $\alpha(s)$ es una serie de la forma

$$\alpha(s) = \sum_{n=1}^{\infty} a_n n^{-s},$$

donde $(a_n)_{n=1}^{\infty}$ es una sucesión en $\mathbb{C}$.

Obsérvese que en el caso en que $a_n = 1$ para todo $n \in \mathbb{N}$, tenemos como serie de Dirichlet a la famosa función $\zeta(s)$ de Riemann:

Definición B.2. Sea $s = \sigma + it \in \mathbb{C}$ con $\sigma > 1$, se define la función zeta de Riemann como la serie

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

Una de las primeras preguntas que surgen al considerar una serie de Dirichlet es la que concierne a la convergencia. Por ejemplo, es bien sabido que para $\varepsilon > 0$, la serie

$$\sum_{n=1}^{\infty} \frac{1}{n^{1+\varepsilon}}$$

converge, por lo que para s con $s = 1 + \varepsilon + it$ la función $\zeta(s)$ es finita, es decir, hay convergencia absoluta en todo un semiplano.

Teorema B.3. *Para una serie de Dirichlet $\alpha(s)$, existe $\sigma_c \in \mathbb{R} \cup \{-\infty, \infty\}$ con la propiedad de que $\alpha(s)$ converge para todo s con $\sigma > \sigma_c$ y no converge para $\sigma < \sigma_c$. Más aun, si s_0 es un punto con $\sigma_0 > \sigma_c$, entonces existe una vecindad de s_0 donde $\alpha(s)$ converge uniformemente. Diremos que σ_c es la abscisa de convergencia de $\alpha(s)$.*

La serie $\alpha(s) = \sum a_n n^{-s}$ es localmente uniformemente convergente para $\sigma > \sigma_c$, y como cada término es una función analítica, $\alpha(s)$ es analítica para $\sigma > \sigma_c$, además, la derivada de la serie es uniformemente convergente y está dada por

$$\alpha'(s) = -\sum_{n=1}^{\infty} a_n (\log n) n^{-s}$$

para s en el semiplano $\sigma > \sigma_c$.

El siguiente teorema es particularmente importante porque nos permite calcular la abscisa de convergencia de una serie de Dirichlet.

Teorema B.4. *Sea $A(x) = \sum_{n \leq x} a_n$. Si $\sigma_c < 0$, entonces $A(x)$ es una función acotada y*

$$\sum_{n=1}^{\infty} a_n n^{-s} = s \int_1^{\infty} A(x) x^{-s-1} dx \tag{B.2}$$

para $\sigma > 0$. Si $\sigma_c \geq 0$, entonces

$$\limsup_{x \to \infty} \frac{\log |A(x)|}{\log x} = \sigma_c,$$

y (B.2) se cumple para $\sigma > \sigma_c$.

El Teorema B.3 nos dice que para $s = \sigma + it \in \mathbb{C}$ con $\sigma < \sigma_c$ no se tiene convergencia para la serie de Dirichlet $\alpha(s) = \sum a_n n^{-s}$ con dicha abscisa de convergencia. Cuando s está sobre la recta $\sigma_c + it$ no necesariamente es una singularidad de $\alpha(s)$, dicho comportamiento dependerá de $(a_n)_{n=1}^{\infty}$.

Teorema B.5. *Sea $\alpha(s) = \sum a_n n^{-s}$ una serie de Dirichlet con abscisa de convergencia σ_c finita. Si $a_n \geq 0$ para toda n entonces el punto σ_c es una singularidad de la función $\alpha(s)$.*

Respecto al comportamiento asintótico de una serie de Dirichlet, se tiene el siguiente teorema, el cual nos será de gran utilidad.

Teorema B.6. *Supongamos que $\alpha(s) = \sum a_n n^{-s}$ tiene una abscisa de convergencia σ_c. Si δ y ε están fijos, $0 < \varepsilon < \delta < 1$, entonces*

$$\alpha(s) \ll (|t| + 4)^{1-\delta+\varepsilon}$$

uniformemente para $\sigma \geq \sigma_c + \delta$. La constante implícita puede depender de los valores δ y ε.

Hemos hablado de series de Dirichlet de una forma general, aunque a nosotros nos interesan aquellas series de Dirichlet asociadas a funciones aritméticas multiplicativas. En este caso particular tenemos una representación muy importante que es consecuencia de la multiplicatividad de la función.

Teorema B.7 (Fórmula del Producto de Euler)**.** *Sea $f(n)$ una función aritmética multiplicativa y supongamos que para $s \in \mathbb{C}$ se tiene que $\sum |f(n)n^{-s}| < \infty$, entonces*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \cdots\right),$$

donde el producto se toma sobre todos los primos p.

Por ejemplo, la función $\zeta(s)$ de Riemann está dada para $\sigma > 1$ por la función aritmética multiplicativa $f(n) = 1$ para todo $n \in \mathbb{N}$, por lo que

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

Definición B.8. Si el producto infinito

$$\prod_{k=1}^{\infty}(1 + |c_k|)$$

converge, entonces se dice que el producto $\prod_{k=1}^{\infty}(1 + |c_k|)$ *converge absolutamente.*

Es siguiente teorema presenta un importante criterio para determinar cuando un producto infinito converge absolutamente.

Teorema B.9. *El producto infinito $\prod_{k=1}^{\infty}(1 + c_k)$ converge absolutamente si y sólo si, la serie infinita $\sum_{k=1}^{\infty} c_k$ converge absolutamente.*

Es importante mencionar que $\zeta(s)$ también cuenta con otra representación, la cual es válida en el semiplano $\sigma > 0$.

Teorema B.10. *Supongamos que $\sigma > 0$, $x > 0$ y que $s \neq 1$. Entonces*

$$\zeta(s) = \sum_{n \leq x} n^{-s} + \frac{x^{1-s}}{s-1} + \frac{\{x\}}{x^s} - s\int_x^{\infty} \{u\}u^{-s-1}du,$$

donde $\{u\}$ denota la parte fraccionaria de u, es decir, $\{u\} = u - \lfloor u \rfloor$, donde $\lfloor u \rfloor$ es la parte entera de u.

Definición B.11. Sea χ un caracter (mód q). Para $\sigma > 1$, definimos la L-función asociada al caracter χ como

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

Como χ es completamente multiplicativo, el Teorema B.7 nos da

$$L(s,\chi) = \prod_{p} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

para $\sigma > 1$. Obsérvese también que debido a la primera relación de ortogonalidad, si $\chi \neq \chi_0$, entonces

$$\sum_{n=1}^{kq} \chi(n) = 0,$$

para $k = 1, 2, 3, ...$ Por lo tanto

$$\left| \sum_{n \leq x} \chi(n) \right| \leq q$$

para cualquier x, y por el Teorema B.4 tenemos que $L(s,\chi)$ converge para $\sigma > 0$, siempre que $\chi \neq \chi_0$.

En el Teorema B.5 hablamos de las singularidades de las series de Dirichlet, y como consecuencia en el caso de χ_0, $L(s,\chi_0)$ tiene un polo en $s = 1$. Sin embargo, para $\chi \neq \chi_0$ esto no sucede.

Teorema B.12. *Sea χ un caracter de Dirichlet* (mód q) *con $\chi \neq \chi_0$. Entonces $L(1,\chi) \neq 0$.*

El siguiente resultado es una ecuación funcional para L-funciones de Dirichlet con implicaciones muy importantes para su estudio analítico.

Teorema B.13 (Ecuación Funcional para Caracteres Primitivos)**.** *Sea χ un caracter primitivo* (mód q)*, entonces para toda s*

$$L(s,\chi) = \epsilon(\chi) L(1-s, \chi^{-1}) 2^s \pi^{s-1} q^{1/2-s} \Gamma(1-s) \operatorname{sen}\left(\frac{\pi}{2}(s+\kappa)\right),$$

donde $\kappa = 0$ si χ es una función par, $\kappa = 1$ en otro caso y

$$\epsilon(\chi) = \frac{G(\chi)}{i^{\kappa}\sqrt{q}}.$$

Observación B.14. En el caso especial de caracteres cuadráticos primitivos χ, se tiene que $\epsilon(\chi) = 1$ y $\chi = \chi^{-1}$, así que la ecuación funcional es de la forma

$$L(s,\chi) = L(1-s,\chi)2^s\pi^{s-1}q^{1/2-s}\Gamma(1-s)\operatorname{sen}\left(\frac{\pi}{2}(s+\kappa)\right)$$

El teorema anterior junto con el Teorema B.12 nos permite concluir que para $\chi \neq \chi_0$, $L(s,\chi)$ posee una extensión analítica entera. También obtenemos la conocida ecuación funcional para $\zeta(s)$.

Corolario B.15. *Para toda $s \neq 1$,*

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

Para una mayor profundización en estos temas, puede consultarse [4].

Apéndice C

Función gamma

Para cualquier número complejo s diferente de un número entero no positivo, definimos la *función gamma* como el producto

$$\Gamma(s) = \frac{e^{-\gamma s}}{s} \prod_{n=1}^{\infty} \frac{e^{s/n}}{1 + s/n},$$

donde γ es la constante de Euler. Obsérvese que de la definición, la función $1/\Gamma$ es una función entera con ceros simples en los enteros no positivos, es decir, $\Gamma(s)$ es distinta de cero y meromorfa con polos simples en los enteros no positivos. La función gamma también satisface la siguiente igualdad conocida como *fórmula de Gauss*

$$\Gamma(s) = \lim_{N \to \infty} \frac{N^s N!}{s(s+1)\cdots(s+N)}. \tag{C.1}$$

Al tomar $s = 1$, vemos que $\Gamma(1) = 1$. De la misma ecuación se sigue

$$s\Gamma(s) = \Gamma(s+1). \tag{C.2}$$

Por inducción, la propiedad anterior nos permite obtener que

$$\Gamma(n+1) = n!$$

para enteros no negativos n. Es por esto que la función gamma es una generalización del factorial de un número entero positivo. Utilizando de nuevo (C.1) vemos que

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\operatorname{sen} \pi s},$$

y con $s = 1/2$ tenemos

$$\Gamma\left(1/2\right) = \sqrt{\pi}.$$

De la definición de la función gamma es posible obtener la *fórmula de duplicación de Legendre*:

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

Respecto al comportamiento asintótico de $\Gamma(s)$ existe la conocida *fórmula de Stirling* dada por el siguiente teorema.

Teorema C.1 (Fórmula de Stirling)**.** *Sea $\delta > 0$, y sea $\mathcal{R} = \mathcal{R}(\delta)$ el conjunto de los números complejos s con $|s| \geq \delta$ y $|\arg s| < \pi - \delta$. Entonces*

$$\Gamma(s) = \sqrt{2\pi}s^{s-1/2}e^{-s}\left(1 + O\left(\frac{1}{|s|}\right)\right)$$

uniformemente para $s \in \mathcal{R}$.

La fórmula de Stirling nos dice que para $|s|$ suficientemente grande,

$$\frac{\Gamma(s)}{\sqrt{2\pi}s^{s-1/2}e^{-s}} \leq 1 + \frac{1}{|s|}.$$

Tomando logaritmos en ambos lados y reacomodando obtenemos

$$\log\Gamma(s) = \log\sqrt{2\pi} + \left(s - \frac{1}{2}\right)\log s - s + O\left(\log\left(1 + \frac{1}{|s|}\right)\right).$$

Aprovechando las propiedades del logaritmo y multiplicando por -1, vemos que

$$\log\left(\frac{1}{\Gamma(s)}\right) = -\log\sqrt{2\pi} - \left(s - \frac{1}{2}\right)\log s + s + O\left(\log\left(1 + \frac{1}{|s|}\right)\right).$$

Consecuentemente tenemos la siguiente igualdad para $\Gamma(s)^{-1}$ bajo las hipótesis del Teorema C.1:

$$\frac{1}{\Gamma(s)} = \frac{1}{\sqrt{2\pi}}s^{\frac{1}{2}-s}e^{s}\left(1 + O\left(\frac{1}{|s|}\right)\right). \tag{C.3}$$

La función $\Gamma(s)$ también puede ser expresada mediante una integral de la siguiente manera:

Teorema C.2 (Integral de Euler)**.** *Para $s \in \mathbb{C}$ con $\mathrm{Re}\, s > 0$, se tiene*

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

Por último, enunciaremos algunas identidades más que la función gamma satisface

a) $\Gamma(\overline{s}) = \overline{\Gamma(s)}$,

b) $|\Gamma(it)|^2 = \dfrac{\pi}{t \sinh \pi t}$,

c) $|\Gamma\left(1/2 + it\right)|^2 = \dfrac{\pi}{\cosh \pi t}$.

Las demostraciones de los resultados aquí expuestos, así como más información sobre la función $\Gamma(s)$ pueden consultarse en [4].

Apéndice D

Polinomios de Bernoulli

Consideremos la sucesión $(b_n(x))_{n=0}^{\infty}$ de polinomios definidos en $[0,1]$ por las condiciones

(1) $b_0(x) = 1$,

(2) para $n \geq 1$, $b_n'(x) = nb_{n-1}(x)$ y

(3) $\int_0^1 b_n(x)dx = 0$.

Esta lista de propiedades implican la identidad

$$\sum_{n=0}^{\infty} b_n(x)\frac{y^n}{n!} = \frac{ye^{xy}}{e^y - 1},$$

permitiéndonos calcular el polinomio $b_n(x)$. Por ejemplo,

$$\begin{array}{ll} b_0(x) = 1 & b_3(x) = x^3 - \frac{3}{2}x^2 + \frac{1}{2}x \\ b_1(x) = x - \frac{1}{2} & b_4(x) = x^4 - 2x^3 + x^2 - \frac{1}{30} \\ b_2(x) = x^2 - x + \frac{1}{6} & b_5(x) = x^5 - \frac{5}{2}x^4 + \frac{5}{3}x^3 - \frac{1}{6}x. \end{array}$$

Definimos la n-ésima función de Bernoulli $B_n(x)$ como la función de periodo 1 que coincide con $b_n(x)$ en el intervalo $[0,1)$. Como $x = \{x\}$ en el intervalo $[0,1)$ y $\{x\}$ es periódica, tenemos

$$B_1(x) = \{x\} - \frac{1}{2}, \quad B_2(x) = \{x\}^2 - \{x\} + \frac{1}{6}, \quad ...$$

Es fácil ver que para $n \geq 2$, $B_n(x)$ es una función continua en $\mathbb{R}$ y diferenciable en $\mathbb{R} \setminus \mathbb{Z}$. Definimos el n-ésimo número de Bernoulli B_n mediante

$$B_n := B_n(0).$$

Para $n \geq 1$ se tiene que $B_{2n+1} = 0$ y de los ejemplos de arriba, vemos que

$$b_0 = 1, \qquad b_1 = -\frac{1}{2}, \qquad b_2 = \frac{1}{6}, \qquad b_4 = \frac{-1}{30}.$$

Por último, las funciones de Bernoulli satisfacen que para n par,

$$|B_n(x)| \leq B_n.$$

Existen muchas propiedades útiles para la teoría analítica de números que las funciones de Bernoulli cumplen, sin embargo, para el propósito de este trabajo no serán necesarias. El lector interesado puede consultar el apéndice de [4] para obtener más información sobre el uso y propiedades de las funciones de Bernoulli.

Bibliografía

[1] É. Fouvry, C. Levesque, M. Waldschmidt. *Representation of integers by cyclotomic binary forms.* Acta Arithmetica, **184**, 67–86, 2018.

[2] K. Győry. *Représentation des nombres entiers par des formes binaires.* Publ. Math. Debrecen **24 (3–4)**, 363–375, 1977.

[3] G. Tenenbaum. *Introduction to analytic and probabilistic number theory.* Press Syndicate of the University of Cambridge, 1995.

[4] H. L. Montgomery, R. C. Vaughan. *Multiplicative Number Theory: I. Classical Theory.* Cambridge University Press, 2006.

[5] H. Iwaniec, E. Kowalski. *Analytic Number Theory* American Mathematical Society Colloquium Publications **53**, American Mathematical Society, Providence, RI, (2004).

[6] M. Mignotte, M. Waldschmidt. *Linear forms in two logarithms and Schneider's method, III.* Ann. Fac. Sci. Toulouse Math. (**5**), 43–75, 1989.

[7] Z. I. Borevich, I. R. Shafarevich. *Number Theory* Academic Press, 1966.

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