CIMAT

Centro de Investigación en Matemáticas, A.C.

CONSTRUCCIÓN ANALÍTICA DE LAS FUNCIONES L P-ÁDICAS INTERPOLANDO NÚMEROS DE BERNOULLI

T E S I S

Que para obtener el grado de

Maestro en Ciencias

con Orientación en

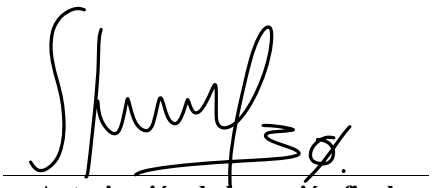
Matemáticas Básicas

Presenta

Holman Alejandro Pérez Ayala

Director de Tesis:

Dr. Jesús Rogelio Pérez Buendía



Autorización de la versión final

Guanajuato, Gto., 01 de septiembre de 2020

"[· · ·] Sin embargo, antes de llegar al verso final ya había comprendido que no saldría jamás de ese cuarto, pues estaba previsto que la ciudad de los espejos (o los espejismos) sería arrasada por el viento y desterrada de la memoria de los hombres en el instante en que Aureliano Babilonia acabara de descifrar los pergaminos, y que todo lo escrito en ellos era irrepetible desde siempre y para siempre, porque las estirpes condenadas a cien años de soledad no tenían una segunda oportunidad sobre la tierra."

Gabriel García Márquez
Cien años de soledad

Agradecimientos

A mi madre y a mi hermana, mi siempre amada familia; al final del sendero una nueva vida espera.

A mi director de tesis, Dr. Jesús Rogelio Pérez Buendía, que con su apoyo, sus consejos y su invaluable experiencia me han guiado de la mejor manera posible.

Al Centro de Investigación en Matemáticas. A. C. (CIMAT) por permitirme continuar mi formación profesional, a su personal administrativo, así como a sus docentes de los cuales aprendí una nueva visión de las matemáticas, ciencia formal que tanto amo.

Al Consejo Nacional de Ciencia y Tecnología (CONACYT) por brindarme los medios económicos (Número de beca: 945430) durante los dos años de estudio que duró el programa de maestría.

Introducción

En noviembre de 1859 el gran matemático alemán *Bernhard Riemann* (1826-1866) publicó su único y fundamental artículo sobre teoría de números, llamado "Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse" ("Sobre el Número de Primos Menores que una Magnitud dada"). La principal herramienta, él escribió, debería ser el uso de la función ζ definida de la siguiente manera:

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

como una función en variable compleja la cual converge absolutamente para $\mathrm{Re}(s) > 1$, y cuya relación con los números primos fue establecida en 1737 por *Leonard Euler* (1707-1783), vía el producto:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p\text{-primo}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

La relación anterior es consecuencia directa del Teorema Fundamental de la Aritmética; esto es, la unicidad de la factorización en números primos en el anillo de los enteros $\mathbb{Z}$. En el mismo artículo, Riemann muestra que $\zeta(s)$ admite una continuación analítica para todo número complejo $s \in \mathbb{C}$; excepto en el valor $s = 1$, donde esta función posee un polo simple. Incluso presenta una ecuación funcional para ζ:

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

La importancia de la investigación hecha por Riemann radica en el hecho que escribe sin dar demostración, una fórmula explícita para la función $\pi(x)$ que cuenta los números primos menores que $x \in \mathbb{R}$ en términos de los ceros de la función ζ. Por esto la famosa hipótesis de Riemann, la cual busca establecer el comportamiento de los ceros no triviales de la función ζ; a saber, que todos ellos poseen parte real igual a $1/2$, reciba tal atención de los matemáticos hasta hoy.

Del estudio realizado por Euler de la función ζ; más específicamente, los valores que toma la función ζ en los enteros pares positivos, encontró que:

$$\zeta(2k) = \frac{(-1)^{k-1}(2\pi)^{2k}}{2 \cdot (2k)!} B_{2k},$$

donde los B_{2k} son los números de Bernoulli. El caso particular $k = 1$, es la solución al famoso problema de Basilea; el cual es, hallar la suma del inverso de los cuadrados de

los enteros positivos:

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Una generalización de esta función ζ son las famosas funciones L de Dirichlet, llamadas así en honor al matemático alemán Gustav Lejeune Dirichlet (1805-1859) las cuales se definen por la serie:

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

donde χ es un carácter de Dirichlet y converge absolutamente para $s \in \mathbb{C}$ con $\mathrm{Re}(s) > 1$. Si $\chi = \chi_1$ es el carácter trivial, se recupera la función zeta de Riemann ya que $L(s, \chi_1) = \zeta(s)$. Al igual que en el caso de la función zeta estas funciones admiten una continuación analítica al plano complejo $\mathbb{C}$ y también un representación como producto de Euler:

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

La primera aplicación de estas fuciones, hecha en 1837, fue en la demostración del Teorema de Dirichlet en Progresiones Aritméticas; la cual usa el hecho que $L(1, \chi) \neq 0$.

En 1847, Ernst Kummer (1810-1893) en el desarrollo de sus ideas sobre campos ciclotómicos, resolvió el Último Teorema de Fermat para todo los primos p que son primos relativos al número de clase del campo ciclotómico $\mathbb{Q}(\zeta_p)$; es decir, si p es uno de tales primos, entonces:

$$x^p + y^p \neq z^p \qquad \forall\ x, y, z \in \mathbb{Z}_+.$$

Para determinar si p divide al número de clase h_p de $\mathbb{Q}(\zeta_p)$ (estos primos son conocidos como "primos regulares"), Kummer estableció que: un primo p es regular si y solo si p divide el numerador de algún número de Bernoulli B_k, con k número par menor o igual a $p - 3$, donde utilizó sus famosas congruencias para los números de Bernoulli; a saber:

Si $m, n \in \mathbb{Z}_+$ son números pares tales que $m \equiv n \not\equiv 0 \pmod{p-1}$, entonces:

$$\frac{B_m}{m} \equiv \frac{B_n}{n} \pmod{p}.$$

Más generalmente, si m, n son enteros positivos pares con $m \equiv n \pmod{\varphi(p^a)}$, donde φ es la función indicatriz de Euler y $n \not\equiv 0 \pmod{p-1}$, entonces:

$$(1 - p^{m-1})\frac{B_m}{m} \equiv (1 - p^{n-1})\frac{B_n}{n} \pmod{p^a}.$$

En 1897 Kurt Hensel (1861-1941) basado en los trabajos de Kummer, desarrolló sistemáticamente la teoría de los campos de números p-ádicos. Él descubrió la norma p-ádica en el campo de los números racionales $\mathbb{Q}$ y completó el campo con respecto a esta norma. Aunque la verdadera importancia de esta construcción fue dada en el Teorema de Ostrowski (1918), donde Alexander Ostrowski (1893-1986) estableció que las únicas normas que se definen en el campo de los números racionales son el valor absoluto usual y la norma p-ádica; salvo equivalencias. Haciendo las debidas completaciones métricas y calculando su cerradura algebraica, obtenemos para cada caso el campo $\mathbb{C}$ de los números complejos con el valor absoluto usual, y los campos $\mathbb{C}_p$ análogos p-ádicos de los números complejos en el caso no arquimediano.

De lo anterior se abre un mundo que hasta ese momento en la investigación matemática no se había explorado. Por tal motivo buscar los análogos p-ádicos de las funciones clásicas definidas en $\mathbb{C}$, sería una empresa que se se llevaría a cabo en el siglo XX. Un desarrollo significativo de este punto de vista fue la interpretación de la congruencias de Kummer para los números de Bernoulli, alrededor de 100 años después del artículo escrito por Riemann, hecha por Tomio Kubota (1930-) y Heinrich-Wolfgang Leopoldt (1927-2011), en el artículo de 1964 llamado "Eine p-adische Theorie der Zetawerte. I. Einführung der p-adischen Dirichletschen L-funktionen" (ver [16]), donde realizan la construcción del análogo p-ádico de la función ζ de Riemann. Observando que:

$$\zeta(1-k) = -\frac{B_k}{k}, \tag{1}$$

junto a las congruencias de Kummer, vía interpolación mostraron la existencia de una función analítica p-ádica $\zeta_p(s)$ tal que:

$$\zeta_p(1-k) = (1-p^{k-1})\zeta(1-k).$$

En esta tesina, estudiamos en paralelo los casos clásico y p-ádico de las funciones L definidas en $\mathbb{C}$ y en $\mathbb{C}_p$, deteniéndonos en cada caso, en el entendimiento de ciertos valores especiales de estas funciones y su relación con los números de Bernoulli. Sus métodos de continuación analítica, notando la diferencia en el conjunto donde las dos clases de funciones L están definidas, pero también advirtiendo, como fue tomada la idea de la construcción p-ádica de las funciones L, a partir de los valores especiales de las funciones L de Dirichlet clásicas.

Históricamente, Hurwitz introdujo su función zeta:

$$\zeta(s,x) = \sum_{n=0}^{\infty} \frac{1}{(n+x)^s}, \qquad 0 < x \leq 1,$$

con el propósito explícito de derivar una continuación analítica para la serie $L(s,\chi)$ observando que esta serie se puede expresar como una combinación lineal de funciones zeta de Hurwitz, esto es:

$$L(s,\chi) = f^{-s} \sum_{a=1}^{f} \chi(a)\zeta\left(s, \frac{a}{f}\right), \quad \text{(ver Obs. 3,4)}.$$

De modo que la continuación analítica de la función zeta de Hurwitz proporciona la continuación analítica de las funciones L de Dirichlet. Por otro lado, al obtener la generalización de la ecuación (1):

$$L(1-n,\chi) = -\frac{B_{n,\chi}}{n} \qquad n \geq 1, \tag{2}$$

donde los $B_{n,\chi}$ son los números de Bernoulli generalizados. Podemos notar que el lado derecho de esta identidad es esencialmente una combinación lineal de términos de la forma:

$$\sum_{j=0}^{n} \binom{n}{j} (f/a)^j B_j,$$

ya que como veremos en el Teorema 1.15:

$$B_{n,\chi} = f^{n-1} \sum_{a=1}^{f} \chi(a) B_n\left(\frac{a}{f}\right), \tag{3}$$

y reemplazando en (2), obtenemos:

$$L(1-n,\chi) = -\frac{1}{f} \cdot \frac{1}{n} \sum_{a=1}^{f} \chi(a) a^n \sum_{j=0}^{n} \binom{n}{j} \left(\frac{f}{a}\right)^j B_j, \quad n \geq 1, \tag{4}$$

donde f es el conductor del carácter χ (ver Definición B.25), $B_n(a/f)$ es el n-ésimo polinomio de Bernoulli evaluado en a/f y B_j es el j-ésimo número de Bernoulli. Es la ecuación (4) la que brinda la dirección correcta en el momento de construir funciones L p-ádicas, dado que tiene sentido reemplazar n por una variable p-ádica.

En los apéndices finales tratamos de una manera mas o menos formal (si este no es el caso, referenciamos debidamente la bibliografía correspondiente), los conceptos necesarios en el desarrollo de la teoría que se utiliza de manera frecuente a lo largo del texto.

En el capítulo 1 presentamos los números de Bernoulli y los números de Bernoulli generalizados asociados a un carácter de Dirichlet y tiene como principal objetivo deducir las congruencias de Kummer utilizando técnicas p-ádicas, y en cuyo proceso, se pueden observar las bases de la interpolación para los valores especiales de la función zeta de Riemann.

El objetivo del capítulo 2 es presentar el concepto de función p-ádica, es decir, funciones definidas en $\mathbb{C}_p$ y que toman valores en $\mathbb{C}_p$, por ende, cuestiones como extensiones analíticas de funciones muy usadas en análisis complejo y herramienta fundamental en el estudio de la funciones L de Dirichlet, encontrarán también su análogo p-ádico vía interpolación.

En el capítulo 3 construimos las funciones L p-ádicas interpolando valores especiales de las funciones L de Dirichlet clásicas, a saber, aquellos valores que involucran a los números de Bernoulli, donde definimos (ver Teorema 3.29):

$$L_p(s,\chi) = \frac{1}{F} \cdot \frac{1}{s-1} \sum_{\substack{a=1 \\ p \nmid a}}^{F} \chi(a) \langle a \rangle^{1-s} \sum_{k=0}^{\infty} \binom{1-s}{k} (F/a)^k B_k \tag{5}$$

con s variable p-ádica, F múltiplo del conductor del carácter de Dirichlet y $\langle a\rangle^{1-s}$ como en la Observación 2.40. Las funciones L p-ádicas que surgen de este método son usualmente llamadas *funciones L p-ádicas analíticas*, que generalizan (4) como resultado de la interpolación realizada en los valores enteros negativos. Utilizamos después las funciones $L_p(s,\chi)$ para lograr una deducción analítica de las congruencias de Kummer que simplifica notablemente los métodos p-ádicos utilizados en el capítulo 1. En el camino, tratamos la extensión analítica de las funciones L de Dirichlet clásicas deduciendo su ecuación funcional, esto con el fin de hacer un paralelo entre los métodos utilizados en análisis complejo y análisis p-ádico a la hora de definir funciones analíticas en determinado conjunto de convergencia, ya sea en $\mathbb{C}$ o en $\mathbb{C}_p$.

Índice general

Capítulo 1

Números de Bernoulli

En este capítulo presentamos los números de Bernoulli y los números de Bernoulli generalizados asociados a un carácter de Dirichlet. Ambos tipos de números de Bernoulli, los cuales poseen una estrecha relación con la función zeta de Riemann y las funciones L de Dirichlet; pues ciertos valores especiales de estas funciones son precisamente estos números multiplicados por determinado factor, son pieza clave en la construcción análoga p-ádica de las funciones L.

El capítulo tiene como principal objetivo deducir las congruencias de Kummer utilizando técnicas p-ádicas, y en cuyo proceso, se pueden observar las bases de la interpolación para los valores especiales de la función zeta de Riemann.

1.1. Números de Bernoulli y la función Zeta de Riemann

Jakob Bernoulli (1654-1705), en su obra póstuma *Ars Conjectandi* (1713) (ver [3]) introdujo los números de Bernoulli al encontrar una fórmula general para la suma:

$$s_k(n) = 1^k + 2^k + \cdots + (n-1)^k. \tag{1.1}$$

Sin embargo, el matemático indio Aryabhata (c.476–550) ya había trabajado en este problema antes, pues en sus investigaciones deriva las fórmulas explícitas para los casos $k = 1, 2$ y 3 (ver [5], p.38).

Definición 1.1. *Se definen los números de Bernoulli, como los números B_k que aparecen en la expansión en serie de potencia de la siguiente función:*

$$\frac{t}{e^t - 1} = \sum_{k=0}^{+\infty} \frac{B_k t^k}{k!}.$$

Observación 1.2. *Algunos de estos números son:*

$$\begin{array}{ccccc} B_0 = 1, & B_1 = -1/2, & B_2 = 1/6, & B_4 = -1/30, & B_6 = 1/42, \\ B_8 = -1/30, & B_{10} = 5/66, & B_{12} = -691/2730, & B_{14} = 7/6, \cdots & \end{array}$$

Presentaremos entonces una fórmula explícita para (1.1). Consideremos la serie de potencias:

$$\sum_{k=0}^{+\infty}\frac{s_k(n)t^k}{k!}=\sum_{k=0}^{+\infty}\frac{t^k}{k!}\sum_{j=0}^{n-1}j^k=\sum_{j=0}^{n-1}\sum_{k=0}^{+\infty}\frac{(tj)^k}{k!}$$
$$=\sum_{j=0}^{n-1}e^{tj}=\frac{e^{nt}-1}{e^t-1}.$$

El intercambio de los símbolos sumatorios se puede realizar por el teorema de Tonelli para series (ver [24]. Teorema 0. 0.2); luego:

$$\begin{aligned}\frac{e^{nt}-1}{e^t-1}&=\frac{e^{nt}-1}{t}\frac{t}{e^t-1}\\&=\left(\frac{1}{t}\sum_{i=1}^{+\infty}\frac{(nt)^i}{i}\right)\left(\sum_{k=0}^{+\infty}\frac{B_kt^k}{k!}\right)\quad\text{(Definición 1.1)}\\&=\left(\sum_{i=1}^{+\infty}\frac{n^it^{i-1}}{i!}\right)\left(\sum_{k=0}^{+\infty}\frac{B_kt^k}{k!}\right).\end{aligned}$$

Por lo tanto, al hacer $k=i-1$ en la serie de la izquierda y multiplicando como series formales tenemos que:

$$\sum_{k=0}^{+\infty}\frac{s_k(n)t^k}{k!}=\left(\sum_{k=0}^{+\infty}\frac{n^{k+1}}{(k+1)!}t^k\right)\left(\sum_{k=0}^{+\infty}\frac{B_k}{k!}t^k\right)=\sum_{k=0}^{+\infty}\left(\sum_{i=0}^{k}\frac{B_in^{k+1-i}}{(k+1-i)!\cdot i!}\right)t^k.$$

y comparando los coeficientes de los t^k al momento de efectuar el producto; tenemos:

$$\frac{s_k(n)}{k!}=\sum_{i=0}^{k}\frac{1}{(k+1-i)!\cdot i!}B_in^{k+1-i}.$$

Al multiplicar ambos lados de la igualdad por $(k+1)!$, vemos que:

$$(k+1)s_k(n)=\sum_{i=0}^{k}\frac{(k+1)!}{(k+1-i)!\cdot i!}B_in^{k+1-i},$$

lo cual sabemos es igual a:

$$(k+1)s_k(n)=\sum_{i=0}^{k}\binom{k+1}{i}B_in^{k+1-i}.\tag{1.2}$$

Por otro lado, notemos que:

$$\binom{k+1}{i}=\frac{k+1}{k+1-i}\binom{k}{i},\quad\text{y}\quad\binom{k}{i}=\binom{k}{k-i};$$

por lo tanto, de la identidad (1.2) tenemos:

$$(k+1)s_k(n)=\sum_{i=0}^{k}\binom{k}{i}\frac{k+1}{k+1-i}B_in^{k+1-i}\quad\Longrightarrow\quad s_k(n)=\sum_{i=0}^{k}\binom{k}{i}\frac{1}{k+1-i}B_in^{k+1-i},$$

y haciendo el cambio de variable $j=k-i$, tenemos que:

$$s_k(n) = \sum_{j=k}^{0} \binom{k}{k-j} \frac{n^{j+1}}{j+1} = \sum_{j=0}^{k} \binom{k}{j} B_{k-j} \frac{n^{j+1}}{j+1}.$$

Con lo cual hemos demostrado el siguiente teorema:

Teorema 1.3. ***Fórmula de Bernoulli.*** *Para $k, n \in \mathbb{Z}_+$, se cumple que:*

$$s_k(n) = \sum_{i=0}^{k} \binom{k}{i} B_{k-i} \frac{n^{i+1}}{i+1}. \tag{1.3}$$

Notemos que $s_k(n)$ en su fórmula general es un polinomio en n de grado $k+1$, con los números de Bernoulli en sus coeficientes.

Ahora continuamos demostrando algunas propiedades de los números de Bernoulli que utilizaremos frecuentemente.

Lema 1.4. *$B_k = 0$ para $k \geq 3$ entero impar.*

Demostración. Observemos primero que:

$$\frac{t}{2} + \sum_{k=0}^{+\infty} \frac{B_k t^k}{k!} = \frac{t}{2} + \frac{t}{e^t - 1} = \frac{te^t + t}{2(e^t - 1)} = \frac{t(e^t + 1)}{2(e^t - 1)}.$$

Sea $f(t) = \frac{t(e^t+1)}{2(e^t-1)}$, demostremos que f es una función par en la variable t; en efecto:

$$f(-t) = \frac{-t(e^{-t} + 1)}{2(e^{-t} - 1)} = \frac{-t(1 + e^t)}{2(1 - e^t)} = \frac{t(e^t + 1)}{2(e^t - 1)} = f(t).$$

Por lo tanto, tenemos que $f(t) = f(-t)$, esto es:

$$\frac{t}{2} + \sum_{k=0}^{+\infty} \frac{B_k}{k!} t^k = -\frac{t}{2} + \sum_{k=0}^{+\infty} (-1)^k \frac{B_k}{k!} t^k. \tag{1.4}$$

Como $B_0 = 1$ y $B_1 = -1/2$ entonces de (1.4), tenemos que:

$$\frac{t}{2} + 1 - \frac{t}{2} + \sum_{k=2}^{+\infty} \frac{B_k}{k!} t^k = -\frac{t}{2} + 1 + \frac{t}{2} + \sum_{k=2}^{+\infty} (-1)^k \frac{B_k}{k!} t^k \implies \sum_{k=2}^{+\infty} \frac{B_k}{k!} t^k = \sum_{k=2}^{+\infty} (-1)^k \frac{B_k}{k!} t^k.$$

Con lo cual $B_k = (-1)^k B_k$ para todo $k \geq 2$. Luego, si $k = 2q + 1$ con $q \geq 1$ tenemos que $B_{2q+1} = -B_{2q+1}$; esto significa, $B_{2q+1} = 0$. Hemos demostrado así que $B_k = 0$ para todo número impar $k \geq 3$.

□

Para establecer propiedades sobre los números de Bernoulli B_{2k} con $k \in \mathbb{Z}_+$, necesitamos conocer la relación entre la función ζ de Riemann y los números de Bernoulli.

En 1734, Euler resolvió el problema de Basilea y dio el increíble resultado:

$$\sum_{n=1}^{+\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Euler incluso fue mas allá y descubrió que para los valores pares de la función zeta de Riemann tenemos:

Teorema 1.5. ***Fórmula de Euler para la Función ζ de Riemann.*** *Para $k \geq 1$ número entero, se cumple que:*

$$\zeta(2k) = \sum_{n\geq 1} \frac{1}{n^{2k}} = (-1)^{k-1} \frac{(2\pi)^{2k}}{2(2k)!} B_{2k}. \tag{1.5}$$

Demostración. Para obtener la fórmula de Euler, tenemos (ver [23], cap. 5, ej. 3.2) para todo $t \in \mathbb{R}$:

$$\sin(\pi t) = \pi t \prod_{n=1}^{+\infty} \left(1 - \frac{t^2}{n^2}\right).$$

En particular para $0 < t < 1$ tomando el logaritmo:

$$\log(\sin \pi t) = \log \pi t + \sum_{n=1}^{+\infty} \log\left(1 - \frac{t^2}{n^2}\right),$$

y derivando:

$$\frac{\pi \cos \pi t}{\sin \pi t} = \frac{\pi}{\pi t} + \sum_{n=1}^{+\infty} \frac{-2t/n^2}{1 - t^2/n^2} = \frac{1}{t}\left(1 - 2t^2 \sum_{n=1}^{+\infty} \frac{1/n^2}{1 - t^2/n^2}\right),$$

por lo tanto:

$$\begin{aligned}
\frac{\pi t \cos \pi t}{\sin \pi t} &= 1 - 2t^2 \sum_{n=1}^{+\infty} \frac{1}{n^2} \cdot \frac{1}{1 - t^2/n^2} \\
&= 1 - 2t^2 \sum_{n=1}^{+\infty} \frac{1}{n^2} \sum_{k=0}^{+\infty} \left(\frac{t}{n}\right)^{2k} \\
&= 1 - 2 \sum_{n=1}^{+\infty} \sum_{k=0}^{+\infty} \left(\frac{t}{n}\right)^{2(k+1)} \\
&= 1 - 2 \sum_{n=1}^{+\infty} \sum_{k=1}^{+\infty} \left(\frac{t}{n}\right)^{2k} \\
&= 1 - 2 \sum_{k=1}^{+\infty} \sum_{n=1}^{+\infty} \left(\frac{t}{n}\right)^{2k} \\
&= 1 - 2 \sum_{k=1}^{+\infty} \zeta(2k) t^{2k}.
\end{aligned}$$

Luego, para $0 < t < 1$ hemos deducido la fórmula:

$$\frac{\pi t \cos(\pi t)}{\sin(\pi t)} = 1 - 2\sum_{k=1}^{+\infty} \zeta(2k) t^{2k}.$$

Por otro lado, recordemos que:

$$\cos \pi t = \frac{e^{i\pi t} + e^{-i\pi t}}{2} \quad \text{y} \quad \sin \pi t = \frac{e^{i\pi t} - e^{-i\pi t}}{2i},$$

en donde $i^2 = -1$, luego:

$$\frac{\cos \pi t}{\sin \pi t} = \frac{\frac{e^{i\pi t}+e^{-i\pi t}}{2}}{\frac{e^{i\pi t}-e^{-i\pi t}}{2i}} = \frac{i(e^{i\pi t} + e^{-i\pi t})}{e^{i\pi t} - e^{-i\pi t}} \implies \frac{\pi t \cos \pi t}{\sin \pi t} = \frac{\pi t i(e^{i\pi t} + e^{-i\pi t})}{e^{i\pi t} - e^{-i\pi t}}.$$

Ahora bien:

$$\begin{aligned} \frac{\pi t i(e^{i\pi t} + e^{-i\pi t})}{e^{i\pi t} - e^{-i\pi t}} &= \frac{\pi t i(e^{2\pi i t} + 1)}{e^{2\pi i t} - 1} \\ &= \pi t i + \frac{2\pi i t}{e^{2\pi i t} - 1} \\ &= \pi i t + \sum_{k=0}^{+\infty} B_k \frac{(2\pi i)^k t^k}{k!}. \end{aligned}$$

De lo anterior y dado que $B_0 = 1$, $B_1 = -1/2$ y $B_k = 0$ para $k \geq 3$ entero impar, deducimos que:

$$\begin{aligned} 1 - 2\sum_{k=1}^{+\infty} \zeta(2k) t^{2k} &= \pi t i + \sum_{k=0}^{+\infty} B_k \frac{(2\pi i)^k t^k}{k!} \\ &= \pi t i + 1 - \pi t i + \sum_{k=1}^{+\infty} \frac{(2\pi i)^{2k}}{(2k)!} B_{2k} t^{2k}, \end{aligned}$$

luego :

$$\sum_{k=1}^{+\infty} (-1) 2\zeta(2k) t^{2k} = \sum_{k=1}^{+\infty} (-1)^k \frac{(2\pi)^{2k}}{(2k)!} B_{2k} t^{2k},$$

por último igualando coeficientes, obtenemos la fórmula de Euler para la función ζ de Riemann como se quería, la cual es:

$$\zeta(2k) = (-1)^{k-1} \frac{(2\pi)^{2k}}{2(2k)!} B_{2k}.$$

□

A continuación listamos algunas consecuencias que se pueden deducir de este teorema.

Observación 1.6. *(i)* $(-1)^k B_{2k} < 0$ *para* $k \geq 0$*, de manera que los* B_{2k} *tienen signo alternado.*

(ii) Como $\zeta(2k) \to 1$ *cuando* $k \to +\infty$*, tenemos que:*

$$|B_{2k}| \sim \frac{2(2k)!}{(2\pi)^{2k}}.$$

(iii) En particular, de la desigualdad $e^k > k^k/k!$*, deducimos que:*

$$(2k)! > \frac{(2k)^{2k}}{e^{2k}} \implies \frac{2(2k)!}{(2\pi)^{2k}} > \frac{2(2k)^{2k}}{(2\pi)^{2k}e^{2k}} = 2 \cdot \left(\frac{k}{\pi e}\right)^{2k};$$

por lo tanto

$$|B_{2k}| > 2 \cdot \left(\frac{k}{\pi e}\right)^{2k} \implies \left|\frac{B_{2k}}{2k}\right| > \frac{1}{k}\left(\frac{k}{\pi e}\right)^{2k} \longrightarrow +\infty \quad si \quad k \to +\infty;$$

con lo cual

$$\left|\frac{B_{2k}}{2k}\right| \longrightarrow +\infty \quad si \quad k \to +\infty \tag{1.6}$$

Por la fórmula de Euler para la función ζ de Riemann sabemos qué valores toma la función zeta en los enteros pares positivos. Hasta la fecha (septiembre de 2020), no se conoce una fórmula general similar a la de Euler para los valores enteros impares positivos; aunque, Roger Apéry (1916-1994) en 1977, demostró que $\zeta(3)$ es número irracional, razón por la cual al valor $\zeta(3)$ se le conoce como constante de Apéry.

Surge entonces la pregunta. ¿Qué valores toma la función zeta en los enteros negativos? Para dar respuesta a esta pregunta notemos que (ver Apéndice A. Proposición A.10) la función ξ definida como sigue:

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

donde Γ es la función gamma (ver A.2), admite una extensión analítica al plano complejo, y además satisface la ecuación funcional:

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

luego:

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

De la fórmula de duplicación de Legendre (ver A.3):

$$\Gamma(s)\Gamma\left(s+\frac{1}{2}\right) = \frac{2\sqrt{\pi}}{2^{2s}}\Gamma(2s), \tag{1.7}$$

para $s/2$ tenemos que:

$$\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right) = \frac{2\sqrt{\pi}}{2^{s}}\Gamma(s).$$

Por otro lado, reemplazando $(1-s)/2$ por s en (ver Proposición A.5):

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s}$$

tenemos que:

$$\Gamma\left(\frac{1-s}{2}\right)\Gamma\left(\frac{1+s}{2}\right) = \frac{\pi}{\sin\left(\pi\frac{1-s}{2}\right)} = \frac{\pi}{\cos \pi s/2},$$

con lo cual:

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

por lo tanto, tenemos que:

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

Entonces, hemos demostrado que:

Lema 1.7. ***Ecuación Funcional Función*** ζ ***de Riemann.*** *Si* $s \in \mathbb{C} - \{0,1\}$, *entonces:*

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

Observación 1.8. *En particular, si* $k > 1$ *con* $k \in \mathbb{Z}$, *tenemos que:*

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

Luego, si $k \geq 2$ es entero par, tomando $k = 2q$ para $q \in \mathbb{Z}_+$, y reemplazando en la ecuación de la observación anterior junto a la fórmula de Euler para la función zeta de Riemann (1.5), tenemos que:

$$\begin{aligned}\zeta(1-2q) &= 2(2\pi)^{-2q}\cos(\pi q)\Gamma(2q)\zeta(2q)\\ &= 2(2\pi)^{-2q}(-1)^q(2q-1)!(-1)^{q-1}\frac{(2\pi)^{2q}}{2(2q)!}B_{2q}\\ &= -\frac{B_{2q}}{2q}.\end{aligned}$$

Por otro lado, si $k \geq 3$ entero impar por Lema 1.4 sabemos que $B_k = 0$, y como por Proposición A.11 la función zeta de Riemann posee ceros en los enteros pares negativos, tenemos que:

$$\zeta(1-k) = -\frac{B_k}{k}, \quad \text{si } k = 2q+1 \ \ \forall q \in \mathbb{Z}_+.$$

Hemos utilizado entonces una ecuación funcional de la función zeta de Riemann para demostrar el siguiente teorema:

Teorema 1.9. *Para $k \in \mathbb{Z}$, con $k \geq 2$, se cumple que:*

$$\zeta(1-k) = -\frac{B_k}{k}. \tag{1.8}$$

Esta relación entre la función zeta de Riemann y los números de Bernoulli es utilizada en 1964 por Leopoldt y Kubota en [16] para la construcción de las función ζ de Riemann p-ádica.

1.2. Números de Bernoulli generalizados

Definición 1.10. *Sea χ carácter de Dirichlet de conductor $f = f_\chi$ (ver Apéndice B. Definición B.25), entonces definimos los* ***números de Bernoulli generalizados*** *$B_{n,\chi}$ usando la función:*

$$F_\chi(t) = \sum_{a=1}^{f} \frac{\chi(a) t e^{at}}{e^{ft}-1} = \sum_{n=0}^{+\infty} B_{n,\chi} \frac{t^n}{n!}. \tag{1.9}$$

Asumimos, a no ser que lo mencionemos explícitamente que $f > 1$, i.e., el carácter de Dirichlet χ no es el carácter principal χ_1 (ver Apéndice B. Teorema B.16).

Al hacer la expansión:

$$\frac{te^{at}}{e^{ft}-1} = \frac{1}{f} + \left(\frac{a}{f} - \frac{1}{2}\right) t + \left(\frac{a^2}{f} - a + \frac{f}{6}\right) \frac{t^2}{2} + \left(\frac{a^3}{f} - \frac{3a^2}{2} + \frac{af}{2}\right) \frac{t^3}{6} + \cdots$$

Se sigue del Teorema B.13 (iii) que:

$$\begin{aligned}
B_{0,\chi} &= 0; \\
B_{1,\chi} &= \frac{1}{f} \sum_{a=1}^{f} \chi(a) a; \\
B_{2,\chi} &= \frac{1}{f} \sum_{a=1}^{f} \chi(a) a^2 - \sum_{a=1}^{f} \chi(a) a; \\
B_{3,\chi} &= \frac{1}{f} \sum_{a=1}^{f} \chi(a) a^3 - \frac{3}{2} \chi(a) a^2 + \frac{f}{2} \sum_{a=1}^{f} \chi(a) a.
\end{aligned}$$

Más adelante (ver Teorema 1.15), daremos una fórmula general para $B_{n,\chi}$ la cuál juega un papel crucial en la generalización de la fórmula (1.8).

Los números de Bernoulli que se definen a partir de la expansión en series de potencias de la función:

$$F(t) = \frac{t}{e^t - 1}, \tag{1.10}$$

con t una indeterminada, por la Definición 1.1, tenemos que[1]:

$$F(t) = \sum_{n=0}^{+\infty} B_n \frac{t^n}{n!}.$$

Por otra parte, sea x otra indeterminada y definamos:

$$F(t,x) = \frac{te^{xt}}{e^t - 1} = \sum_{n=0}^{+\infty} B_n(x) \frac{t^n}{n!}, \tag{1.11}$$

entonces:

$$\begin{aligned} F(t,x) &= F(t)e^{xt} \\ &= \left(\sum_{n=0}^{+\infty} B_n \frac{t^n}{n!}\right)\left(\sum_{n=0}^{+\infty} x^n \frac{t^n}{n!}\right) \\ &= \sum_{n=0}^{+\infty}\left(\sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k}\right)\frac{t^n}{n!}. \end{aligned}$$

Así, la multiplicación como series formales induce la siguiente definición:

Definición 1.11. *El n-ésimo **polinomio de Bernoulli** se define como:*

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k}.$$

Observación 1.12. *Los polinomios de Bernoulli $B_n(x)$ con $n \geq 0$, son polinomios en la variable x con coeficientes racionales. Como $B_0 = 1$, $B_n(x)$ es un polinomio de grado n. Algunos de ellos son:*

$$B_0(x) = 1,\ B_1(x) = x - \frac{1}{2},\ B_2(x) = x^2 - x + \frac{1}{6},\ \cdots$$

Observación 1.13. *Al hacer $x = 0$, obtenemos $B_k(0) = B_k$.*

Observación 1.14.

$$s_k(n) = \frac{1}{k+1}\left(B_{k+1}(n) - B_{k+1}\right);$$

ya que por (1.2) y la Definición 1.11, tenemos que:

$$(k+1)s_k(n) = \sum_{i=0}^{k} \binom{k+1}{i} B_i n^{k+1-i}, \quad y \quad B_{k+1}(n) = \sum_{i=0}^{k} \binom{k+1}{i} B_i n^{k+1-i} + B_{k+1}.$$

[1]En esta definición tenemos que $B_1 = -1/2$; sin embargo, en varias referencias, en particular Iwasawa (ver [14]) toma a B_1 con signo positivo. En esta tesina, seguimos tomando el signo negativo para el número de Bernoulli B_1.

El siguiente teorema da explícimatamente una fórmula para los números de Bernoulli generalizados en términos de los polinomios de Bernoulli. Fórmula de vital importancia en la construcción de las funciones L p-ádicas; ya que de esta se desprende la idea utilizada para su definición, la cual involucra los valores que toman las funciones L de Dirichlet clásicas en los enteros negativos.

Teorema 1.15. *Sea χ carácter de Dirichlet de conductor $f > 1$, si $f|F$ con $F \in \mathbb{Z}_+$, entonces:*

$$B_{n,\chi} = F^{n-1} \sum_{a=1}^{F} \chi(a) B_n(a/F). \tag{1.12}$$

Demostración. Reemplazando x por a/F y t por Ft en (1.11), entonces:

$$\frac{Fte^{\left(\frac{a}{F}\right)Ft}}{e^{Ft}-1} = \sum_{n=0}^{+\infty} B_n(a/F)\frac{(Ft)^n}{n!};$$

esto es:

$$\frac{te^{at}}{e^{Ft}-1} = \frac{1}{F}\sum_{n=0}^{+\infty} B_n(a/F)\frac{(Ft)^n}{n!}.$$

Luego:

$$\begin{aligned}\sum_{a=1}^{F} \frac{\chi(a)te^{at}}{e^{Ft}-1} &= \sum_{a=1}^{F}\chi(a)\frac{1}{F}\sum_{n=0}^{+\infty} B_n(a/F)\frac{(Ft)^n}{n!} \\ &= \sum_{n=0}^{+\infty}\left(F^{n-1}\sum_{a=1}^{F}\chi(a)B_n(a/F)\right)\frac{t^n}{n!}.\end{aligned}$$

Donde hemos realizado intercambios del signo sumatorio ya que las series son convergentes (ver [8], Teorema 7.5). Por otro lado, sea $g = F/f$ y $a = b + cf$, $1 \leq b \leq f$, entonces:

$$\begin{aligned}\sum_{a=1}^{F} \frac{\chi(a)te^{at}}{e^{Ft}-1} &= \sum_{b=1}^{f}\sum_{c=0}^{g-1}\chi(b)\frac{te^{(b+cf)t}}{e^{gft}-1} \\ &= \sum_{b=1}^{f}\chi(b)\frac{te^{bt}}{e^{gft}-1}\sum_{c=0}^{g-1}e^{cft} \\ &= \sum_{b=1}^{f}\chi(b)\frac{te^{bt}}{e^{ft}-1} \\ &= \sum_{n=0}^{+\infty} B_{n,\chi}\frac{t^n}{n!}.\end{aligned}$$

Donde la última igualdad se obtiene por la Definición 1.10. Por último, comparando coeficientes obtenemos el resultado requerido.

□

Observación 1.16. *Si $\chi = \chi_1$ es el carácter principal de conductor $f = 1$, entonces:*

$$F_{\chi_1}(t) = F(t)e^t \implies B_{n,\chi_1} = B_n \ \forall\ n \neq 1.$$

Es de notar que la función:

$$F(t)e^t = \frac{te^t}{e^t - 1},$$

también es utilizada para la definición de los números de Bernoulli, como en el caso de Iwasawa (ver [14]). Aunque, con esta función tenemos que $B_1 = 1/2$.

Observación 1.17. *Sea* χ *carácter de Dirichlet de conductor* f*, y sea:*

$$F_\chi(t,x) = F_\chi(t)e^{xt} = \sum_{a=1}^{f} \frac{\chi(a)te^{(a+x)t}}{e^{ft}-1}.$$

Haciendo una expansión en serie de potencias en la variable t*, tenemos que:*

$$F_\chi(t,x) = \sum_{n=0}^{+\infty} B_{n,\chi}(x)\frac{t^n}{n!};$$

procediendo de manera análoga como se hizo con la función $F(t)$*, podemos obtener:*

$$F_\chi(t,x) = \sum_{n=0}^{+\infty}\left(\sum_{k=0}^{n}\binom{n}{k}B_{k,\chi}x^{n-k}\right)\frac{t^n}{n!}.$$

Lo anterior nos sugiere la siguiente definición:

Definición 1.18. *Sea* χ *carácter de Dirichlet de conductor* f*, definimos el* ***polinomio de Bernoulli generalizado*** *como sigue:*

$$B_{n,\chi}(x) = \sum_{k=0}^{n}\binom{n}{k}B_{k,\chi}x^{n-k}.$$

Observación 1.19. *Algunas propiedades de* $B_{n,\chi}$ *y* $B_{n,\chi}(x)$ *son:*

(i) $B_{n,\chi}(0) = B_{n,\chi}$ *para todo* $n \geq 0$, $n \in \mathbb{Z}$;

(ii)

$$B_{0,\chi} = \frac{1}{f}\sum_{a=1}^{f}\chi(a) = 0, \quad si\ \chi \neq \chi_1.$$

Lo anterior por el Teorema B.13 (iii). Por lo tanto, el grado del polinomio $B_{n,\chi}(x)$ *es menor a* n*, i.e.,* $gr(B_{n,\chi}(x)) < n$*, si* $\chi \neq \chi_1$.

Teorema 1.20. *Sea χ carácter de Dirichlet de conductor f, entonces para $n \geq 0$, tenemos que:*

$$(-1)^n B_{n,\chi}(-x) = \chi(-1) B_{n,\chi}(x),$$

además:

$$B_{n,\chi} = 0 \quad \text{para } n \geq 1 \text{ y } n \not\equiv \delta_\chi \pmod 2.$$

Donde δ_χ es definido en el Apéndice B, observación B.11.

Demostración. Dado que:

$$\begin{aligned} F_\chi(-t,-x) &= \sum_{a=1}^{f} \frac{\chi(a)(-t)e^{-(a-x)t}}{e^{-ft}-1} \\ &= \sum_{a=1}^{f} \frac{\chi(a)te^{(f-a+x)t}}{e^{ft}-1} \\ &= \chi(-1)\sum_{a=1}^{f} \frac{\chi(f-a)te^{(f-a+x)t}}{e^{ft}-1} \\ &= \chi(-1)F_\chi(t,x) \quad \text{si } \chi \neq \chi_1. \end{aligned}$$

Por otro lado:

$$F_\chi(-t,-x) = \sum_{n=0}^{+\infty} (-1)^n B_{n,\chi}(-x)\frac{t^n}{n!},$$

y de la identidad $F_\chi(-t,-x) = \chi(-1)F_\chi(t,x)$ si $\chi \neq \chi_1$, tenemos que:

$$F_\chi(-t,-x) = \sum_{n=0}^{+\infty} \chi(-1)B_{n,\chi}(x)\frac{t^n}{n!}.$$

Por último, igualando coeficientes obtenemos que:

$$(-1)^n B_{n,\chi}(-x) = \chi(-1)B_{n,\chi}(x), \quad n \geq 0;$$

como se quería. Al hacer $x = 0$ en la identidad anterior, obtenemos el segundo resultado. □

Observación 1.21. *Tenemos hasta el momento ciertos valores muy útiles para calcular números de Bernoulli:*

(i) Si $\chi = \chi_1$ el carácter principal, entonces:

$$\begin{aligned} &B_0 = 1, && B_n \neq 0 \quad \text{para enteros pares } n \geq 2 \\ &B_1 = -1/2, && B_n = 0 \quad \text{para enteros impares } n \geq 3. \end{aligned}$$

(ii) Si $\chi \neq \chi_1$, tenemos que:

$$\begin{aligned} &B_{0,\chi} = 0, \\ &B_{n,\chi} = 0, \quad \text{para } n \geq 1, \quad n \not\equiv \delta_\chi \pmod 2. \end{aligned}$$

Como en el caso (i), podemos tener un análogo al caso $B_n \neq 0$ para $n \geq 2$ par, el cual es:

$$B_{n,\chi} \neq 0 \quad \text{para } n \geq 1, \quad n \equiv \delta_\chi \pmod 2,$$

en cuya justificación necesitamos la no nulidad de las funciones L de Dirichlet en los puntos del plano con parte real mayor o igual a 1 (ver Observación 3.24).

(iii) Si χ es carácter de Dirichlet de conductor f. Para $f|F$, con $F \in \mathbb{Z}_+$ se cumple que:

$$B_{n,\chi} = F^{n-1} \sum_{a=1}^{F} \chi(a) B_n(a/F).$$

1.3. Congruencias de Kummer I

Nuestro objetivo ahora es derivar las congruencias de Kummer y sentar las bases para la interpolación p-ádica de la función zeta de Riemman, cuyos conceptos se usan en la definición de las funciones L p-ádicas. Es conveniente para entender completamente esta sección ir de la mano con una lectura del Apéndice C.

Lema 1.22. *Sea p número primo. Entonces pB_k es p-entero, i.e., $pB_k \in \mathbb{Z}_{(p)}$ para todo p-primo (Ver Apéndice C. Definición C.22).*

Demostración. Demostremos por inducción completa sobre k. Si $k = 1$, entonces $pB_1 = -p/2$; por tanto tenemos dos opciones: si $p = 2$, entonces $pB_1 = -1 \in \mathbb{Z}_{(p)}$; por otro lado, si $p \geq 3$, entonces $p \nmid 2$; luego $pB_1 \in \mathbb{Z}_{(p)}$, (ver Apéndice C. Teorema C.23 (i)).

Supongamos cierto para $j \in \mathbb{Z}_+$ tal que $1 \leq j < k$, i.e., $pB_j \in \mathbb{Z}_{(p)}$. Demostremos que es cierto para k, sea $n = p$ en (1.3), entonces:

$$s_k(p) = \sum_{i=0}^{k} \binom{k}{i} \frac{p^{i+1}}{i+1} B_{k-i};$$

por lo tanto:

$$s_k(p) = pB_k + \sum_{i=1}^{k} \binom{k}{i} \frac{p^i}{i+1} (pB_{k-i}).$$

Dado que $p^i \geq 2^i \geq i+1$, vemos que $\nu_p(\frac{p^i}{i+1}) \geq 0$ (ver Apéndice C. Definición C.5), esto es $p^i/(i+1) \in \mathbb{Z}_{(p)}$; luego, por hipótesis de inducción cada uno de los pB_{k-i} es p-entero; además, como $\mathbb{Z}_{(p)}$ es un anillo y se cumple que $s_k(n) \in \mathbb{Z} \subset \mathbb{Z}_{(p)}$ y finalmente $\binom{k}{i} \in \mathbb{Z} \subset \mathbb{Z}_{(p)}$, entonces:

$$s_k(p) - \sum_{i=1}^{k} \binom{k}{i} \frac{p^i}{i+1} (pB_{k-i}) = pB_k \in \mathbb{Z}_{(p)},$$

como se quería demostrar.

□

Corolario 1.23. *Sea $B_k = U_k/V_k$ con $m.c.d(U_k, V_k) = 1$, entonces V_k es libre de cuadrados.*

Demostración. Si $p^2|V_k$ para algún primo p, entonces pB_k todavía posee un factor p en su denominador, lo cual implica que $pB_k \notin \mathbb{Z}_{(p)}$. Esto contradice el lema anterior.

□

Podemos refinar el argumento del lema anterior utilizando la relación de equivalencia que definimos en $\mathbb{Q}_p$ el campo de los números p-ádicos (ver Apéndice C. Lema C.26).

Lema 1.24. *Si $k \geq 2$ es entero par, entonces:*

$$pB_k \equiv s_k(p) \ (mód\ p).$$

Demostración. Si $k \geq 4$ es entero par, entonces $k-1 \geq 3$ es entero impar; por tanto $B_{k-1} = 0$ y asi:

$$\begin{aligned} s_k(p) &= \sum_{i=0}^{k} \binom{k}{i} \frac{p^{i+1}}{i+1} B_{k-i} \\ &= pB_k + k\frac{p^2}{2} B_{k-1} + p\sum_{i=2}^{k} \binom{k}{i} \frac{p^{i-1}}{i+1}(pB_{k-i}); \end{aligned}$$

por lo tanto:

$$s_k(p) = pB_k + p\sum_{i=2}^{k} \binom{k}{i} \frac{p^{i-1}}{i+1}(pB_{k-i}).$$

Afirmamos que $\nu_p\left(\frac{p^{i-1}}{i+1}\right) \geq 0$ para $i \geq 2$; en efecto, para $p = 2$ tenemos que si $i = 2$, entonces $\frac{2^{i-1}}{i+1} = \frac{2}{3}$; de modo que $\nu_2\left(\frac{2^{i-1}}{i+1}\right) \geq 0$. Si $i > 2$, entonces $2^{i-1} \geq i+1$, y así $\nu_2\left(\frac{2^{i-1}}{i+1}\right) \geq 0$.

Por otro lado, si p es primo con $p > 2$, entonces $p^{i-1} \geq 3^{i-1} \geq i+1$ siempre que $i \geq 2$. Luego, $\nu_p\left(\frac{p^{i-1}}{i+1}\right) \geq 0$; por lo tanto $p^{i-1}/(i+1)$ es p-entero. Y así, junto al lema anterior sabemos que $pB_{k-i} \in \mathbb{Z}_{(p)}$, debido a lo cual obtenemos:

$$\begin{aligned} \nu_p(s_k(p) - pB_k) &= \nu_p\left(p\sum_{i=2}^{k} \binom{k}{i} \frac{p^{i-1}}{i+1}(pB_{k-i})\right) \\ &= \nu_p(p) + \nu_p\left(\sum_{i=2}^{k} \binom{k}{i} \frac{p^{i-1}}{i+1}(pB_{k-i})\right) \\ &\geq 1 + \text{mín}\left\{\nu_p\left(\binom{k}{i} \frac{p^{i-1}}{i+1}(pB_{k-i})\right)\right\}_{i=2}^{k} \geq 1; \end{aligned}$$

con lo cual:

$$s_k(p) \equiv pB_k \ (\text{mód}\ p) \ \text{ si } k \geq 4.$$

Si $k = 2$ sabemos que $B_2 = 1/6$, entonces para p-primo:

$$s_2(p) = \frac{1}{6}[p(p-1)(2p-1)] \ \text{ y } \ pB_2 = \frac{p}{6}.$$

Entonces:

$$\begin{aligned} \nu_p(s_2(p) - pB_2) &= \nu_p\left(\frac{p}{6}[(p-1)(2p-1)-1]\right) \\ &= \nu_p(p/6) + \nu_p(2p^2 - 3p) \\ &= \nu_p(p) - \nu_p(6) + \nu_p(p) + \nu_p(2p-3) \\ &= 2 + \nu_p(2p-3) - \nu_p(6) \\ &\geq 2 - \nu_p(6) \geq 1 \ \ \forall\ p\text{-primo}; \end{aligned}$$

por lo tanto $s_2(p) \equiv pB_2 \pmod{p}$.

□

También tenemos el siguiente resultado elemental.

Lema 1.25. *Si* $(p-1) \nmid k$, *entonces* $s_k(p) \equiv 0 \pmod{p}$. *Por otro lado, si* $(p-1)|k$, *entonces* $s_k(p) \equiv -1 \pmod{p}$.

Demostración. Sea g raíz primitiva módulo p. Entonces, si $(p-1) \nmid k$:

$$s_k(p) \equiv \sum_{j=0}^{p-2} (g^j)^k = \frac{g^{k(p-1)} - 1}{g^k - 1} \pmod{p};$$

en consecuencia:

$$\nu_p\left(s_k(p) - \frac{g^{k(p-1)} - 1}{g^k - 1}\right) \geq 1.$$

Por otro lado, el pequeño Teorema de Fermat asegura que $g^{p-1} \equiv 1 \pmod{p}$; con lo cual $g^{k(p-1)} \equiv 1 \pmod{p}$, debido a lo cual $\nu_p(g^{k(p-1)} - 1) \geq 1$. Ahora bien, si $g^k \equiv 1 \pmod{p}$ por Teorema 10.1 en [1], obtenemos que $k \equiv 0 \pmod{p-1}$, i.e., $(p-1)|k$ lo cual es contradictorio; por consiguiente $p \nmid (g^k - 1)$ esto implica que $\nu_p(g^k - 1) = 0$, luego:

$$\nu_p\left(\frac{g^{k(p-1)} - 1}{g^k - 1}\right) = \nu_p(g^{k(p-1)} - 1) - \nu_p(g^k - 1) = \nu_p(g^{k(p-1)} - 1) \geq 1.$$

De lo anterior concluimos que:

$$\begin{aligned}\nu_p(s_k(p)) &= \nu_p\left(s_k(p) - \frac{g^{k(p-1)} - 1}{g^k - 1} + \frac{g^{k(p-1)} - 1}{g^k - 1}\right) \\ &\geq \min\left\{\nu_p\left(s_k(p) - \frac{g^{k(p-1)} - 1}{g^k - 1}\right), \nu_p\left(\frac{g^{k(p-1)} - 1}{g^k - 1}\right)\right\} \geq 1;\end{aligned}$$

esto es, $s_k(p) \equiv 0 \pmod{p}$.

En el caso que $(p-1)|k$; luego $k = (p-1)q$ con $q \in \mathbb{Z}$, de manera que:

$$s_k(p) = \sum_{i=1}^{p-1} i^k = \sum_{i=1}^{p-1} (i^{p-1})^q.$$

Por el pequeño Teorema de Fermat $i^{p-1} \equiv 1 \pmod{p}$, entonces $i^k \equiv 1 \pmod{p}$, de lo anterior obtenemos que:

$$s_k(p) \equiv p - 1 \equiv -1 \pmod{p}.$$

□

A continuación presentamos el famoso Teorema de von Staudt-Clausen. Este resultado fue demostrado de manera independiente por el astrónomo y matemático danés Thomas Clausen (1801–1885) y el matemático alemán Karl Georg Christian von Staudt (1798–1867), (ver [6] y [25]).

Teorema 1.26. ***von Staudt-Clausen****. Para k entero par mayor o igual a 0, tenemos que:*

$$B_k + \sum_{(p-1)|k} \frac{1}{p} \in \mathbb{Z}$$

Demostración. Si $(p-1) \nmid k$, el Lema 1.25 implica que $s_k(p) \equiv 0 \pmod{p}$, luego por Lema 1.24, $pB_k \equiv 0 \pmod{p}$, por lo tanto $\nu_p(pB_k) \geq 1$, así $\nu_p(pU_k) - \nu_p(V_k) \geq 1$, por lo que:

$$\nu_p(V_k) \leq \nu_p(pU_k) - 1 = \nu_p(p) + \nu_p(U_k) - 1 = \nu_p(U_k).$$

Por lo visto, tenemos que $\nu_p(B_k) \geq 0$, i.e., $B_k \in \mathbb{Z}_{(p)}$ y así $p \nmid V_k$.

Si $(p-1)|k$, entonces por el Lema 1.25, $s_k(p) \equiv -1 \pmod{p}$, luego por el Lema 1.24 tenemos que $pB_k \equiv -1 \pmod{p}$. Supongamos que $p \nmid V_k$, entonces $\nu_p(V_k) = 0$, de lo que se sigue que $\nu_p(pB_k) = \nu_p(p) + \nu_p(B_k) = 1 + \nu_p(U_k) \geq 1$, por lo tanto $pB_k \equiv 0 \pmod{p}$, lo anterior implica que $0 \equiv -1 \pmod{p}$, lo cual es contradictorio. Concluimos entonces que $p|V_k$.

En consecuencia, los primos que dividen a V_k son todos los primos p tales que $(p-1)|k$. Entonces;

$$B_k + \frac{1}{p} = \frac{pB_k + 1}{p} \in \mathbb{Z}_{(p)} \quad \forall\ p\text{-primo tal que } (p-1)|k,$$

y como $1/q \in \mathbb{Z}_{(p)}$ para todo q-primo, con $q \neq p$, por tal motivo tenemos que:

$$B_k + \sum_{\substack{(q-1)|k \\ q\text{-primo}}} \frac{1}{q} \in \mathbb{Z}_{(p)}.$$

Por esta razón, se sigue que:

$$B_k + \sum_{\substack{(q-1)|k \\ q-\text{primo}}} \frac{1}{q} \in \mathbb{Z}_{(p)} \quad \forall\ p\text{-primo con } (p-1)|k.$$

Si p es primo tal que $(p-1) \nmid k$ entonces $p \nmid V_k$, y así $B_k \in \mathbb{Z}_{(p)}$ y los q-primos en el denomidador de

$$\sum_{\substack{(q-1)|k \\ q-\text{primo}}} \frac{1}{q},$$

son diferentes de p, entonces

$$\sum_{\substack{(q-1)|k \\ q-\text{primo}}} \frac{1}{q} \in \mathbb{Z}_{(p)}.$$

De lo anterior y por la Observación C.24

$$B_k + \sum_{(p-1)|k} \frac{1}{p} \in \mathbb{Z}$$

□

Observación 1.27. *Es sugerente pensar que los B_k tienen "polos simples" en los primos p tales que $(p-1)|k$ y la suma en el teorema anterior puede ser vista como la parte "polar" de B_k. También notamos que $6|V_k$ para todo $k \geq 2$ entero par.*

Teorema 1.28. *Sea $k \geq 2$ entero par. Entonces*

$$V_k s_k(n) \equiv U_k n \ (\textit{mód}\ n^2) \quad \forall\ n \geq 1.$$

Demostración. Como antes, de la fórmula de Bernoulli para $s_k(n)$ tenemos

$$s_k(n) = B_k n + \sum_{i=1}^{k} \binom{k}{i} B_{k-i} \frac{n^{i+1}}{i+1}. \tag{1.13}$$

Sea $k = 2\kappa$ con $\kappa \in \mathbb{Z}_+$, como $B_{k-i} = 0$ si $k-i$ es impar mayor o igual a 3. Por tal motivo, si $i = 2j$ con $j \in \mathbb{Z}_+$, tenemos que (1.13) se convierte en

$$s_{2\kappa}(n) = B_{2\kappa} n + \sum_{j=1}^{\kappa} \binom{2\kappa}{2j} \frac{1}{2j+1} B_{2(\kappa-j)} n^{2j+1} \tag{1.14}$$

entonces, al multiplicar (1.14) por $V_{2\kappa}$, obtenemos

$$V_{2\kappa} s_{2\kappa}(n) - U_{2\kappa} n = \left(\sum_{j=1}^{\kappa} \binom{2\kappa}{2j} \frac{V_{2\kappa}}{2j+1} B_{2(\kappa-j)} n^{2j-1} \right) n^2.$$

Deseamos probar que el lado derecho es un entero múltiplo de n^2. Par hacer esto, sea

$$V_{2\kappa} \frac{B_{2(\kappa-j)}}{2j+1} n^{2j-1} = \frac{c_j}{d_j}, \quad j = 1, 2, ..., \kappa,$$

con $c_j, d_j \in \mathbb{Z}$ y m.c.d$(c_j, d_j) = 1$. Probaremos que m.c.d$(d_j, n) = 1$. Sea

$$A = d_j V_{2\kappa} U_{2(\kappa-j)} n^{2j-1} \quad \text{y} \quad A' = c_j (2j+1) V_{2(\kappa-j)},$$

en consecuencia $A = A'$.

Si p es un primo tal que $p|d_j$ y $p|n$ entonces $p^{2j}|A$ y también $p^{2j}|A'$. Por otro lado, $p \nmid c_j$ ya que m.c.d$(d_j, c_j) = 1$. Dado que $p^2 \nmid V_{2(\kappa-j)}$, tenemos necesariamente que $p|(2j+1)$, por lo tanto $p \neq 2$. Ahora escribiendo $2j+1 = p^a r$, con $p \nmid r$ y $a \geq 1$, notamos que $\nu_p(V_{2(\kappa-j)}) = 1$, ya que si $p \nmid V_{2(\kappa-j)}$, entonces $a \geq 2j$, esto implica que $2j+1 = p^a r \geq p^{2j} r \geq p^{2j}$, lo cual es absurdo. Tomando entonces la valuación p-ádica de A y A' tenemos que

$$2j = 1 + (2j-1) \leq \nu_p(A) = \nu_p(A') = \nu_p(2j+1) + 1,$$

de manera que

$$p^a - 2 \leq p^a r - 2 = 2j - 1 \leq \nu_p(2j+1) = a,$$

luego

$$p^a \leq a + 2. \tag{1.15}$$

Analicemos ahora que sucede si $p > 3$ con $a \geq 1$, entonces

$$p^a > 3^a = (1+2)^a \geq 1 + 2a = 1 + a + a \geq a + 2,$$

esto es, $p^a > a + 2$, entonces por la desigualdad (1.15), tenemos una contradicción. Si $p = 3$ y $a > 1$, entonces

$$3^a = (1+2)^a \geq 1 + 2a = 1 + a + a \geq a + 3,$$

esto es, $3^a \geq a+2$, entonces por la desigualdad (1.15), tenemos que $a+2 \geq 3^a \geq a+3$, lo que implica que $2 \geq 3$, que es absurdo. Por último, si $p = 3$ y $a = 1$, sabemos que $3|V_{2\kappa}$ y $3|V_{2(\kappa-j)}$ entonces,

$$3 \leq 2j + 1 = 1 + 1 + (2j-1) \leq \nu_3(A) = \nu_3(A') = \nu_3(2j+1) + 1 = 2,$$

donde concluimos que $3 \leq 2$, un absurdo. Entonces, hemos demostrado que

$$V_{2\kappa} s_{2\kappa}(n) - U_{2\kappa} n = \frac{x}{y} n^2,$$

donde $x, y, z \in \mathbb{Z}$ y m.c.d(n, y) =m.c.d$(x, y) = 1$. Luego como $n^2 \frac{x}{y} \in \mathbb{Z}$ esto implica que $y = 1$, con lo cual

$$V_{2\kappa} s_{2\kappa}(n) \equiv U_{2\kappa} n \ (\text{mód } n^2) \implies V_k s_k(n) \equiv U_k n \ (\text{mód } n^2).$$

□

Ahora deduciremos las congruencias de Voronoi, de las cuales se siguen las congruencias de Kummer. Tal parece que Voronoi probó estas congruencias en 1889 mientras era un estudiante.

Teorema 1.29. ***Congruencias de Voronoi -1889-.*** *Sea $n \in \mathbb{N}$ y m.c.d$(a, n) = 1$. Entonces,*

$$(a^k - 1) s_k(n) \equiv kna^{k-1} \sum_{j=1}^{n-1} \left[\frac{ja}{n}\right] j^{k-1} \ (mód\ n^2) \ \ \forall\ k \in \mathbb{Z}_+.$$

Demostración. Para cada j con $1 \leq j < n$, escribimos $ja = q_j n + r_j$ donde $0 \leq r_j < n$ (algoritmo de la división). Entonces $q_j = [ja/n]$ y tenemos

$$(ja)^k \equiv r_j^k + kq_j n r_j^{k-1} \ (\text{mód } n^2),$$

ya que por teorema del binomio

$$(ja)^k = (q_j n + r_j)^k = r_j^k + kq_j n r_j^{k-1} + \binom{k}{2} q_j^2 n^2 r_j^{k-2} + \cdots + q_j^k n^k,$$

entonces

$$(ja)^k - (r_j^k + kq_jnr_j^{k-1}) = \left[\binom{k}{2}q_j^2r_j^{k-2} + \cdots + q_j^kn^{k-2}\right]n^2.$$

Por otra parte, dado que $r_j = ja - q_jn$, tenemos

$$r_j^{k-1} = (ja)^{k-1} - (k-1)(q_jn)(ja)^{k-2} + \binom{k-1}{2}(q_jn)^2(ja)^{k-3} - \cdots + (-1)^{k-1}(q_jn)^{k-1},$$

luego,

$$kq_jnr_j^{k-1} = kq_jn(ja)^{k-1} + \left[-k(k-1)q_j^2n(ja)^{k-2} + \sum_{i=2}^{k-1}(-1)^i\binom{k-1}{i}kq_j^{i+1}n^{i-1}(ja)^{k-1-i}\right]n^2,$$

con lo cual

$$(ja)^k \equiv r_j^k + kq_jn(ja)^{k-1} \text{ (mód } n^2).$$

Dado que j recorre a los enteros de 1 a $n-1$, también lo hace r_j, ya que m.c.d$(a,n) = 1$. En consecuencia, sumando las congruencias anteriores desde $j = 1$ a $n-1$ obtenemos

$$\sum_{j=1}^{n-1}(ja)^k \equiv \sum_{j=1}^{n-1}\left(r_j^k + kq_jn(ja)^{k-1}\right) \text{ (mód } n^2),$$

entonces

$$a^k\sum_{j=1}^{n-1}j^k \equiv \sum_{j=1}^{n-1}r_j^k + kn\sum_{j=1}^{n-1}q_j(ja)^{k-1} \text{ (mód } n^2),$$

luego

$$a^ks_k(n) \equiv s_k(n) + kna^{k-1}\sum_{j=1}^{n-1}\left[\frac{ja}{n}\right]j^{k-1} \text{ (mód } n^2),$$

así pues

$$(a^k-1)s_k(n) \equiv kna^{k-1}\sum_{j=1}^{n-1}\left[\frac{ja}{n}\right]j^{k-1} \text{ (mód } n^2)$$

□

Corolario 1.30. *Si $k \geq 2$ es entero par entonces*

$$(a^k-1)U_k \equiv kV_ka^{k-1}\sum_{j=1}^{n-1}\left[\frac{ja}{n}\right]j^{k-1} \text{ (}mód\ n\text{)} \tag{1.16}$$

Demostración. Por el Teorema 1.28 tenemos que para $k \geq 2$, entero par. y $n \geq 1$:

$$V_k s_k(n) \equiv U_k n \ (\text{mód } n^2),$$

y por el Teorema 1.29 (Voronoi), tenemos que para $n \geq 1$ y m.c.d$(a, n) = 1$, se cumple que:

$$(a^k - 1)s_k(n) \equiv kna^{k-1} \sum_{j=1}^{n-1} \left[\frac{ja}{n}\right] j^{k-1} \ (\text{mód } n^2).$$

Luego

$$V_k s_k(n) - U_k n = q_1 n^2, \text{ con } q_1 \in \mathbb{Z}$$

al multiplicar por $(a^k - 1)$, tenemos

$$V_k(a^k - 1)s_k(n) - (a^k - 1)U_k n = q_2 n^2, \text{ con } q_2 \in \mathbb{Z}, \tag{1.17}$$

por otro lado, tenemos que

$$(a^k - 1)s_k(n) - kna^{k-1} \sum_{j=1}^{n-1} \left[\frac{ja}{n}\right] j^{k-1} = q_3 n^2, \text{ con } q_3 \in \mathbb{Z},$$

luego, reemplazando en (1.17) tenemos

$$V_k \left(kna^{k-1} \sum_{j=1}^{n-1} \left[\frac{ja}{n}\right] j^{k-1} + q_3 n^2 \right) - (a^k - 1)U_k n = q_2 n^2,$$

entonces

$$\left(kV_k a^{n-1} \sum_{j=1}^{n-1} \left[\frac{ja}{n}\right] - (a^k - 1)U_k \right) n = (q_2 - V_k q_3)n^2.$$

De donde se tiene el teorema.

□

Seguimos ahora con el siguiente teorema, el cual debe su nombre al matemático y astrónomo inglés John Couch Adams (1819-1892), famoso por encontrar matemáticamente al planeta Neptuno.

Teorema 1.31. ***Congruencias de Adams -1878-.*** *Si $(p-1) \nmid k$, entonces $\frac{B_k}{k}$ es p-entero, i.e., si $(p-1) \nmid k$, entonces $\frac{B_k}{k} \in \mathbb{Z}_{(p)}$.*

Demostración. Sea $\nu_p(k) = t$, para algún $t \in \mathbb{Z}_+$, entonces por Corolario 1.30 con $n = p^t$, deducimos que $(a^k - 1)U_k \equiv 0 \ (\text{mód } p^t)$. Sea a una raíz primitiva módulo p, podemos asegurar que p es primo relativo a $a^k - 1$, ya que si $p|(a^k - 1)$ entonces $a^k \equiv 1 \ (\text{mód } p)$ y por el Teorema 10.1 en [1] tenemos $k \equiv 0 \ (\text{mód } p-1)$, lo cual es contradictorio. Luego $U_k \equiv 0 \ (\text{mód } p^t)$, por otro lado dado que por Teorema 1.26 $p \nmid V_k$ por lo tanto

$$\nu_p(B_k/k) = \nu_p(U_k) - \nu_p(k) - \nu_p(V_k) = \nu_p(U_k) - \nu_p(k) \geq t - t = 0.$$

□

Teorema 1.32. ***Congruencia de Kummer -1851-.*** *Sea $k \geq 2$ entero par, p-primo tal que $(p-1) \nmid k$. Si $k \equiv k'$ (mód $\varphi(p^e)$), donde φ es la función phi de Euler, entonces*

$$(1-p^{k-1})\frac{B_k}{k} \equiv (1-p^{k'-1})\frac{B_{k'}}{k'} \ (mód\ p^e)$$

Demostración. Sea $t = \nu_p(k)$, luego $k = p^t r$ con $p \nmid r$ y escribimos $B_k = U_k/V_k$ como antes. En (1.16) tomamos $n = p^{e+t}$ y así

$$(a^k-1)U_k \equiv kV_k a^{k-1} \sum_{j=1}^{p^{e+t}-1} \left[\frac{ja}{p^{e+t}}\right] j^{k-1} \ (\text{mód } p^{e+t}).$$

Dado que $(p-1) \nmid k$, entonces m.c.d$(p, V_k) = 1$ por el Teorema 1.26 de von Staudt-Clausen. Luego

$$(a^k-1)\frac{B_k}{k} \equiv a^{k-1} \sum_{j=1}^{p^{e+t}-1} \left[\frac{ja}{p^{e+t}}\right] j^{k-1} \ (\text{mód } p^e), \tag{1.18}$$

en efecto,

$$(a^k-1)U_k - kV_k a^{k-1} \sum_{j=1}^{p^{e+t}-1} \left[\frac{ja}{p^{e+t}}\right] j^{k-1} = qp^{e+t}, \quad q \in \mathbb{Z},$$

al dividir entre $kV_k \neq 0$ tenemos

$$(a^k-1)\frac{B_k}{k} - a^{k-1} \sum_{j=1}^{p^{e+t}-1} \left[\frac{ja}{p^{e+t}}\right] j^{k-1} = \frac{q}{kV_k}p^{e+t} = \frac{q}{p^t r V_k} = \frac{q}{rV_k}p^e,$$

y como $\nu_p(qp^e/rV_k) = \nu_p(qp^e) - \nu_p(rV_k) = e + \nu_p(q) \geq e$.

Empezamos con el caso $e = 1$. En el lado derecho de la congruencia anterior podemos omitir los j's divisibles por p ya que $e = 1$. Dado que $k \equiv k'$ (mód $p-1$), entonces $j^{k-1} \equiv j^{k'-1}$ (mód p) con m.c.d$(j, p) = 1$, en efecto, $k - k' = (p-1)q$ con $q \in \mathbb{Z}$, sin pérdida de generalidad sea $k \geq k'$, por el pequeño teorema de Fermat:

$$\begin{aligned} j^{p-1} \equiv 1 \ (\text{mód } p) &\implies j^{(p-1)q} \equiv 1 \ (\text{mód } p) \\ &\implies j^{k-k'} \equiv 1 \ (\text{mód } p) \\ &\implies j^k \equiv j^{k'} \ (\text{mód } p), \end{aligned}$$

de tal manera que $j^{k-1} \equiv j^{k'-1}$ (mód p). Tomando a una raíz primitiva módulo p, entonces

$$\begin{aligned} a^{k-1} \sum_{j=1}^{p^{t+1}-1} \left[\frac{ja}{p^{t+1}}\right] j^{k-1} &\equiv a^{k'-1} \sum_{j=1}^{p^{t+1}-1} \left[\frac{ja}{p^{t+1}}\right] j^{k'-1} \ (\text{mód } p) \\ &\equiv (a^{k'}-1)\frac{B_{k'}}{k'} \ (\text{mód } p), \end{aligned}$$

en vista de ello,

$$\begin{aligned}(a^k-1)\frac{B_k}{k} &\equiv (a^{k'}-1)\frac{B_{k'}}{k'} \pmod p\\ &\equiv (a^k-1)\frac{B'_k}{k'} \pmod p.\end{aligned}$$

Luego

$$\frac{B_k}{k} \equiv \frac{B_{k'}}{k'} \pmod p.$$

Cuando $e>1$, escribimos

$$\sum_{j=1}^{p^{e+t}-1}\left[\frac{ja}{p^{e+t}}\right]j^{k-1} = \sum_{\substack{j=1\\ \text{m.c.d}(j,p)=1}}^{p^{e+t}-1}\left[\frac{ja}{p^{e+t}}\right]j^{k-1} + p^{k-1}\sum_{j=1}^{p^{e+t-1}-1}\left[\frac{ja}{p^{e+t-1}}\right]j^{k-1}, \tag{1.19}$$

ya que $\varphi(p^{e+t}) = p^{e+t-1}(p-1)$.

La congruencia (1.18) con $e-1$ en lugar de e, nos da para $k\geq 2$ lo siguiente

$$(a^k-1)\frac{B_k}{k} \equiv a^{k-1}\sum_{j=1}^{p^{e+t-1}-1}\left[\frac{ja}{p^{e+t-1}}\right]j^{k-1} \pmod{p^{e-1}},$$

entonces

$$p^{k-1}(a^k-1)\frac{B_k}{k} \equiv a^{k-1}p^{k-1}\sum_{j=1}^{p^{e+t-1}-1}\left[\frac{ja}{p^{e+t-1}}\right]j^{k-1} \pmod{p^{e-1}}.$$

Sea

$$x = (a^k-1)\frac{B_k}{k} - a^{k-1}\sum_{j=1}^{p^{e+t-1}-1}\left[\frac{ja}{p^{e+t-1}}\right]j^{k-1},$$

y supongamos que $k-1+\nu_p(x) = e-1$, entonces $k+\nu_p(x)=e$, según esto $e\geq k+e-1$, esto es $k\leq 1$, lo cual es contradictorio. Así

$$p^{k-1}(a^k-1)\frac{B_k}{k} \equiv a^{k-1}\sum_{j=1}^{p^{e+t-1}-1}\left[\frac{ja}{p^{e+t-1}}\right]j^{k-1} \pmod{p^{e}},$$

luego

$$p^{k-1}(a^k-1)\frac{B_k}{k} \equiv a^{k-1}\sum_{j=1}^{p^{e+t}-1}\left[\frac{ja}{p^{e+t}}\right]j^{k-1} - a^{k-1}\sum_{\substack{j=1\\ \text{m.c.d}(j,p)=1}}^{p^{e+t}-1}\left[\frac{ja}{p^{e+t}}\right]j^{k-1} \pmod{p^{e}},$$

entonces

$$\begin{aligned}a^{k-1}\sum_{\substack{j=1\\ \text{m.c.d}(j,p)=1}}^{p^{e+t}-1}\left[\frac{ja}{p^{e+t}}\right]j^{k-1} &\equiv a^{k-1}\sum_{j=1}^{p^{e+t}-1}\left[\frac{ja}{p^{e+t}}\right]j^{k-1} - p^{k-1}(a^k-1)\frac{B_k}{k} \pmod{p^e}\\ &\equiv (a^k-1)\frac{B_k}{k} - p^{k-1}(a^k-1)\frac{B_k}{k} \pmod{p^e}.\end{aligned}$$

Por lo tanto

$$(1-p^{k-1})(a^k-1)\frac{B_k}{k} \equiv a^{k-1} \sum_{\substack{j=1 \\ \text{m.c.d}(j,p)=1}}^{p^{e+t}-1} \left[\frac{ja}{p^{e+t}}\right] j^{k-1} \ (\text{mód } p^e).$$

Como $k \equiv k' \ (\text{mód } \varphi(p^e))$ entonces $k-k' = \varphi(p^e)q$, con $q \in \mathbb{Z}$. Así, por el Teorema de Euler

$$a^{\varphi(p^e)} \equiv 1 \ (\text{mód } p^e) \ \text{ ya que } \ \text{m.c.d}(a, p^e) = 1,$$

entonces

$$a^{\varphi(p^e)q} \equiv 1 \ (\text{mód } p^e) \implies a^{k-k'} \equiv 1 \ (\text{mód } p^e),$$

por consiguiente

$$a^{k-1} \equiv a^{k'-1} \ (\text{mód } p^e),$$

por el mismo razonamiento si $\text{m.c.d}(j,p) = 1$, tenemos $j^{k-1} \equiv j^{k'-1} \ (\text{mód } p^e)$.

Análogamente, tenemos que

$$(1-p^{k'-1})(a^{k'}-1)\frac{B_{k'}}{k'} \equiv a^{k'-1} \sum_{\substack{j=1 \\ \text{m.c.d}(j,p)=1}}^{p^{e+t}-1} \left[\frac{ja}{p^{e+t}}\right] j^{k'-1} \ (\text{mód } p^e).$$

De esa manera, concluimos:

$$(1-p^{k'-1})(a^{k'}-1)\frac{B_{k'}}{k'} \equiv (1-p^{k-1})(a^k-1)\frac{B_k}{k} \ (\text{mód } p^e).$$

Como $p \nmid (a^k-1)$, obtenemos el resultado deseado

$$(1-p^{k-1})\frac{B_k}{k} \equiv (1-p^{k'-1})\frac{B_{k'}}{k'} \ (\text{mód } p^e).$$

□

Observación 1.33. *El valor*

$$(1-p^{k'-1})\frac{B_k}{k}$$

puede ser interpretado como el valor $\zeta(1-k)$ con el factor p de Euler removido, i.e.,

$$\begin{aligned} \frac{B_k}{k} - \frac{B_k}{k}p^{k-1} = \frac{B_k}{k} + \zeta(1-k)p^{k-1} &\implies (1-p^{k-1})\frac{B_k}{k} = -\zeta(1-k) + \zeta(1-k)p^{k-1} \\ &\implies (1-p^{k-1})\frac{B_k}{k} = \zeta(1-k)(p^{k-1}-1). \end{aligned}$$

Definición 1.34. *Un primo p será llamado **regular** si p no divide a ningún numerador de los B_k con k entero par y $k \leq p-3$. Si p no es regular, lo llamaremos **irregular**.*

Observación 1.35. *Se desconoce si hay infinitos primos regulares. Sin embargo, tenemos el siguiente resultado.*

Teorema 1.36. *Existen infinitos primos irregulares.*

Demostración. Razonemos por contradicción. Sean $p_1, ..., p_s$ el conjunto de los primos irregulares. Sea k número par y definamos $n = k(p_1 - 1)\cdots(p_s - 1)$ si $s \geq 1$. De otro modo, definimos $n = k$. Por (1.6) $|B_n/n| \to \infty$ cuando $k \to \infty$, luego podemos tomar k suficientemente grande tal que $|B_n/n| > 1$. Sea p-primo tal que $\nu_p(B_n/n) > 0$. Por Teorema de von Staudt-Clausen, tenemos que $(p-1) \nmid n$, si no, tenemos que $(p-1)|n$ y así $p|V_n$, de modo que $\frac{B_n}{n} \notin \mathbb{Z}_{(p)}$. Entonces, $p \neq p_i$ para $1 \leq i \leq s$ y $p \neq 2$. Ahora mostramos que p es irregular. En efecto, sea $n \equiv m \pmod{p-1}$ con $1 \leq m < p-1$, ya que $(p-1) \nmid n$. Más aún, m es par ya que n es par. Por la congruencia de Kummer

$$\frac{B_n}{n} \equiv \frac{B_m}{m} \pmod{p}.$$

Entonces, $\nu_p(B_m/m) > 0$, ya que:

$$\nu_p\left(\frac{B_m}{m}\right) = \nu_p\left(\frac{B_m}{m} - \frac{B_n}{n} + \frac{B_n}{n}\right) \geq \min\left\{\nu_p\left(\frac{B_m}{m} - \frac{B_n}{n}\right), \nu_p\left(\frac{B_n}{n}\right)\right\} \geq 1.$$

Por lo tanto

$$0 < \nu_p\left(\frac{B_m}{m}\right) = \nu_p(B_m) - \nu_p(m) \implies \nu_p(B_m) > \nu_p(m).$$

De donde concluimos que $\nu_p(B_m) > 0$, esto es, p es primo irregular. □

Capítulo 2

Interpolación p-ádica

El objetivo de este capítulo es presentar el concepto de función p-ádica, es decir, funciones definidas en $\mathbb{C}_p$ y que toman valores en $\mathbb{C}_p$, análogo p-ádico de los números complejos, por ende, cuestiones como extensiones analíticas de funciones muy usadas en análisis complejo y herramienta fundamental en el estudio de la funciones L de Dirichlet, encontraran también su análogo p-ádico vía interpolación. Cabe resaltar que Kubota y Leopoldt, en 1964, construyeron las funciones L p-ádicas vía interpolación p-ádica de valores especiales de funciones L de Dirichlet, por ejemplo usando las congruencias de Kummer ellos construyeron la función zeta de Riemann p-ádica ζ_p cuyos valores en los enteros negativos coinciden con los de la función zeta de Riemann, hasta un factor de correción explícito.

2.1. Funciones p-ádicas

Necesitamos tener primero claro algunos conceptos básicos sobre análisis p-ádico. Algunas veces, por razones técnicas, es conveniente encajar $\mathbb{C}_p$ en $\mathbb{C}$, o al contrario. Ya que ambos campos son isomorfos algebraicamente, aunque no lo sean desde el punto de vista topológico. Ambos campos poseen el mismo grado de trascendencia sobre $\mathbb{Q}$, y ambos se obtienen empezando por $\mathbb{Q}$, adjuntando bases de transcendencia, y después tomando su cerradura algebraica.

Empezamos con un entero p-ádico $x \in \mathbb{Z}_p$. Por Teorema C.23, (ver Apéndice C), existe una sucesión $(\alpha_n)_n$ de enteros $\alpha_n \to x$ tal que:

- $\alpha_n \equiv x \pmod{p^n}$,
- $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$,
- $0 \leq \alpha_n < p^n$.

Al representar α_n en base p, la congruencia $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$ simplemente dice que los últimos n dígitos de ambos números son iguales. Es decir, tenemos

$$\begin{aligned}
\alpha_0 &= b_0 && 0 \leq b_0 < p,\\
\alpha_1 &= b_0 + b_1 p && 0 \leq b_1 < p,\\
\alpha_2 &= b_0 + b_1 p + b_2 p^2 && 0 \leq b_2 < p,\\
\alpha_3 &= b_0 + b_1 p + b_2 p^2 + b_3 p^3 && 0 \leq b_3 < p,
\end{aligned}$$

y así sucesivamente. Tomando todas estas expansiones juntas, entonces

$$x = b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \cdots . \tag{2.1}$$

Tenemos entonces que

Lema 2.1. *Cada $x \in \mathbb{Z}_p$, se puede escribir en la forma (2.1) de manera única.*

Demostración. Ver [11]. Cap. 3. Pág. 68. □

Esto mismo puede ser generalizado para cada elemento $x \in \mathbb{Q}_p$, y obtenemos.

Lema 2.2. *Cada $x \in \mathbb{Q}_p$ puede ser escrito de la forma*

$$x = \sum_{n \geq m} b_n p^n,$$

con $0 \leq b_n < p$ y $m = \nu_p(x)$. Esta representación es única.

Demostración. Ver [11]. Cap. 3. Pág 68.

□

Aunque para hablar de conceptos como sumas infinitas, necesitamos saber si estas series efectivamente definen un número p-ádico, es decir, constatar su convergencia. Por esta razón, centraremos un poco nuestra atención sobre criterios de convergencia de sucesiones y series en $\mathbb{Q}_p$.

Observación 2.3. *Por Teorema C.17, tenemos que $\mathbb{Q}_p$ es completo, quiere decir que toda sucesión de Cauchy en $\mathbb{Q}_p$ converge en $\mathbb{Q}_p$. Más aún, al ser $\mathbb{Q}_p$ espacio no arquimedeano podemos caracterizar las sucesiones de Cauchy en $\mathbb{Q}_p$ de una maera más práctica que en $\mathbb{R}$.*

Lema 2.4. *Una sucesión $(a_n)_n$ en $\mathbb{Q}_p$ es una sucesión de Cauchy, y por tanto convergente, si y solo si satisface*

$$\lim_{n \to +\infty} |a_{n+1} - a_n|_p = 0.$$

Demostración. Solo resta probar la condición necesaria. Sea $\varepsilon > 0$, entonces existe $N \in \mathbb{N}$, tal que

$$n \geq N \implies |a_{n+1} - a_n|_p < \varepsilon.$$

Debido a lo cual, si $n, m \geq N$, con $n \leq m$, tenemos que:

$$\begin{aligned} |a_n - a_m|_p &= |(a_n - a_{n+1}) + (a_{n+1} - a_{n+2}) + \cdots + (a_{m-1} - a_m)|_p \\ &\leq \text{máx}\{|a_n - a_{n+1}|_p, |a_{n+1} - a_{n+2}|_p, \cdots, |a_{m-1} - a_m|_p\} < \varepsilon. \end{aligned}$$

De manera que, obtenemos el resultado deseado.

□

Una importante consecuencia de este lema y la cual contrasta bastante del caso no arquimedeano es el siguiente lema.

Lema 2.5. *Una serie infinita* $\sum_{n\geq 0} a_n$ *con* $a_n \in \mathbb{Q}_p$ *es convergente si y solo si*

$$\lim_{n\to\infty} |a_n|_p = 0,$$

en cuyo caso también tenemos

$$\left|\sum_{n=0}^{+\infty} a_n\right|_p \leq \max_n |a_n|_p$$

Demostración. Resta probar la condición suficiente. Sea $|a_n|_p \to 0$, y sea

$$s_N = \sum_{n=1}^{N} a_n.$$

Dado que $\mathbb{Q}_p$ es completo, basta probar que la sucesión $(s_N)_{N\geq 1}$ es de Cauchy. Luego

$$|s_{N+1} - s_N|_p = |a_{N+1}|_p \longrightarrow 0.$$

Para deducir la última desigualdad, tenemos que. Si $\sum_n a_n = 0$, la desigualdad se cumple trivialmente. Si no, entonces

$$|s_N|_p \leq \max_{0\leq n\leq N} |a_n|_p,$$

como $|a_n|_p \to 0$, por Lema 3.2.10 de [11], tenemos que a partir de cierto $N_1 \in \mathbb{Z}_+$, $|a_n|_p = |a_m|_p$, para todo $n, m \geq N_1$. Por tanto

$$\max_{0\leq n\leq N_1} |a_n|_p = \max_n |a_n|_p,$$

por otro lado, a partir de cierto $N_2 \in \mathbb{Z}_+$, tenemos que

$$\left|\sum_{n=0}^{+\infty} a_n\right|_p = \left|\sum_{n=0}^{N_2} a_n\right|_p = |s_{N_2}|_p,$$

por Lema 3.2.10 de [11]. Al hacer $M = \max\{N_1, N_2\}$, entonces

$$\left|\sum_{n=0}^{+\infty} a_n\right|_p = \left|\sum_{n=0}^{M} a_n\right|_p = |s_M|_p \leq \max_{0\leq n\leq M} |a_n|_p = \max_n |a_n|_p.$$

Como se quería demostrar

□

Las ideas básicas acerca de funciones y continuidad permaneces sin cambios cuando trabajamos en el lado p-ádico, ya que en todo caso estos conceptos solo dependen de la estructura métrica. Nuestro objetivo entonces será explorar las ideas principales sobre algunas funciones definidas por series de potencias, en particular las versiones p-ádicas de la exponencial y el logaritmo.

Definición 2.6. *Definimos*

$$\boldsymbol{Exp}(X) = \sum_{n=0}^{+\infty} \frac{X^n}{n!},$$

como serie formal.

Observación 2.7. *Como (ver Apéndice C, Lema C.9 (i))*

$$\nu_p(n!) = \sum_{j=1}^{+\infty} \left[\frac{n}{p^j}\right] = \frac{n - (n_0 + n_1 + \cdots + n_k)}{p-1}$$
$$\implies \quad \nu_p(n!) < \frac{n}{p-1}.$$

Por otro lado, notemos que para $j \in \mathbb{Z}_+$

$$\frac{n}{p^j} < \left[\frac{n}{p^j}\right] + 1 \quad \implies \quad \left[\frac{n}{p^j}\right] > \frac{n}{p^j} - 1.$$

Tenemos también, si $p^a \leq n < p^{a+1}$

$$\begin{aligned}\nu_p(n!) = \sum_{j=1}^{+\infty} \left[\frac{n}{p^j}\right] &> \sum_{j=1}^{a} \frac{n}{p^j} - a \\ &= n\left(\frac{1 - p^{-(a+1)}}{1 - p^{-1}} - 1\right) - a \\ &= n\left(\frac{p^a - 1}{p^a(p-1)}\right) - a \\ &= \frac{n}{p-1} - a - \frac{np^{-a}}{p-1}.\end{aligned}$$

Luego, si $p^a \leq n < p^{a+1}$*, entonces*

$$a \log p \leq \log n \quad \implies \quad -a \geq -\frac{\log n}{\log p}$$

y

$$np^{-a} < p \quad \implies \quad -\frac{np^{-a}}{p-1} > -\frac{p}{p-1}.$$

De todo lo anterior, concluimos que:

$$\frac{n-p}{p-1} - \frac{\log n}{\log p} < \nu_p(n!) < \frac{n}{p-1}.$$

Se sigue por tanto que $|x^n/n!|_p \to 0$ *cuando* $n \to +\infty$ *si* $|x|_p < p^{-1/(p-1)}$ *y por otro lado* $|x^n/n!|_p \to \infty$ *si* $|x|_p > p^{-1/(p-1)}$*. Esto indica que* ***Exp****(X) tiene radio de convergencia* $p^{-1/(p-1)} < 1$*. Con lo cual, podemos definir una función exponencial p-ádica la cual no tiene una región de convergencia tan grande como su análoga compleja.*

Definición 2.8. *Sea* $r_p = p^{-1/(p-1)}$*, y definamos* $B(0, r_p) = \{x \in \mathbb{Z}_p : |x|_p < r_p\}$*. Definimos la función* ***exponencial p-ádica*** *de* $x \in B(0, r_p)$ *como*

$$\exp_p(x) = \boldsymbol{Exp}(x) = \sum_{n=0}^{+\infty} \frac{x^n}{n!}.$$

Proposición 2.9. *Si $x, y \in B(0, r_p)$ tenemos que $x + y \in B(0, r_p)$, también*

$$\exp_p(x \cdot y) = \exp_p(x) + \exp_p(y).$$

Demostración. Por definición de la exponencial p-ádica, tenemos

$$\begin{aligned}
\exp_p(x+y) &= \sum_{n=0}^{+\infty} \frac{(x+y)^n}{n!} = \sum_{n=0}^{+\infty} \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \\
&= \sum_{n=0}^{+\infty} \sum_{k=0}^{n} \frac{1}{n!} \frac{n!}{(n-k)!k!} x^{n-k} y^k \\
&= \sum_{n=0}^{+\infty} \sum_{k=0}^{n} \frac{x^{n-k}}{(n-k)!} \frac{y^k}{k!} \\
&= \left(\sum_{m=0}^{+\infty} \frac{x^m}{m!} \right) \left(\sum_{k=0}^{+\infty} \frac{y^k}{k!} \right) \\
&= \exp_p(x) \cdot \exp_p(y).
\end{aligned}$$

□

Observación 2.10. *Notemos que $e = \exp_p(1)$ no está definida, pero $\exp_p(p)$ ($\exp_p(4)$ si $p = 2$) si lo está. Podríamos definir $e = (\exp_p(p))^{1/p}$ pero este no necesariamente sería único.*

Definición 2.11. *Definimos*

$$\boldsymbol{Log}(1+X) = \sum_{n=1}^{+\infty} (-1)^{n+1} \frac{X^n}{n}.$$

Como serie formal.

Observación 2.12. *Notemos que*

$$\nu_p(n) \leq \frac{\log n}{\log p} \quad \textit{implica que} \quad \frac{\nu_p(n)}{n} \leq \frac{\log n}{n} \cdot \frac{1}{\log p},$$

entonces

$$\frac{\nu_p(n)}{n} \leq C \log(n^{1/n}) \longrightarrow 0,$$

cuando $n \to +\infty$, i.e., para $a_n = (-1)^{n+1}/n$, tenemos

$$\sqrt[n]{|a_n|_p} = p^{\nu_p(n)/n} \longrightarrow 1 \quad \textit{cuando} \quad n \to \infty.$$

Entonces el radio de convergencia de la serie es 1, *(ver [11]. Cap. 4, Proposición 4.3.1), esto es la serie converge si $|x|_p < 1$.*

*La conclusión es que **Log**(1+X) define una función en el ideal $p\mathbb{Z}_p$ de los enteros p-ádicos. Esto sugiere que deberiamos definir el logaritmo en la manera obvia.*

Definición 2.13. *Sea* $p\mathbb{Z}_p = \{x \in \mathbb{Z}_p : |x|_p < 1\}$. *Definimos el* ***logaritmo p-ádico*** *de* $x \in p\mathbb{Z}_p$ *como*

$$\log_p(1+x) = \textbf{\textit{Log}}(1+x) = \sum_{n=1}^{+\infty} (-1)^{n+1} \frac{x^n}{n}.$$

En este caso, la función $\log_p$ *se puede extender a todo* $\mathbb{C}_p^\times$.

Proposición 2.14. *Existe una única extensión de* $\log_p$ *a todo* $\mathbb{C}_p^\times$ *tal que* $\log_p(p) = 0$ *y* $\log_p(xy) = \log_p(x) + \log_p(y)$ *para todo* $x, y \in \mathbb{C}_p^\times$.

Demostración. Ver Washington [27]. Cap. 5, Proposición 5.4. □

Observación 2.15. *Estas dos funciones son inversas una de la otra en el conjunto* $B(0, r_p) \subset \mathbb{Z}_p$. *Esto es claro como identidades de series de potencias formales. Para probarlo rigorosamente, necesitamos hacer estimaciones de las funciones y asegurarnos que ellas están en el dominio de definición. Por lo tanto, necesitamos mostrar que*

$$|x|_p < r_p \implies |\exp_p(x) - 1|_p < 1$$

y

$$|x|_p < r_p \implies |\log_p(1+x)|_p < r_p.$$

Para verificar la primera desigualdad, note que $\nu_p(x) > 1/(p-1)$ *implica que para* $n \geq 2$,

$$\nu_p\left(\frac{x^{n-1}}{n!}\right) = (n-1)\nu_p(x) - \nu_p(n!) > \frac{n-1}{p-1} - \frac{n-s}{p-1} = \frac{s-1}{p-1} \geq 0,$$

donde s *es la suma de los dígitos en la expansión p-ádica de* n *(ver Apéndice C. Lema C.9). Así que* $|x^{n-1}/n!|_p < 1$ *y así* $|x^n/n!|_p < |x|_p$ *de lo cual deducimos*

$$|\exp_p(x) - 1|_p \leq \max_{n \geq 1} \left|\frac{x^n}{n!}\right|_p < |x|_p < r_p < 1.$$

De modo que, $\log_p(\exp_p(x))$, *se expande como serie de potencias y tenemos permitido intercambiar símbolos sumatorios para deducir que es igual a* x *(por series formales).*

Por otro lado, para verificar la segunda desigualdad, si $|x|_p < r_p$ *entonces*

$$\begin{aligned}\nu_p\left((-1)^{n+1}\frac{x^n}{n}\right) - \nu_p(x) &= (n-1)\nu_p(x) - \nu_p(n) \\ &> \frac{n-1}{p-1} - \nu_p(n) = (n-1)\left(\frac{1}{p-1} - \frac{\nu_p(n)}{n-1}\right).\end{aligned}$$

Si $n = p^\alpha n_1$ *con* $m.c.d(p, n_1) = 1$, *tenemos*

$$\frac{\nu_p(n)}{n-1} = \frac{\alpha}{p^\alpha n_1 - 1} \leq \frac{\alpha}{p^\alpha - 1} = \frac{\alpha}{(p-1)(p^{\alpha-1} + p^{\alpha-2} + \cdots + p + 1)} \leq \frac{1}{p-1}.$$

$\therefore \nu_p((-1)^{n+1}x^n/n) - \nu_p(x) > 0$ *para* $n > 1$, *i.e.,*

$$\left|(-1)^{n+1}\frac{x^n}{n}\right|_p < |x|_p \implies \left|\frac{x^n}{n}\right|_p < |x|_p.$$

Luego

$$\begin{aligned}|\log_p(1+x)|_p &= \left|\sum_{n=1}^{+\infty}(-1)^{n+1}\frac{x^n}{n}\right|_p \\ &\leq \max_n \left|\frac{x^n}{n}\right|_p < |x|_p < r_p.\end{aligned}$$

Entonces la identidad formal de la serie de potencias $\exp_p(\log_p(1+x)) = 1+x$ *se satisface, si* $|x|_p < r_p$.

De lo anterior, podemos explícitar un resultado práctico en deducciones posteriores:

Lema 2.16. *Si* $|x|_p < p^{-1/(p-1)}$ *entonces* $|\log_p(1+x)|_p = |x|_p$ *y si* $|x|_p \leq p^{-1/(p-1)}$ *entonces* $|\log_p(1+x)|_p \leq |x|_p$.

Demostración. Si $n < p$ entonces $|n|_p = 1$, y en general $|n|_p \geq n^{-1}$, ya que al tomar $n = p^{\nu_p(n)}m$ con $p \nmid m$ entonces $n \geq p^{\nu_p(n)}$, por lo tanto

$$\frac{1}{n} \leq \frac{1}{p^{\nu_p(n)}} = |n|_p.$$

De manera que, si $|x|_p < p^{-1/(p-1)}$ tenemos

$$\left|\frac{x^n}{n}\right|_p = |x|_p^{n-1} \cdot |x|_p < p^{(1-n)/(p-1)} \cdot |x|_p < |x|_p \quad \text{si} \quad 2 \leq n < p,$$

y

$$\left|\frac{x^n}{n}\right|_p < n \cdot |x|_p^{n-1} \cdot |x|_p < n \cdot p^{(1-n)/(p-1)} \cdot |x|_p \leq |x|_p \quad \text{si} \quad n \geq p,$$

ya que $np^{(1-n)/(p-1)}$ es decreciente para $n \geq p$. Debido a lo cual

$$|x - \frac{x^2}{2} + \cdots|_p = |x|_p.$$

□

Otra propiedad deseable de estas dos funciones definidas en series de potencias sería la continuidad, propiedad que queda establecida en el siguiente lema:

Lema 2.17. *Sea* $f(X) = \sum_n a_n X^n$ *una serie de potencias con coeficientes en* $\mathbb{Q}_p$, *y sea* $\mathcal{D} \subseteq \mathbb{Q}_p$ *su región de convergencia, i.e., el conjunto* $x \in \mathbb{Q}_p$ *para los cuales* $f(X)$ *converge. La función*

$$f : \mathcal{D} \to \mathbb{Q}_p,$$

definida por $x \mapsto f(x)$ *es continua en* $\mathcal{D}$.

Demostración. Si $\mathcal{D} = \{0\}$, entonces la afirmación se tiene, ya que f define una función continua. Sea $\varepsilon > 0$, para $x \in \mathcal{D}$ con $|x|_p \neq 0$, definimos

$$M = \max_n\{|a_n x^n|_p\} \quad \text{y} \quad \delta = \min\left\{|x|_p, \frac{\varepsilon|x|_p}{M}\right\},$$

si $M = 0$, etonces $f = 0$, y la afirmación se cumple, luego podemos asumir $M \neq 0$. Por otro lado, si $|x-y|_p < \delta$, entonces $|x-y|_p < |x|_p$, de modo que

$$|y|_p \leq \max\{|x-y|_p, |x|_p\} = |x|_p,$$

esto es $|y|_p \leq |x|_p$, también tenemos que

$$|x|_p \leq \max\{|x-y|_p, |y|_p\} = |y|_p,$$

ya que si el máximo fuese igual a $|x-y|_p$, entonces $|x|_p < |x-y|_p$, lo cual contradice nuestra hipótesis. De tal forma $|x|_p \leq |y|_p$ que junto a lo anterior tenemos que $|x|_p = |y|_p$. Ahora bien:

$$\begin{aligned} |f(x) - f(y)|_p &= \left|\sum_n a_n(x^n - y^n)\right|_p \\ &\leq \max_n\{|a_n(x^n - y^n)|_p\} = \max_n\left\{|a_n|_p|x-y|_p\left|\sum_{j=1}^n x^{n-j}y^{j-1}\right|_p\right\}, \end{aligned}$$

por otro lado, dado que $|x|_p = |y|_p$, siempre que $|x-y|_p < \delta$, tenemos

$$\left|\sum_{j=1}^n x^{n-j}y^{j-1}\right|_p \leq \max_{1\leq j\leq n}\{|x^{n-j}y^{j-1}|_p\} = \max_{1\leq j\leq n}\{|x|_p^{n-1}\} = |x|_p^{n-1}.$$

Por consiguiente

$$|f(x) - f(y)|_p \leq \max_n\{|a_n|_p|x-y|_p|x|_p^{n-1}\} < \frac{\delta}{|x|_p}\max_n\{|a_n|_p|x|_p^n\} = \frac{\delta}{|x|_p}\cdot M < \varepsilon.$$

De manera que f es continua en $\mathcal{D}$.

□

2.2. Método de Mahler para la Interpolación p-ádica

Si tenemos una sucesión de enteros $(a_k)_{k\geq 1}$ podemos preguntar: ¿Con qué condiciones existe una función continua $f : \mathbb{Z}_p \to \mathbb{Q}_p$ tal que $f(k) = a_k$?

Dado que $\mathbb{Z}_p$ es compacto (ver Apéndice C. Obs. C.25), tal función debe ser uniformemente continua y acotada. Por tal motivo, una condición necesaria es que para cada $m \in \mathbb{Z}_+$, existe $N = N(m) \in \mathbb{Z}_+$ tal que

$$k \equiv k' \pmod{p^N} \implies a_k \equiv a_{k'} \pmod{p^m}. \tag{2.2}$$

Es decir, siempre que k y k' sean cercanos con $|\cdot|_p$, entonces a_k y $a_{k'}$ son cercanos con $|\cdot|_p$. En efecto, como f es continua, entonces dado $\varepsilon > 0$ existe $\delta > 0$ tal que para $k \in \mathbb{Z}_p$, si $k' \in \mathbb{Z}_p$ es tal que

$$|k - k'|_p < \delta \implies |f(k) - f(k')|_p < \varepsilon,$$

esto es,

$$p^{-\nu_p(k-k')} < \delta \implies p^{-\nu_p(a_k - a_{k'})} < \varepsilon.$$

Tenemos que si $\varepsilon = p^{-m}$, entonces existe $\delta_m > 0$ tal que

$$p^{-\nu_p(k-k')} < \delta_m \implies p^{-\nu_p(a_k - a_{k'})} < p^{-m}.$$

Por otro lado, para ese $\delta_m > 0$ existe $N = N(m) \in \mathbb{N}$, tal que si $n \geq N$, implica que $p^{-n} < \delta_m$, (convergencia de $(p^{-n})_{n\geq 1}$ en el valor absoluto usual). Debido a lo cual, si $\nu_p(k - k') \geq N$, es decir si $k \equiv k' \pmod{p^N}$, tenemos que:

$$\begin{aligned} p^{-\nu_p(k-k')} \leq p^{-N} < \delta_m &\implies p^{-\nu_p(a_k - a_{k'})} < p^{-m} \\ &\implies \nu_p(a_k - a_{k'}) > m \\ &\implies a_k \equiv a_{k'} \pmod{p^m}. \end{aligned}$$

Recíprocamente, afirmamos que el problema de interpolación se reduce a verificar (2.2), lo cual queda dicho en el siguiente teorema.

Teorema 2.18. *Supongamos que una sucesión de números $f(k) \in \mathbb{Q}_p$, $k = 0, 1, 2, ...$, es acotada respecto a la norma p-ádica y satisface la siguiente condición. Para cada número natural m, existe un natural $N = N(m)$ tal que*

$$k \equiv k' \ (mód\ p^N) \implies f(k) \equiv f(k') \ (mód\ p^m). \tag{2.3}$$

Entonces, existe una función continua $\hat{f} : \mathbb{Z}_p \to \mathbb{Q}_p$ tal que $\hat{f}(k) = f(k)$.

Demostración. Definimos la función $\hat{f} : \mathbb{Z}_p \to \mathbb{Q}_p$ como sigue. Sea $x \in \mathbb{Z}_p$, tomamos una sucesión de enteros $(n_i)_{i\geq 1}$ tal que $n_i \to x$ en la norma p-ádica y definimos

$$\hat{f}(x) = \lim_{i\to\infty} f(n_i).$$

El límite existe ya que $(f(n_i))_{i\geq 1}$ es sucesión de Cauchy respecto a $|\cdot|_p$. En efecto, sea $\varepsilon > 0$, por propiedad arquimediana existe $m \in \mathbb{Z}_+$ tal que $m \cdot \varepsilon > 1$ y dado que $p^m > m$, entonces $p^{-m} < \varepsilon$. Por otro lado, por hipótesis para este $m \in \mathbb{Z}_+$ existe $N \in \mathbb{N}$ tal que se satisface (2.3), por tanto y dado que $n_i \to x$ en $|\cdot|_p$, para este N natural existe $i_0 \in \mathbb{N}$ tal que si $i, i' \geq i_0$ entonces $|n_i - n_{i'}|_p < p^{-N}$, esto es

$$p^{-\nu_p(n_i - n_{i'})} < p^{-N}, \quad \therefore \quad \nu_p(n_i - n_{i'}) > N \text{ siempre que } i, i' \geq i_0 \in \mathbb{N},$$

i.e., $n_i \equiv n_{i'} \pmod{p^N}$, lo cual por (2.3) implica que $f(n_i) \equiv f(n_{i'}) \pmod{p^m}$, por lo tanto

$$|f(n_i) - f(n_{i'})|_p < p^{-m} < \varepsilon \ \text{ siempre que } i, i' \geq i_0 \in \mathbb{N}.$$

Más aún, si $(n_i')_{i\geq 1}$ es cualquier otra sucesión de enteros que converge a x en la norma p-ádica, tenemos que

$$\lim_{i\to\infty} f(n_i) = \lim_{i\to\infty} f(n_i').$$

En efecto, sean

$$\lim_{i\to\infty} f(n_i) = L \quad \text{y} \quad \lim_{i\to\infty} f(n_i') = M,$$

sea $\varepsilon > 0$, análogamente al razonamiento anterior, existe $m \in \mathbb{N}$ tal que $p^{-m} < \varepsilon$, para este m existe $N = N(m) \in \mathbb{N}$ tal que se satisface (2.3), para este N como $n_i \to x$ y $n_i' \to x$ existe $i_0 \in \mathbb{N}$ tal que si $i \geq i_0$ entonces $|n_i - n_i'|_p < p^{-N}$, con lo cual $\nu_p(n_i - n_i') > N$, esto implica que $n_i \equiv n_i'$ (mód p^N), entonces por (2.3) tenemos que $f(n_i) \equiv f(n_i')$ (mód p^m), i.e., $\nu_p(f(n_i) - f(n_i')) \geq m$, entonces $|f(n_i) - f(n_i')|_p \leq p^{-m} < \varepsilon$ siempre que $i \geq i_0 \in \mathbb{N}$.

Por otra parte, existe $i_1 \in \mathbb{N}$ tal que si $i \geq i_1$ entonces $|f(n_i) - L|_p < \varepsilon$ y también $|f(n_i') - M|_p < \varepsilon$. De lo anterior, si $i \geq \text{máx}\{i_0, i_1\}$, entonces

$$|L - M|_p \leq \text{máx}\{|L - f(n_i)|_p, |f(n_i) - f(n_i')|_p, |f(n_i') - M|_p\} < \varepsilon$$

Lo anterior demuestra que la función $\hat{f}$ está bien definida. Por último probaremos la continuidad de la función $\hat{f}$. Sea $y \in \mathbb{Z}_p$, debemos demostrar que

$$\lim_{x\to y} \hat{f}(x) = \hat{f}(y).$$

Esto es, que para todo $\varepsilon > 0$ existe $\delta > 0$ tal que para $x \in \mathbb{Z}_p$

$$\text{si } |x - y|_p < \delta \implies |\hat{f}(x) - \hat{f}(y)|_p < \varepsilon.$$

Sea $\varepsilon > 0$, luego por el mismo argumento existe $m \in \mathbb{N}$ tal que $p^{-m} < \varepsilon$. Por otro lado, como $x, y \in \mathbb{Z}_p$, sean $(n_i)_{i\geq 1}$ y $(m_i)_{i\geq 1}$ sucesiones de enteros tales que $n_i \to x$ y $m_i \to y$ en $|\cdot|_p$, luego para el m mencionado anteriormente existe $N = N(m) \in \mathbb{N}$ tal que se satisface (2.3), entonces para este N, existe $i_0 \in \mathbb{N}$ tal que si $i \geq i_0$, entonces $|n_i - x|_p < p^{-N}$, $|m_i - y|_p < p^{-N}$ y si además suponemos $|x - y|_p < p^{-N}$, tenemos que si $i \geq i_0$, entonces

$$|n_i - m_i|_p \leq \text{máx}\{|n_i - x|_p, |x - y|_p, |y - m_i|_p\} < p^{-N},$$

esto es, $n_i \equiv m_i$ (mód p^N), lo cual implica por (2.3) que $f(n_i) \equiv f(m_i)$ (mód p^m), que en terminos de la norma p-ádica queda $|f(n_i) - f(m_i)|_p \leq p^{-m} < \varepsilon$.

Además, existe $i_1 \in \mathbb{N}$ tal que si $i \geq i_1$ entonces

$$|\hat{f}(x) - f(n_i)|_p < \varepsilon \quad \text{y} \quad |f(m_i) - \hat{f}(y)|_p < \varepsilon,$$

por definición de $\hat{f}(x)$ y $\hat{f}(y)$. Por tanto, si $i \geq \text{máx}\{i_0, i_1\}$ y $\delta = p^{-N}$, entonces

$$|\hat{f}(x) - \hat{f}(y)|_p \leq \text{máx}\{|\hat{f}(x) - f(n_i)|_p, |f(n_i) - f(m_i)|_p, |f(m_i) - \hat{f}(y)|_p\} < \varepsilon,$$

siempre que $|x - y|_p < \delta$. Concluimos entonces que $\hat{f}$ es continua, y así termina la demostración.

□

Observación 2.19. *Como una aplicación del teorema anterior, observemos que si* $n \equiv 1$ *(mód p), i.e.,* $n = 1 + qp$ *para algún* $q \in \mathbb{Z}$*, entonces la función* $f(k) = n^k$*, puede ser interpolada de forma p-ádica. Para ver esto, necesitamos verficar las condiciones del Teorema 2.18, primero notemos que* $f(k) \in \mathbb{Z}_p$ *para todo* $k = 0, 1, 2 \cdots$ *. Luego el conjunto de los* $f(k)$ *es acotado en* $\mathbb{Q}_p$*. Por otro lado, tomemos* $m \in \mathbb{N}$ *y definamos* $N = m - 1 \in \mathbb{Z}$*, tomando* $k, k' \in \mathbb{Z}$*, tal que si* $k \equiv k'$ *(mód* p^{m-1}*), tenemos que* $k - k' = q_0 p^{m-1}$*, notemos también que:*

$$(1 + qp)^{p^{m-1}} \equiv 1 \ (mód\ p^m),$$

en efecto, por teorema del binomio

$$(1 + qp)^{p^{m-1}} = 1 + \sum_{j=1}^{p^{m-1}} \binom{p^{m-1}}{j} (qp)^j,$$

ahora bien, como (ver Apéndice C, Lema C.9)

$$\nu_p\left(\binom{p^{m-1}}{j}(qp)^j\right) = (m-1) + \nu_p(q^j) + j - \nu_p(j) \geq m,$$

entonces

$$\nu_p((1 + qp)^{p^{m-1}} - 1) \geq m.$$

De lo anterior,

$$n^{(k-k')} = n^{q_0 p^{m-1}} = (1 + qp)^{q_0 p^{m-1}} \equiv 1 \ (mód\ p^m),$$

por tal motivo y dado que $m.c.d(n, p) = 1$*,* $n^k \equiv n^{k'}$ *(mód* p^m*). Luego por Teorema 2.18 la función* $f : \mathbb{N} \to \mathbb{Q}_p$ *tal que* $f(k) = n^k$ *con* $m.c.d(n, p) = 1$ *admite una extensión como función continua* $\hat{f} : \mathbb{Z}_p \to \mathbb{Q}_p$*, tal que* $\hat{f}(k) = n^k$*.*

Ahora, pasaremos a la definición de la función gamma p-ádica. Consideremos la sucesión

$$a_k = \prod_{\substack{j<k \\ \text{m.c.d}(j,p)=1}} j,$$

y verificamos que las condiciones del Teorema 2.18 se cumplen. Debemos comparar la distancia p-ádica entre a_{k+p^s} y a_k, con $s \in \mathbb{Z}_+$. Observemos que

$$a_{k+p^s} = \left(\prod_{\substack{j<p^s \\ \text{m.c.d}(j,p)=1}} j\right)\left(\prod_{\substack{p^s<j<k+p^s \\ \text{m.c.d}(j,p)=1}} j\right),$$

el primer factor es el producto de un sistema completo de residuos módulo p^s. En este producto podemos emparejar clases residuales que sean inversas entre si, siempre que sean distintas. Cuando la clase residual x coincide con su propia inversa módulo p^s, tenemos que $x^2 \equiv 1$ (mód p^s). Para primos impares p, las únicas soluciones de

$$x^2 \equiv 1 \ (\text{mód}\ p^s) \ \ \forall\ s \in \mathbb{Z}_+$$

son $x = 1$ y $x = -1$, por el Lema de Hensel (ver Lema C.27). Luego tenemos

$$\begin{aligned} a_{k+p^s} &\equiv - \prod_{\substack{p^s<j<k+p^s \\ \text{m.c.d}(j,p)=1}} j \ (\text{mód } p^s) \\ &\equiv -a_k \ (\text{mód } p^s). \end{aligned}$$

Por lo tanto, si hacemos un ligero ajuste de signo en nuestra definición de los a_k, podemos hacer interpolación p-ádica. De acuerdo a Morita (ver [21], pág 368), tenemos la siguiente definición.

Definición 2.20. ***Función Gamma p-ádica****. Definimos la función Γ_p para $p \neq 2$, como $\Gamma_p(0) = 1$ y*

$$\Gamma_p(n) = (-1)^n \prod_{\substack{j<n \\ m.c.d(j,p)=1}} j.$$

Por el cálculo hecho anteriormente notamos que:

$$\Gamma_p(k+p^s) = (-1)^{k+p^s} a_{k+p^s} \equiv (-1)^{k+1+p^s} a_k = (-1)^{1+p^s} \Gamma_p(k) \ (\text{mód } p^s),$$

de manera que

$$\Gamma_p(k+p^s) \equiv \Gamma_p(k) \ (\text{mód } p^s).$$

Luego del Teorema 2.18, la función Γ_p se puede extender de manera continua a $\mathbb{Z}_p$.

El teorema de aproximación de Weierstrass (1885) (ver [26]), del matemático alemán Karl Weierstrass (1815-1897), dice que una función continua en un intervalo cerrado puede ser aproximada uniformemente por polinomios. El análogo p-ádico de este teorema clásico es el teorema de Mahler (1958) (ver [17]), del también matemático alemán Kurt Mahler (1903-1988). Este teorema plantea que para cualquier función continua $f : \mathbb{Z}_p \to \mathbb{Q}_p$, existen números $c_k \in \mathbb{Q}_p$ tal que

$$f(x) = \sum_{k=0}^{+\infty} \binom{x}{k} c_k.$$

Por tanto la sucesión de sumas parciales de esta serie da la aproximación deseada para $f(x)$. Aunque claro está, para demostrar esta afirmación necesitamos formalizar ciertos conceptos que están involucrados en ella, como por ejemplo, para qué casos ésta serie es convergente, además de saber que significa el coeficiente binomial en cuyo argumento aparecen números p-ádicos.

Observación 2.21. *Primero hagamos una serie de observaciones referentes a análisis combinatorio para deducir condiciones necesarias en la busqueda de nuestra objetivo, tenemos que:*

$$\binom{p^n}{k} \equiv 0 \ (\textit{mód } p)$$

para $1 \leq k < p^n$, *ya que (ver Apéndice C, Lema C.9 (iii))*

$$\nu_p\left(\binom{p^n}{k}\right) = n - \nu_p(k) \geq 1.$$

De la fórmula de inversión binomial, tenemos que:

$$b_n = \sum_{k=0}^{n} \binom{n}{k} a_k, \tag{2.4}$$

si y solo si

$$a_n = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} b_k. \tag{2.5}$$

En efecto, asumiendo (2.4), tenemos

$$\begin{aligned}
b_0 &= \binom{0}{0} a_0, \\
b_1 &= \binom{1}{0} a_0 + \binom{1}{1} a_1, \\
b_2 &= \binom{2}{0} a_0 + \binom{2}{1} a_1 + \binom{2}{2} a_2, \\
&\vdots \\
b_{n-1} &= \binom{n-1}{0} a_0 + \binom{n-1}{1} a_1 + \cdots + \binom{n-1}{n-2} a_{n-2} + \binom{n-1}{n-1} a_{n-1}, \\
b_n &= \binom{n}{0} a_0 + \binom{n}{1} a_1 + \binom{n}{2} a_2 + \binom{n}{3} a_3 + \cdots + \binom{n}{n-2} a_{n-2} + \binom{n}{n-1} a_{n-1} + a_n.
\end{aligned}$$

De lo anterior, despejando para cada b_k *el último término* $\binom{k}{k} a_k = a_k$, *y reemplazándolo en la identidad correspondiente al término* b_{k+1}, *obtenemos recursivamente:*

$$a_n = \sum_{j=0}^{n-1} \binom{n-1}{j} (-1)^j (b_{n-j} - b_{n-j-1}),$$

al hacer $k = n - j$, *entonces* $j = n - k$ *y así*

$$\begin{aligned}
a_n &= \sum_{k=n}^{1} \binom{n-1}{n-k} (-1)^{n-k} (b_k - b_{k-1}) \\
&= \sum_{k=1}^{n} \binom{n-1}{k-1} (-1)^{n-k} (b_k - b_{k-1}).
\end{aligned}$$

Por último, analizando términos consecutivos k *y* $k+1$, *notamos que:*

$$(-1)^{n-k} \binom{n-1}{k-1} (b_k - b_{k-1}) + (-1)^{n-k-1} \binom{n-1}{k} (b_{k+1} - b_k)$$

$$= (-1)^{n-k+1}\binom{n-1}{k-1}b_{k-1} + \left[(-1)^{n-k}\binom{n-1}{k-1} + (-1)^{n-k}\binom{n-1}{k}\right]b_k + (-1)^{n-k-1}\binom{n-1}{k}b_{k+1}$$
$$= (-1)^{n-k+1}\binom{n-1}{k-1}b_{k-1} + \binom{n}{k}(-1)^{n-k}b_k + (-1)^{n-k-1}\binom{n-1}{k}b_{k+1}.$$

Por esta razón, y al notar que reagrupando convenientemente, obtenemos:

$$a_n = (-1)^n b_0 + \sum_{k=1}^{n-1}\binom{n}{k}(-1)^{n-k}b_k + b_n,$$

de manera que verificamos (2.5). Este proceso también funciona recíprocamante, luego se demuestra la afirmación.

Fijando $m \in \mathbb{Z}_+$ y tomando la sucesión $(a_k)_{k\geq 1}$, donde

$$a_k = \begin{cases} (-1)^m & si \quad k = m \\ 0 & si \quad k \neq m. \end{cases}$$

Entonces de la fórmula de inversión binomial, se obtiene la siguiente relación de ortogonalidad

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k}\binom{k}{m} = \begin{cases} (-1)^m & si \quad n = m \\ 0 & si \quad n \neq m. \end{cases} \tag{2.6}$$

En efecto, para $j \geq 0$ tenemos por (2.4) que $b_j = (-1)^m\binom{j}{m}$, en particular si $0 \leq j < m$ tenemos $b_j = 0$. Entonces de (2.5) para $n \in \mathbb{N}$ obtenemos:

$$\begin{aligned} a_n &= \sum_{j=0}^{n}(-1)^{n-j}\binom{n}{j}b_j \\ &= \sum_{j=m}^{n}(-1)^{n+m-j}\binom{n}{j}\binom{j}{m}, \end{aligned}$$

al hacer el cambio de variable $k = n + m - j$, obtenemos:

$$a_n = \sum_{k=n}^{m}(-1)^k\binom{n}{n+m-k}\binom{n+m-k}{m},$$

notando que

$$\binom{n}{n+m-k}\binom{n+m-k}{m} = \binom{n}{k}\binom{k}{m} \quad para\ k = m, m+1, ..., n.$$

tenemos que

$$a_n = \sum_{k=m}^{n}(-1)^k\binom{n}{k}\binom{k}{m} = \sum_{k=0}^{n}(-1)^k\binom{n}{k}\binom{k}{m},$$

ya que para $k < m$, se tiene que $\binom{k}{m} = 0$. Así, por definición de la sucesión $(a_n)_{n\geq 1}$ obtenemos la relación de ortogonalidad buscada.

Si $f : \mathbb{Z}_p \to \mathbb{Q}_p$ es continua, sea

$$a_n(f) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k), \tag{2.7}$$

por (2.5), tenemos

$$f(n) = \sum_{k=0}^{n} \binom{n}{k} a_k(f). \tag{2.8}$$

Esto sugiere como podemos resolver el problema de interpolación p-ádica. Dada una sucesión $f(0), f(1), f(2), \cdots$, definimos $a_n(f)$ como en (2.7) y tomemos la función para $x \in \mathbb{Z}_p$ como:

$$f(x) = \sum_{k=0}^{+\infty} \binom{x}{k} a_k(f), \tag{2.9}$$

donde para $x \in \mathbb{Z}_p$, definimos

$$\binom{x}{n} = \begin{cases} \frac{x(x-1)\cdots(x-n+1)}{n!} & si \quad n \geq 1, \\ 1 & si \quad n = 0. \end{cases} \tag{2.10}$$

Si podemos demostrar que esta es una serie convergente en norma p-ádica, resolveremos el problema.

Observemos que la función coeficiente binomial definida en (2.10) es una función continua en variable p-ádica y toma valores enteros para $x \in \mathbb{Z}$, ya que si $n \neq 0$, considerando el polinomio

$$P_n(X) = \frac{X(X-1)\cdots(X-n+1)}{n!} \in \mathbb{Q}[X],$$

el cual tiene grado n en la variable X, este define una función continua de $\mathbb{Q}_p$ en si mismo (ver Lema 2.17) y si $n = 0$ es una función constante. Ahora, sabemos que el coeficiente binomial $\binom{m}{n} \in \mathbb{Z}$, si $m, n \in \mathbb{Z}_+$. Por tanto, para $\alpha \in \mathbb{Z}_+$, tenemos

$$P_n(\alpha) = \binom{\alpha}{n} \in \mathbb{Z}.$$

En otras palabras la función continua P_n mapea el conjunto $\mathbb{Z}_+$ en $\mathbb{Z}$. Por continuidad, también mapea la clausura de $\mathbb{Z}_+$ en $\mathbb{Z}_p$ a la clausura de $\mathbb{Z}$ en $\mathbb{Z}_p$. Por otro lado, como cualquier elemento de $\mathbb{Z}_p$ es el límite de una sucesión de enteros positivos (la suma parcial de su representación p-ádica, ver Lema 2.2). Entonces la clausura de $\mathbb{Z}_+$ es todo $\mathbb{Z}_p$, y concluimos que P_n mapea $\mathbb{Z}_p$ en $\mathbb{Z}_p$. Esto es

$$\left| \binom{x}{n} \right|_p \leq 1 \quad \forall\ x \in \mathbb{Z}_p.$$

Luego por la definición de $f(x)$ (2.9), tenemos que

$$\left| \binom{x}{n} a_n(f) \right|_p \leq |a_n(f)|_p.$$

La clave en la demostración del Teorema de Mahler es mostrar que $|a_k(f)|_p \to 0$ *cuando* $k \to +\infty$*, siempre que las hipótesis del Teorema 2.18 se cumplan. En esencia la demostración que presentamos sigue la dirección tomada por Bójanic, (ver [4]).*

Definición 2.22. ***Operador Diferencia****. El operador diferencia* Δ^n *para* $n \in \mathbb{Z}_+$ *y una función* f *está definido por*

$$\Delta^n f(x) = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} f(x+k).$$

Por tanto,

$$\begin{aligned}
&\Delta f(x) = f(x+1) - f(x),\\
&\Delta^2 f(x) = f(x+2) - 2f(x+1) + f(x),\\
&\Delta^3 f(x) = f(x+3) - 3f(x+2) + 3f(x+1) - f(x),\\
&\quad \cdots \qquad \cdots \qquad \cdots \qquad \cdots \qquad \cdots
\end{aligned}$$

Proposición 2.23. Δ^n *es un operador lineal.*

Demostración. Sea α escalar y f, g funciones, entonces

$$\begin{aligned}
\Delta^n[\alpha f(x) + g(x)] &= \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} [\alpha f(x+k) + g(x+k)]\\
&= \alpha \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} f(x+k) + \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} g(x+k)\\
&= \alpha \Delta^n f(x) + \Delta^n g(x).
\end{aligned}$$

□

Pasamos ahora, a la demostración de dos lemas de los cuales se sigue el teorema de Mahler.

Lema 2.24. *Para* $n \in \mathbb{Z}_+$*, y* f *función, tenemos*

$$\Delta^n f(x) = \sum_{j=0}^{m} \binom{m}{j} \Delta^{n+j} f(x-m).$$

Demostración. Es suficiente mostrar que

$$f(x) = \sum_{j=0}^{m} \binom{m}{j} \Delta^j f(x-m),$$

y el resultado se obtiene aplicando Δ^n a los dos lados de la igualdad junto a la proposición anterior. Notemos que

$$\begin{aligned}
\sum_{j=0}^{m} \binom{m}{j} \Delta^j f(x-m) &= \sum_{j=0}^{m} \binom{m}{j} \sum_{k=0}^{j} \binom{j}{k} (-1)^{j-k} f(x-m+k)\\
&= \sum_{j=0}^{m} \sum_{k=0}^{j} (-1)^{j-k} \binom{m}{j} \binom{j}{k} f(x-m+k)\\
&= \sum_{k=0}^{j} (-1)^{-k} f(x-m+k) \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{j}{k}.
\end{aligned}$$

Por la relación de ortogonalidad (2.6), la suma interna es igual a 0 a menos que $k = m$, donde será igual a $(-1)^m$, luego

$$\sum_{j=0}^{m} \binom{m}{j} \Delta^j f(x-m) = (-1)^{-m} \cdot f(x) \cdot (-1)^m = f(x).$$

□

Lema 2.25. *Para cualquier sucesión $f(0), f(1), f(2), \cdots$, definimos*

$$a_n(f) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k).$$

Entonces

$$\sum_{j=0}^{m} \binom{m}{j} a_{n+j}(f) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k+m).$$

Demostración. Para $m = 0$ es claro. Por Lema 2.24,

$$\Delta^n f(m) = \sum_{j=0}^{m} \binom{m}{j} \Delta^{n+j} f(0).$$

Por otro lado, por definición 2.22

$$\Delta^n f(m) = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} f(m+k),$$

y

$$\Delta^n f(0) = a_n(f) \implies \Delta^{n+j} f(0) = a_{n+j}(f),$$

por consiguiente

$$\Delta^n f(m) = \sum_{j=0}^{m} \binom{m}{j} a_{n+j}(f) \quad \text{y} \quad \Delta^n f(m) = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} f(m+k).$$

□

Observación 2.26. *El siguiente teorema es el análogo p-ádico del teorema clásico de Weierstrass que dice que cualquier función continua en $[-1,1]$ puede ser uniformemente aproximada por polinomios.*

Teorema 2.27. ***Mahler -1958-.*** *Sea $f : \mathbb{Z}_p \to \mathbb{Q}_p$ función continua, y sea*

$$a_n(f) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k).$$

Entonces $a_n(f) \to 0$ cuando $n \to +\infty$ y por tanto la serie

$$\sum_{k=0}^{+\infty} \binom{x}{k} a_k(f)$$

converge uniformemente en $\mathbb{Z}_p$. Más aún,

$$f(x) = \sum_{k=0}^{+\infty} \binom{x}{k} a_k(f). \tag{2.11}$$

Demostración. Dado que $\mathbb{Z}_p$ es compacto y f es continua, f es uniformemente continua. Por tanto, dado $s \in \mathbb{Z}_+$, existe un entero $t \in \mathbb{Z}_+$ tal que para $x, y \in \mathbb{Z}_p$,

$$|x-y|_p \leq p^{-t} \implies |f(x)-f(y)|_p \leq p^{-s}.$$

En particular,

$$|f(k+p^t)-f(k)|_p \leq p^{-s},$$

para $k = 0, 1, 2, \cdots$. También dado que f es continua en $\mathbb{Z}_p$ y $\mathbb{Z}_p$ es compacto, entonces f es acotada en $\mathbb{Z}_p$. Sin pérdida de generalidad, supongamos que $|f(x)|_p \leq 1$ para todo $x \in \mathbb{Z}_p$, entonces $|a_n(f)|_p \leq 1$ para todo n. Por Lema 2.25 y la fórmula para $a_n(f)$ que allí se presenta, tenemos:

$$\sum_{j=0}^{p^t} \binom{p^t}{j} a_{n+j}(f) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k+p^t),$$

luego

$$a_{n+p^t}(f) + a_n(f) + \sum_{j=1}^{p^t-1} \binom{p^t}{j} a_{n+j}(f) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k+p^t),$$

de manera que

$$a_{n+p^t}(f) + \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k) = -\sum_{j=1}^{p^t-1} \binom{p^t}{j} a_{n+j}(f) + \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k+p^t),$$

con lo cual

$$a_{n+p^t}(f) = -\sum_{j=1}^{p^t-1} \binom{p^t}{j} a_{n+j}(f) + \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} [f(k+p^t) - f(k)].$$

Dado que $\binom{p^t}{j} \equiv 0 \pmod{p}$ para $1 \leq j < p^t$, tenemos

$$|a_{n+p^t}(f)|_p \leq \max_{1 \leq j < p^t} \{p^{-1}|a_{n+j}(f)|_p, p^{-s}\} \implies |a_k(f)|_p \leq p^{-1} \text{ para } k \geq p^t,$$

ya que $|a_{n+j}(f)|_p \leq 1$, para $1 \leq j < p^t$.

Reemplazando n por $n+p^t$ en la penúltima desigualdad tenemos que

$$|a_{n+2p^t}|_p \leq \max_{1 \leq j < p^t} \{p^{-1}|a_{n+p^t+j}(f)|_p, p^{-s}\} \implies |a_k(f)|_p \leq p^{-2} \text{ para } k \geq 2p^t$$

ya que por lo anterior $|a_{n+p^t+j}(f)|_p \leq p^{-1}$. Repitiendo este proceso $(s-1)$-veces, tenemos que:

$$|a_k(f)|_p \leq p^{-s} \text{ para } k \geq sp^t,$$

luego como $s \in \mathbb{Z}_+$ es arbitrario $|a_k(f)|_p \to 0$ cuando $k \to +\infty$. De modo que, la serie

$$\sum_{k=0}^{+\infty} \binom{x}{k} a_k(f), \quad \text{con } x \in \mathbb{Z}_p$$

converge a $f(x)$, ya que ambas funciones son continuas y por la fórmula de inversión binomial para $a_n(f)$ con $n \in \mathbb{Z}_+$, tenemos que

$$f(n) = \sum_{k=0}^{n} \binom{n}{k} a_k(f),$$

esto es, ambas funciones coinciden en un subconjunto denso de $\mathbb{Z}_p$, además de que

$$\left| \binom{x}{k} \right|_p \leq 1 \quad \text{para } x \in \mathbb{Z}_p.$$

□

Corolario 2.28. *Sea $(a_n)_{n\geq 1}$ una sucesión en $\mathbb{C}_p$. Definamos*

$$b_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} a_k.$$

Entonces, existe una función continua $f : \mathbb{Z}_p \to \mathbb{C}_p$ tal que $f(n) = a_n$ si y solo si $b_n \to 0$ en norma p-ádica cuando $n \to +\infty$.

Demostración. La condición necesaria se sigue directamente del teorema anterior haciendo $b_n = a_n(f)$, con $f(k) = a_k$. Recíprocamente, por la fórmula de inversión binomial para b_n, tenemos que

$$a_n = \sum_{k=0}^{n} \binom{n}{k} b_k,$$

al definir la función $f : \mathbb{Z}_p \to \mathbb{C}_p$ como

$$f(x) = \sum_{k=0}^{+\infty} \binom{x}{k} b_k,$$

notamos que la serie converge ya que $b_n \to 0$ en norma p-ádica y por tanto define una función que es uniformemente continua con $f(n) = a_n$.

□

Planteamos a continuación en que subconjuntos de $\mathbb{C}_p$ se obtiene convergencia para determinada función continua p-ádica. Bajo ciertas condiciones, es posible mostrar que la serie anterior se extiende a una función analítica para $|x|_p < R$ con $R > 1$, es decir un conjunto más grande que $\mathbb{Z}_p$.

Lema 2.29. *Sea $P_i(x) = \sum_{n=0}^{\infty} a_{n,i} x^n$ una sucesión de series de potencias que convergen en algún subconjunto fijo D de $\mathbb{C}_p$. Supongamos que para cada n, $a_{n,i} \to a_{n,0}$ cuando $i \to \infty$ y que para cada $x \in D$ y $\varepsilon > 0$ existe $n_0 = n_0(x, \varepsilon)$ tal que*

$$\left| \sum_{n>n_0} a_{n,i} x^n \right|_p < \varepsilon \tag{2.12}$$

uniformemente en i. Entonces $\lim_{i\to\infty} P_i(x) = P_0(x)$ para todo $x \in D$.

Demostración. Dado $\varepsilon > 0$ y $x \in D$ por hipótesis existe $n_0 = n_0(x, \varepsilon)$ tal que se satisface (2.12). Entonces,

$$\begin{aligned}
|P_0(x) - P_i(x)|_p &= \left|\sum_{n=0}^{+\infty}(a_{n,0} - a_{n,i})x^n\right|_p \\
&= \left|\sum_{n=0}^{n_0}(a_{n,0} - a_{n,i})x^n + \sum_{n>n_0}(a_{n,0} - a_{n,i})x^n\right|_p \\
&\leq \max\left\{\left|\sum_{n=0}^{n_0}(a_{n,0} - a_{n,i})x^n\right|_p, \left|\sum_{n>n_0} a_{n,0}x^n\right|_p, \left|\sum_{n>n_0} a_{n,i}x^n\right|_p\right\} \\
&\leq \max_{0\leq n\leq n_0}\{|a_{n,0} - a_{n,i}|_p|x|_p^n, \varepsilon\} = \varepsilon,
\end{aligned}$$

para i suficientemente grande ya que tenemos que $a_{n,i} \to a_{n,0}$.

□

Teorema 2.30. *Sea $r < p^{-1/(p-1)} < 1$ y para $x \in \mathbb{C}_p$,*

$$f(x) = \sum_{n=0}^{+\infty}\binom{x}{n}a_n,$$

con $|a_n|_p \leq Mr^n$ para algún $M > 0$. Entonces $f(x)$ puede ser expresada como serie de potencias con radio de convergencia de al menos $R = (rp^{1/(p-1)})^{-1}$.

Observación 2.31. *Note que $R > 1$ luego el teorema da una región más amplia de convergencia de de la función f definida como serie de Mahler.*

Demostración. Consideremos las sumas parciales

$$P_i(x) = \sum_{n\leq i}\binom{x}{n}a_n = \sum_{n\leq i}a_{n,i}x^n.$$

Entonces

$$a_{n,i} = a_n\frac{\text{entero}}{n!} + a_{n+1}\frac{\text{entero}}{(n+1)!} + \cdots,$$

por lo tanto

$$|a_{n,i}|_p \leq \max_{j\geq n}\left|\frac{a_j}{j!}\right|_p \leq \max_{j\geq n} Mr^j p^{j/(p-1)} \leq MR^{-n},$$

ya que $\nu_p(j!) \leq j/(p-1)$ (ver, Apéndice C. Lema C.7). También,

$$\begin{aligned}
|a_{n,i} - a_{n,i+k}|_p &= \left|a_{i+1}\frac{\text{entero}}{(i+1)!} + \cdots + a_{i+k}\frac{\text{entero}}{(i+k)!}\right|_p \\
&\leq MR^{-(i+1)} \longrightarrow 0 \text{ cuando } i \to +\infty.
\end{aligned}$$

Por consiguiente $(a_{n,i})_{i\geq 1}$ es una sucesión de Cauchy, definamos $a_{n,0} = \lim_{i\to\infty} a_{n,i}$, entonces $|a_{n,0}|_p \leq MR^{-n}$. Ahora tomamos

$$P_0(x) = \sum_{n=0}^{+\infty}a_{n,0}x^n.$$

Observemos que

$$\limsup \sqrt[n]{|a_{n,0}|_p} \leq \frac{1}{R} \limsup \sqrt[n]{M} = \frac{1}{R} \implies R \leq \rho = \frac{1}{\limsup \sqrt[n]{|a_n|_p}}.$$

Entonces, P_0 converge para $x \in \mathbb{C}_p$, con $|x|_p < R$. Por otro lado, como los P_i son polinomios ellos convergen en

$$D = \{x \in \mathbb{C}_p : |x|_p < R\}.$$

Adicionalmente, para $|x|_p < R$, tenemos que $|x|_p R^{-1} < 1$, por consiguiente:

$$|x|_p^{n+1} R^{-n-1} < |x|_p^n R^{-n}, \quad \forall\, n \in \mathbb{Z}_+,$$

de modo que

$$\left| \sum_{n>n_0} a_{n,i} x^n \right|_p \leq \max_{n>n_0} \{MR^{-n}|x|_p^n\} < MR^{-n_0}|x|_p^{n_0} \longrightarrow 0$$

cuando $n_0 \to \infty$ uniformemente en i. Luego por el lema anterior, $|P_0(x) - P_i(x)|_p \leq \varepsilon$ uniformemente para $|x|_p < R$. De manera que $f(x)$ es analítica en D, como se quería demostrar.

□

Observación 2.32. *Por el Teorema de Mahler (ver Teorema 2.27)*

$$f(x) = \sum_{n=0}^{+\infty} \binom{x}{n} a_n(f)$$

es una función continua siempre que se satisfagan las condiciones de Teorema 2.18. Si, adicionalmente, la sucesión $a_n = f(n)$ satisface las condición de crecimiento del Teorema 2.30, i.e., $|a_n|_p \leq Mr^n$ para algún $M > 0$, entonces obtenemos una continuación analítica p-ádica de $f(x)$ a un dominio más amplio.

En el siguiente capítulo, usaremos el Teorema 2.30 para obtener una continuación analítica p-ádica de la función zeta de Riemann y más generalmente de las funciones L de Dirichlet.

Observación 2.33. *Podemos dar ahora una aplicación a la teoría de interpolación dada hasta el momento. Si $n \equiv 1$ (mód p), como se mostró en la Observación 2.19, la función $f(m) = n^m$, con $m \in \mathbb{Z}_+$ admite una extensión como función continua $\hat{f} : \mathbb{Z}_p \to \mathbb{Q}_p$, tal que $\hat{f}(m) = f(m)$. Luego por el Teorema de Mahler (ver Teorema 2.27) tenemos que:*

$$\hat{f}(s) = \sum_{k=0}^{+\infty} \binom{s}{k} a_k(\hat{f}), \quad s \in \mathbb{Z}_p$$

donde $a_k(\hat{f}) \to 0$ cuando $k \to \infty$, siendo

$$a_k(\hat{f}) = \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} \hat{f}(j).$$

Por otro lado, como $\hat{f}(m) = f(m) = n^m$ *si* $m \in \mathbb{Z}_+$, *entonces para* $k \in \mathbb{Z}_+$

$$\begin{aligned} a_k(\hat{f}) &= \sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}n^j \\ &= \sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}(1-(n-1))^j \\ &= \sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}\sum_{i=0}^{j}\binom{j}{i}(n-1)^i \\ &= \sum_{i=0}^{j}(n-1)^i(-1)^k\sum_{j=0}^{k}(-1)^{-j}\binom{k}{j}\binom{j}{i} \\ &= \sum_{i=0}^{j}(n-1)^i(-1)^k\sum_{j=0}^{k}(-1)^{j}\binom{k}{j}\binom{j}{i} \\ &= (n-1)^k \end{aligned}$$

ya que por la relación de ortogonalidad (2.6), la suma interna es $(-1)^k$ *solo si* $i = k$ *y* 0 *si* $i \neq k$. *Entonces al definir*

$$n^s := \hat{f}(s) = \sum_{k=0}^{+\infty}\binom{s}{k}(n-1)^k, \qquad \forall\ s \in \mathbb{Z}_p,$$

Al tomar $M = 1$ *y* $r = p^{-1}$, *como* $n \equiv 1$ *(mód p), entonces:*

$$|(n-1)^k|_p \leq p^{-k} = Mr^k,$$

de manera que por el Teorema 2.30, n^s *define una función analítica p-ádica con radio de convergencia* $R = p^{(p-2)/(p-1)} > 1$, *i.e.,* n^s *está bien definida para todo* $s \in \mathbb{C}_p$, *con* $|s|_p < p^{(p-2)/(p-1)}$.

2.3. Carácter de Teichmüller

Observación 2.34. *Para simplificar notación, introducimos un parámetro q como sigue:*

$$q = \begin{cases} p & si \quad p > 2, \\ 4 & si \quad p = 2. \end{cases}$$

Sea $f(X) = X^m - 1 \in \mathbb{Z}_p[X]$, *con* $m|(p-1)$. *Entonces la congruencia* $f(X) \equiv 0$ *(mód p), tiene m soluciones distintas ya que* $(\mathbb{Z}/p\mathbb{Z})^\times$ *es un grupo cíclico de orden* $p-1$ *(ver [1], Teorema 10.4, cap. 10, pág. 207) y para cada una de estas soluciones, las condiciones del Lema de Hensel (ver Apéndice C, Lema C.27) se satisfacen, luego cada una de ellas pueden ser levantadas a* $\mathbb{Q}_p$.

En particular, si $p > 2$ *y* $m = p-1$ *vemos que para cada* $1 \leq j \leq p-1$ *existe un número* $\omega(j) \in \mathbb{Z}_p$ *tal que* $\omega(j) \equiv j$ *(mód p) y* $\omega(j)^{p-1} = 1$ *(Lema de Hensel), es decir en* $\mathbb{Z}_p$ *se encuentran todas las* $(p-1)$*-raíces de la unidad, más aún, estas raíces se encuentran en* $\mathbb{Z}_p^\times$, *si* $p = 2$, *tenemos que la congruencia* $x^2 \equiv 1$ *(mód 4)*

posee exactamente dos soluciones que pueden ser levantadas a $\mathbb{Q}_2$. Luego, el número de raíces de la unidad en $\mathbb{Q}_p$ es siempre $\varphi(q)$, dónde φ es la función indicatriz de Euler.

El punto es que la función exponencial p-ádica $\exp_p(x)$ estará definida en $q\mathbb{Z}_p$ (ver Definición 2.8) y el logaritmo p-ádico $\log_p(x)$ estará definido en $1+q\mathbb{Z}_p$ (ver Definición 2.13).

Definamos dos subconjuntos de $\mathbb{Z}_p^\times$:

$$U = \{x \in \mathbb{Z}_p^\times : |x-1|_p < 1\},$$

y

$$U_1 = \{x \in \mathbb{Z}_p^\times : |x-1|_p < p^{-1/(p-1)}\}.$$

Notemos que:

- Si $x \in 1 + p\mathbb{Z}_p$, entonces $x = 1 + p \cdot a$ con $a \in \mathbb{Z}_p$, de modo que

  $$|x-1|_p = |p \cdot a|_p = |p|_p |a|_p \leq p^{-1} < 1,$$

  así $x \in U$. Recíprocamente, si $x \in U$, tenemos que $|x-1|_p < 1$, i.e., $\nu_p(x-1) > 0$, que es lo mismo que $\nu_p(x-1) \geq 1$, con lo cual:

  $$x \equiv 1 \ (\text{mód } p\mathbb{Z}_p) \implies x - 1 = p \cdot a, \text{ con } a \in \mathbb{Z}_p,$$

  así $x \in 1 + p\mathbb{Z}_p$. De lo anterior, $U = 1 + p\mathbb{Z}_p$.

- Si $x \in U_1$, entonces $|x-1|_p < p^{-1/(p-1)} \leq p^0 = 1$, luego $x \in U$, i.e., $U_1 \subseteq U \subset \mathbb{Z}_p^\times$. Por otro lado, si $p > 2$ y $x \in 1 + p\mathbb{Z}_p$, entonces $|x-1|_p < 1$, i.e., $\nu_p(x-1) \geq 1$, con lo cual:

  $$|x-1|_p = p^{-\nu_p(x-1)} \leq p^{-1} < p^{-1/(p-1)}, \text{ si } p > 2,$$

  así $x \in U_1$, de modo que por el item anterior $x \in U$, luego, $U_1 = U$ siempre que $p > 2$.

- Si $p = 2$, tenemos que

  $$U_1 = \{x \in \mathbb{Z}_2^\times : |x-1|_2 < 2^{-1}\},$$

  de tal forma que si $x \in U_1$, entonces $\nu_2(x-1) > 1$, i.e., $\nu_2(x-1) \geq 2$, luego:

  $$x \equiv 1 \ (\text{mód } 2^2\mathbb{Z}_2) \iff x - 1 = 4 \cdot a, \text{ con } a \in \mathbb{Z}_2,$$

  así $U_1 \subseteq 1 + 4\mathbb{Z}_2$. Recíprocamente, si $x \in 1 + 4\mathbb{Z}_2$, entonces, $x - 1 = 4 \cdot a$, con $a \in \mathbb{Z}_2$, de modo que:

  $$|x-1|_2 = |4 \cdot a|_2 = |4|_2 |a|_2 \leq |4|_2 = 2^{-2} < 2^{-1},$$

  con lo cual $1 + 4\mathbb{Z}_2 \subseteq U_1$.

Hemos probado entonces que $U = 1 + p\mathbb{Z}_p$ y $U_1 = 1 + q\mathbb{Z}_p$. En consecuencia $U_1 \subseteq U$, además $U_1 = U$ siempre que $p > 2$, y de la mismas identidades tenemos que U y U_1 son subgrupos de $\mathbb{Z}_p^\times$.

Proposición 2.35. *Sean U y U_1 como están definidos anteriormente, y sea:*

$$W = \{x \in \mathbb{Z}_p : |x|_p < p^{-1/(p-1)}\} = q\mathbb{Z}_p,$$

considerado como grupo aditivo.

(i) El logaritmo p-ádico $\log_p$ define un homomorfismo de grupos

$$\log_p : U \longrightarrow \mathbb{Z}_p^+,$$

cuya imagen está contenida en el ideal $p\mathbb{Z}_p$.

(ii) El logaritmo p-ádico $\log_p$ define un isomorfismo de grupos

$$\log_p : U_1 \longrightarrow W,$$

con inversa $\exp_p$. En particular, $U_1 \cong W \cong \mathbb{Z}_p^+$ es libre de torsión.

Observación 2.36. *Un grupo es libre de torsión si no existen elementos $x \neq 1$ tal que $x^m = 1$ para algún m.*

Demostración. Ver [11], Proposición 4.5.9, pág. 121. □

Corolario 2.37. *Para p-primo, tenemos un isomorfismo $\mathbb{Z}_p^\times \cong V \times U_1$, donde $U_1 \cong \mathbb{Z}_p^+$ es un grupo libre de torsión y V es la parte de torsión de $\mathbb{Z}_p^\times$. Más aún:*

(i) V es el conjunto de raíces de la unidad en $\mathbb{Q}_p$, el cual es subgrupo de $\mathbb{Z}_p^\times$, y

(ii) $V \cong (\mathbb{Z}/q\mathbb{Z})^\times$, luego V es un grupo cíclico de orden $\varphi(q)$, donde φ es la función indicatriz de Euler.

Demostración. Ver [11], Corolario 4.5.10, pág 122. □

Observación 2.38. *Una consecuencia directa del corolario anterior, es que para un primo $p > 2$, existe una inclusión*

$$\omega : \mathbb{F}_p^\times \cong V \hookrightarrow \mathbb{Z}_p^\times,$$

*donde $\mathbb{F}_p$ es el campo con p elementos. Podemos extender ω a $\mathbb{F}_p$ tomando $\omega(0) = 0$. La función ω es llamada el **representante de Teichmüller**, y este aparece frecuentemente de muchas formas diferentes. Si componemos esta función con el mapeo "reducción módulo p" de $\mathbb{Z}$ a $\mathbb{F}_p$,*

$$\mathbb{Z} \longrightarrow \mathbb{F}_p \xrightarrow{\omega} \mathbb{Z}_p\,,$$

*obtenemos un carácter de Dirichlet con valores en $\mathbb{Z}_p$, el cual es usualmente llamado el **carácter de Teichmüller** y se denota por ω. Si $p = 2$, por el Corolario 2.37 (ii), $V \cong (\mathbb{Z}/4\mathbb{Z})^\times$, definimos*

$$\omega : V \cong (\mathbb{Z}/4\mathbb{Z})^\times \hookrightarrow \mathbb{Z}_2^\times,$$

extendemos a todo $\mathbb{Z}/4\mathbb{Z}$ *tomando* $\omega(x) = 0$ *si* $m.c.d(x,2) > 1$, *al componer esta función con el mapeo "reducción módulo* 4*"* de $\mathbb{Z}$ *a* $\mathbb{Z}/4\mathbb{Z}$,

$$\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \xrightarrow{\omega} \mathbb{Z}_2 \ ,$$

obtenemos un carácter de Dirichlet con valores en $\mathbb{Z}_2$. *En efecto, debemos mostrar que para* $j, k \in (\mathbb{Z}/q\mathbb{Z})^\times$ *se cumple que* $\omega(jk) = \omega(j)\omega(k)$, *como*

$$\begin{array}{ccccc} \omega(j) \equiv j \ (\textit{mód } q) & y & \omega(k) \equiv k \ (\textit{mód } q) & \Longrightarrow & \omega(j)\omega(k) \equiv jk \ (\textit{mód } q), \\ \omega(j)^{p-1} = 1 & y & \omega(k)^{p-1} = 1 & \Longrightarrow & (\omega(j)\omega(k))^{p-1} = 1, \quad \textit{si } p > 2, \\ \omega(j)^2 = 1 & y & \omega(k)^2 = 1 & \Longrightarrow & (\omega(j)\omega(k))^2 = 1, \quad \textit{si } p = 2. \end{array}$$

Por la unicidad en el Lema de Hensel $\omega(jk) = \omega(j)\omega(k)$, *si* $p > 2$. *Si* $p = 2$ *la unicidad se establece por las dos posibilidades de solución de la congruencia* $x^2 \equiv 1$ *(mód* 4*).*

Como el caso del carácter de Dirichlet (ver Apéndice B, Definición B.9), vamos a definir el carácter de Teichmüller para utilizarlo en cálculos explícitos más adelante.

Definición 2.39. ***Carácter de Teichmüller*** *Para* $x \in \mathbb{Z}$, *definamos*

$$\omega(x) = \begin{cases} \omega(x \ \textit{mód } p) & \textit{si} \quad x \neq 0, \\ 0 & \textit{si} \quad x = 0. \end{cases}$$

Observación 2.40. *Nuestro objetivo es hacer una extensión de este carácter a un subconjunto de* $\mathbb{Q}_p$, *p-primo, y demostrar que cumple propiedades analíticas deseables.*

Dado $a \in \mathbb{Z}_p^\times$ *por el Corolario 2.37, podemos escribir*

$$a = \omega(a)\langle a \rangle,$$

donde ω *es el carácter de Teichmüller y a su vez la proyección de* $\mathbb{Z}_p^\times$ *sobre* V *y* $\langle a \rangle$ *es la proyección de* $\mathbb{Z}_p^\times$ *sobre* $U_1 = 1 + q\mathbb{Z}_p$. *Luego, como* $\omega(a) \equiv a$ *(mód* q*), tenemos*

$$\omega(a)\langle a \rangle \equiv \omega(a) (\textit{mód } q) \implies \langle a \rangle \equiv 1 (\textit{mód } q),$$

ya que $\omega(a) \in \mathbb{Z}_p^\times$, *esto es,* $|\langle a \rangle - 1|_p \leq q^{-1}$.

Consideremos la función $f(s) = \langle a \rangle^s$, *con* $a \in \mathbb{Z}_p^\times$ *y* $s \in \mathbb{Z}_p$, *la cual definimos:*

$$f(s) = \langle a \rangle^s := \exp_p(s \log_p \langle a \rangle).$$

Por Lema 2.16, tenemos que:

$$|\log_p \langle a \rangle|_p = |\log_p(1 + (\langle a \rangle - 1))|_p \leq |\langle a \rangle - 1|_p \leq q^{-1},$$

la función así definida converge para $|s|_p < qp^{-1/(p-1)}$. *Si* $s = 1$ *entonces* $\langle a \rangle^1 = \langle a \rangle$ *ya que* $\exp_p(\log_p \langle a \rangle) = \langle a \rangle$.

Por otro lado, usando un razonamiento análogo al utilizado en la Observación 2.33, podemos expandir en serie:

$$(1+(\langle x\rangle-1))^s=\sum_{n=0}^{+\infty}\binom{s}{n}(\langle x\rangle-1)^n.$$

Dado que $|\langle x\rangle-1|_p\leq q^{-1}$, *podemos tomar* $r=q^{-1}$ *y* $M=1$ *en el Teorema 2.30. Y concluimos que esta serie representa una función analítica con radio de convergencia* $R=qp^{-1/(p-1)}$. *De hecho*

$$\exp_p(s\log_p\langle a\rangle)=\sum_{n=0}^{+\infty}\binom{s}{n}(\langle a\rangle-1)^n$$

ya que las funciones son analíticas en s *y son iguales cuando* $s\in\mathbb{Z}_+$. *Como los enteros positivos tienen a* 0 *como punto de acumulación p-ádico, las funciones deben ser identicamente iguales.*

Capítulo 3

Funciones L de Dirichlet y L p-ádicas

En este capítulo construimos las funciones L p-ádicas interpolando valores especiales de las funciones L de Dirichlet clásicas, a saber, aquellos valores que involucran a los números de Bernoulli. Las funciones L p-ádicas que surgen de este método son usualmente llamadas *funciones L p-ádicas analíticas*, utilizando después estas funciones para lograr una nueva deducción de las congruencias de Kummer.

En el camino, omitiendo algunos detalles técnicos, tratamos la extensión analítica de las funciones L de Dirichlet clásicas deduciendo su ecuación funcional, esto con el fin de hacer un paralelo entre los métodos utilizados en análisis complejo y análisi p-ádico a la hora de definir funciones analíticas en determinado conjunto de convergencia, ya sea $\mathbb{C}$ o $\mathbb{C}_p$.

3.1. Funciones L de Dirichlet y función zeta de Hurwitz

De la Definición B.9, si χ es un carácter de Dirichlet primitivo módulo $f \in \mathbb{Z}_+$ (f es conductor para χ), extendemos χ a todos los números enteros por:

$$\chi(n) = \begin{cases} \chi(n \text{ mód } f) & \text{si} \quad \text{m.c.d}(n, f) = 1 \\ 0 & \text{si} \quad \text{m.c.d}(n, f) \neq 1. \end{cases}$$

Definición 3.1. *Para $s = \sigma + it \in \mathbb{C}$, con $\sigma > 1$. La serie de Dirichlet asociada al carácter de Dirichlet primitivo módulo $f \in \mathbb{Z}_+$, está dada por:*

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

Notemos que si $\chi = \chi_1$ el carácter principal, la serie L de Dirichlet se reduce a la

función zeta de Riemann (ver Apéndice A. Definición A.1), es decir:

$$L(s,\chi_1)=\sum_{n=1}^{+\infty}\frac{\chi_1(n)}{n^s}=\sum_{n=1}^{+\infty}\frac{1}{n^s}=\zeta(s).$$

Para estudiar estas series L de Dirichlet introducimos la función zeta de Hurwitz:

Definición 3.2. *Definimos la serie zeta de Hurwitz como*

$$\zeta(s,x)=\sum_{n=0}^{+\infty}\frac{1}{(n+x)^s},\quad 0<x\leq 1.$$

Cuando $x=1$ la serie zeta de Hurwitz se reduce a la serie zeta de Riemann, $\zeta(s)=\zeta(s,1)$.

Proposición 3.3. *La serie $\zeta(s,x)$ converge absolutamente para $Re(s)>1$. La convergencia es uniforme en cada semiplano $Re(s)\geq 1+\alpha$, $\alpha>0$, luego $\zeta(s,x)$ es una función analítica en el semiplano $Re(s)>1$.*

Demostración. Sea $\sigma=\mathrm{Re}(s)$, si $\sigma\geq 1+\alpha$, entonces

$$\sum_{n=1}^{+\infty}|(n+x)^{-s}|=\sum_{n=1}^{+\infty}(n+x)^{-\sigma}\leq\sum_{n=1}^{+\infty}(n+x)^{-(1+\alpha)}<+\infty,$$

lo anterior se cumple para todo $\alpha>0$, y procediendo de forma análoga a la prueba de la Proposición A.2, se completa la demostración.

□

Observación 3.4. *Históricamente, Hurwitz introdujo su función zeta con el propósito explícito de derivar una continuación analítica para la serie $L(s,\chi)$, observando que esta serie se puede expresar como una combinación lineal de funciones zeta de Hurwitz.*

En efecto, sea χ carácter de Dirichlet módulo f el conductor de χ y $s=\sigma+it$, con $\sigma>1$. Reordenando los términos en la serie $L(s,\chi)$ de acuerdo a las clases residuales módulo f. Esto es:

$$n=mf+a,\quad \textit{donde } 1\leq a\leq f\quad y\quad m=0,1,2,\cdots,$$

obtenemos

$$\begin{aligned}L(s,\chi)&=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}\\&=\sum_{a=1}^{f}\sum_{m=0}^{\infty}\frac{\chi(mf+a)}{(mf+a)^s}\\&=\frac{1}{f^s}\sum_{a=1}^{f}\chi(a)\sum_{m=0}^{\infty}\frac{1}{(m+a/f)^s}\\&=f^{-s}\sum_{a=1}^{f}\chi(a)\zeta(s,a/f).\end{aligned}$$

En vista de lo anterior, hemos deducido que:

$$L(s,\chi) = f^{-s}\sum_{a=1}^{f}\chi(a)\zeta\left(s,\frac{a}{f}\right).$$

Luego esta representación de $L(s,\chi)$ como combinación lineal de funciones zeta de Hurwitz muestra que las propiedades de las funciones L dependen de las propiedades de $\zeta(s,a/f)$. Por ejemplo, de la Proposición 3.3 deducimos que $L(s,\chi)$ define una función analítica de s en el semiplano $Re(s) > 1$.

Como primer objetivo, deseamos obtener la continuación analítica de $\zeta(s,x)$ más allá de la línea $\sigma = 1$, la cual nos dará la continuación analítica de las funciones L de Dirichlet. Existen varias formas de hacerlo, nosotros utilizaremos una que no involucra integral de contorno y después describiremos otra que si involucra integral de contorno, la cual nos proporciona nuestro segundo objetivo, obtener ecuaciones funcionales para las funciones $L(s,\chi)$, pues son con estas ecuaciones que usualmente se trabaja después de realizada la continuación analítica.

3.1.1. Continuación analítica de $\zeta(s,x)$ sin integral de contorno

El objetivo de esta sección es obtener el siguiente resultado:

$$L(1-n,\chi) = -\frac{B_{n,\chi}}{n} \quad n \in \mathbb{Z}_+,$$

donde $B_{n,\chi}$ son los números de Bernoulli generalizados presentados en el Capítulo 1. Para esto, utilizamos las propiedades de la función zeta de Hurwitz, las cuales necesitan de su continuación analítica.

Aunque la continuación analítica al plano complejo de una función que es holomorfa en una región conexa del plano, es única. Y dado que la continuación analítica de la función zeta de Hurwitz utilizando el método clásico de la integral de contorno, proporciona ecuaciones funcionales para las funciones L de Dirichlet. No deja de ser interesante, ver métodos alternativos para resolver un mismo problema, pues usando técnicas variadas, podríamos resolver cuestiones que impliquen conceptos parecidos, de una forma que no sea la usual. Este método, es el utilizado esencialmente por Murty y Sinha en [19].

Lema 3.5. *Sea $s \in \mathbb{C}$, con $Re(s) > 1$, entonces*

$$\log\left|\binom{-s}{r}\right| \leq \sum_{j=1}^{r}\log\left(1+\frac{|s|}{j}\right) \ll |s|M\log r, \quad r \in \mathbb{Z}_{>1} \text{ y } M > 0.$$

Demostración. Tenemos que:

$$\left|\binom{-s}{r}\right| = \frac{|-s(-s-1)(-s-2)\cdots(-s-r+1)|}{|1\cdot 2\cdot 3\cdots(r-1)\cdot r|} = \left|\frac{s}{r}\right|\cdot\left|\frac{s+1}{1}\right|\cdot\left|\frac{s+2}{2}\right|\cdots\left|\frac{s+(r-1)}{r-1}\right|,$$

entonces

$$\begin{aligned}\log\left|\binom{-s}{r}\right| &= \log\left|1+\frac{s}{1}\right| + \log\left|1+\frac{s}{2}\right| + \cdots + \log\left|1+\frac{s}{r-1}\right| + \log\left|\frac{s}{r}\right| \\ &\leq \log(1+|s|) + \log\left(1+\frac{|s|}{2}\right) + \cdots + \log\left(1+\frac{|s|}{r-1}\right) + \log\left(\frac{|s|}{r}\right) \\ &\leq \sum_{j=1}^{r}\log\left(1+\frac{|s|}{j}\right) < |s|\sum_{j=1}^{r}\frac{1}{j} = |s|\left(-\log r + \sum_{j=1}^{r}\frac{1}{j} + \log r\right) \\ &\leq |s| + |s|\log r,\end{aligned}$$

el último paso en la desigualdad anterior debido a la definición de la constante de Euler-Mascheroni (ver [1], pág. 53), a saber:

$$\gamma = \lim_{r\to\infty}\left(-\log r + \sum_{j=1}^{r}\frac{1}{j}\right) < 1.$$

Luego al tomar $M_0 > 0$ tal que $M_0 \log r > 1$, el teorema queda demostrado al elegir $M = M_0 + 1$.

□

Teorema 3.6. *La serie $\zeta(s,x)$, con $0 < x \leq 1$, define una función meromorfa en $\mathbb{C}$ con polo simple en $s = 1$.*

Demostración. Como para $x = 1$, la función zeta de Hurwitz es igual a la función zeta de Riemann, por Proposición A.11, esta define una función meromorfa con polo simple en $s = 1$. Podemos considerar entonces $0 < x < 1$, por otra parte notando que:

$$\zeta(s,x) = x^{-s} + \sum_{n=1}^{+\infty}\frac{1}{(n+x)^s} \quad \text{y} \quad \zeta(s) = \sum_{n=1}^{+\infty}\frac{1}{n^s}$$

obtenemos

$$-x^{-s} + \zeta(s,x) - \zeta(s) = \sum_{n=1}^{+\infty}\left(\frac{1}{(n+x)^s} - \frac{1}{n^s}\right). \tag{3.1}$$

Por otro lado, como

$$\frac{1}{(n+x)^s} - \frac{1}{n^s} = \frac{1}{n^s}\left[\left(1+\frac{x}{n}\right)^{-s} - 1\right],$$

entonces para $n \in \mathbb{Z}_+$, se cumple que $|x/n| < 1$, así por teorema del binomio

$$\left(1+\frac{x}{n}\right)^{-s} = \sum_{r=0}^{+\infty}\binom{-s}{r}\frac{x^r}{n^r},$$

luego

$$\frac{1}{n^s}\left[\left(1+\frac{x}{n}\right)^{-s} - 1\right] = \frac{1}{n^s}\sum_{r=1}^{+\infty}\binom{-s}{r}\frac{x^r}{n^r}$$

reemplazando en (3.1):

$$\begin{aligned}\sum_{n=1}^{+\infty}\left(\frac{1}{(n+x)^s}-\frac{1}{n^s}\right) &= \sum_{n=1}^{+\infty}\left[\frac{1}{n^s}\sum_{r=1}^{+\infty}\binom{-s}{r}\frac{x^r}{n^r}\right]\\ &= \sum_{r=1}^{+\infty}\sum_{n=1}^{+\infty}\left[\binom{-s}{r}\frac{x^r}{n^{s+r}}\right]\\ &= \sum_{r=1}^{+\infty}\binom{-s}{r}x^r\sum_{n=1}^{+\infty}\frac{1}{n^{s+r}}\\ &= \sum_{r=1}^{+\infty}\binom{-s}{r}x^r\zeta(s+r).\end{aligned}$$

Hemos deducido que:

$$-\frac{1}{x^s}+\zeta(s,x)-\zeta(s)=\sum_{r=1}^{+\infty}\binom{-s}{r}\zeta(s+r)x^r, \tag{3.2}$$

con $\mathrm{Re}(s)>1$. De hecho, como la función zeta de Riemann $\zeta(s)$ posee una extensión meromorfa a $\mathbb{C}$ con polo en $s=1$, si $\mathrm{Re}(s)>0$ entonces $\mathrm{Re}(s+r)=\mathrm{Re}(s)+r>1$, luego la serie de la derecha en (3.2) converge absolutamente en el semiplano $\mathrm{Re}(s)>0$. En efecto, para r suficientemente grande $|\zeta(s+r)|<C$, con $C>0$, aplicando el test de la raíz junto al Lema 3.5, tenemos que:

$$\left|\binom{-s}{r}\zeta(s+r)x^r\right|^{1/r} < C^{1/r}\left|\binom{-s}{r}\right|^{1/r} \ll \left(Ce^{M|s|}\right)^{1/r} r^{1/r} \longrightarrow 1,$$

cuando $r\to\infty$. Por tanto $\zeta(s,x)$ posee un polo en $s=1$ ya que $\zeta(s)$ cuenta con uno allí y es meromorfa en el semiplano $\mathrm{Re}(s)>0$. Procediendo inductivamente para $N\in\mathbb{Z}_+$, tenemos que:

$$\sum_{r=1}^{+\infty}\binom{-s}{r}\zeta(s+r)x^r=\sum_{r=1}^{N}\binom{-s}{r}\zeta(s+r)x^r+\sum_{r=N+1}^{+\infty}\binom{-s}{r}\zeta(s+r)x^r.$$

Si $\mathrm{Re}(s)>-N$, entonces $\mathrm{Re}(s+r)>1$ para los $r>N$ enteros, luego la segunda serie de la parte derecha converge absolutamente en esta región. Por otro lado

$$\binom{-s}{r}\zeta(s+r)x^r=\frac{(-1)^r}{r!}s(s+1)(s+2)\cdots(s+r-1)\zeta(s+r)x^r \quad \text{con} \quad r=1,2,\cdots,N.$$

Entonces, si $\mathrm{Re}(s)>-N$, la función $\zeta(s+r)$ posee un polo en $s=1-r$ que se cancela con la multiplicación por el coeficiente binomial $\binom{-s}{r}$. Con lo cual, la primera suma del lado derecho define una función meromorfa en el semiplano $\mathrm{Re}(s)>-N$. Como $N\in\mathbb{Z}_+$ es arbitrario, tenemos que la función

$$\zeta(s,x)=x^{-s}+\zeta(s)+\sum_{r=1}^{+\infty}\binom{-s}{r}\zeta(s+r)x^r$$

define una función meromorfa en $\mathbb{C}$ con polo en $s=1$. Por último, probemos que este polo es simple, en efecto

$$\lim_{s\to1}(s-1)\zeta(s,x)=\lim_{s\to1}(s-1)x^{-s}+\lim_{s\to1}(s-1)\zeta(s)+\lim_{s\to1}(s-1)\sum_{r=1}^{+\infty}\binom{-s}{r}\zeta(s+r)x^r=1.$$

□

Consideramos ahora, un análogo para la función zeta de Hurwitz, de la relación entre los números de Bernoulli y la función zeta de Riemman, a saber:

$$\zeta(1-k) = -\frac{B_k}{k} \quad k > 1.$$

Proposición 3.7. *Para $k \geq 2$ se cumple*

$$\zeta(1-k,x) = -\frac{B_k(x)}{k}, \quad 0 < x \leq 1,$$

donde $B_k(x)$ es el k-ésimo polinomio de Bernoulli.

Demostración. Por el teorema anterior tenemos que para $s \in \mathbb{C} - \{1\}$

$$-\frac{1}{x^s} + \zeta(s,x) - \zeta(s) = \sum_{r=1}^{+\infty} \binom{-s}{r} \zeta(s+r)x^r \tag{3.3}$$

$$= \sum_{r=1}^{+\infty} \frac{(-1)^r}{r!} s(s+1)\cdots(s+r-1)\zeta(s+r)x^r, \tag{3.4}$$

Si $s = 1-k$, tenemos para $r > k$ que los términos de la serie son iguales a cero, ya que $\zeta(1-k+r)$ es analítica y el coeficiente binomial $\binom{k-1}{r} = 0$.

Para $r = k$, notamos que $\zeta(1-k+r)$ posee un polo simple, luego al hacer variar r tenemos:

$$\lim_{r\to k}(r-k)\zeta(1-k+r) = 1,$$

esto implica que

$$\begin{aligned}
&\lim_{r\to k} \frac{(-1)^r}{r!}(1-r)(2-r)\cdots(r-1-k)(r-k)\zeta(1-k+r) \\
&= \frac{(-1)^k}{k!}\cdot(-1)^{k-1}\cdot(k-1)(k-2)\cdots 1 \cdot \lim_{r\to k}(r-k)\zeta(1-k+r) \\
&= -\frac{(k-1)!}{k!} = -\frac{1}{k},
\end{aligned}$$

luego al tomar el límite $s \to (1-k)$ en (3.3), tenemos que:

$$-\frac{1}{x^{1-k}} + \zeta(1-k,x) - \zeta(1-k) = -\frac{x^k}{k} + \sum_{r=1}^{k-1} \binom{k-1}{r} \zeta(1-k+r)x^r.$$

Por lo tanto

$$\begin{aligned}
\zeta(1-k,x) &= x^{k-1} + \zeta(1-k) - \frac{x^k}{k} + \sum_{r=1}^{k-1} \binom{k-1}{r} \zeta(1-k+r)x^r \\
&= x^{k-1} - \frac{B_k}{k} - \frac{x^k}{k} - \sum_{r=1}^{k-2} \binom{k-1}{r} \frac{B_{k-r}}{k-r} x^r + \zeta(0)x^{k-1} \\
&= \frac{x^{k-1}}{2} - \frac{B_k}{k} - \frac{x^k}{k} - \frac{1}{k}\sum_{r=1}^{k-2} \binom{k}{r} B_{k-r}x^r \\
&= -\frac{1}{k}kB_1x^{k-1} - \frac{1}{k}B_kx^0 - \frac{1}{k}B_0x^k - \frac{1}{k}\sum_{r=1}^{k-2} \binom{k}{r} B_{k-r}x^r \\
&= -\frac{1}{k}\sum_{r=0}^{k} \binom{k}{r} B_{k-r}x^r = -\frac{B_k(x)}{k}.
\end{aligned}$$

Dónde hemos utilizado los hechos

$$\zeta(1-k) = -\frac{B_k}{k} \quad \forall\ k \geq 2, \quad B_0 = 1, \quad \text{y} \quad \zeta(0) = B_1 = -\frac{1}{2}$$

□

Teorema 3.8. *Para el carácter principal χ_1 módulo f, la serie $L(s, \chi_1)$ define una función meromorfa en $\mathbb{C}$ con polo en $s = 1$ y residuo $\varphi(f)/f$. Si $\chi \neq \chi_1$, entonces $L(s, \chi)$ define una función entera.*

Demostración. Por Observación 3.4 sabemos que

$$L(s, \chi) = f^{-s} \sum_{b=1}^{f} \chi(b)\zeta(z, b/f)$$

De esta combinación lineal se sigue la continuación analítica para $L(s, \chi)$ por la proposición anterior. Más aún, sabemos por Apéndice B, Teorema B.13 (iii) que:

$$\sum_{b \pmod f} \chi(b) = \begin{cases} \varphi(f) & \text{si} \quad \chi = \chi_1, \\ 0 & \text{si} \quad \chi \neq \chi_1. \end{cases}$$

Dado que $\zeta(s, b/f)$ posee un polo simple en $s = 1$ con residuo 1, la función $\chi(b)\zeta(s, b/f)$ posee un polo simple en $s = 1$ con residuo $\chi(b)$. De modo que:

$$\begin{aligned} \text{Res}_{s=1} L(s, \chi) &= \lim_{s \to 1}(s-1)L(s, \chi) \\ &= \lim_{s \to 1}(s-1)f^{-s} \sum_{b \pmod f} \chi(b)\zeta(s, b/f) \\ &= \sum_{b \pmod f} \lim_{s \to 1} \chi(b) f^{-s}(s-1)\zeta(s, b/f) \\ &= \sum_{b \pmod f} \chi(b) f^{-1} \\ &= \frac{1}{f} \sum_{b=1}^{f} \chi(b). \end{aligned}$$

Lo cual implica cada uno de los enunciados del teorema.

□

Corolario 3.9. *Para χ carácter de Dirichlet de conductor f, se cumple que*

$$L(1-n, \chi) = -\frac{B_{n,\chi}}{n}, \quad \forall\ n \geq 1.$$

Demostración. Para $n \geq 1$, haciendo $s = 1 - n$ obtenemos

$$\begin{aligned} L(1-n, \chi) &= f^{n-1} \sum_{b=1}^{f} \chi(b)\zeta(1-n, b/f) \\ &= f^{n-1} \sum_{b=1}^{f} -\chi(b)\frac{B_n(b/f)}{n} \\ &= -\frac{f^{n-1}}{n} \sum_{b=1}^{f} \chi(b) B_n(b/f) \\ &= -\frac{B_{n,\chi}}{n}. \end{aligned}$$

Donde hemos aplicado el Teorema 1.15.

□

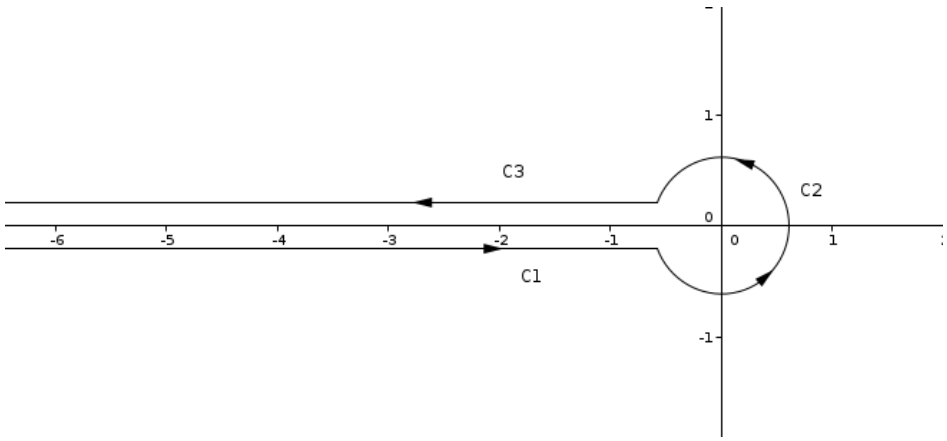


Figura 3.1: Contorno C de Integración

La importancia de la ecuación que aparece en el Corolario 3.9, donde aparecen los valores que toman las funciones L de Dirichlet en los enteros negativos, los cuales involucran a los números generalizados de Bernoulli, radica en el hecho, que son precisamente estos valores los que van a ser interpolados con el objetivo de crear funciones L p-ádicas que coincidan con estos valores en los enteros negativos. Objetivo, que se cumple parcialmente y del cual nos daremos cuenta un poco más adelante.

3.1.2. Fórmula de Hurwitz para $\zeta(s,x)$ y Ecuación funcional para las funciones L

Como ya advertimos anteriormente, la continuación analítica de la función zeta de Hurwitz proporciona la continuación analítica de las funciones L de Dirichlet. Más aún, en el momento de construir funciones L p-ádicas haremos uso de un análogo p-ádico de esta función Zeta de Hurwitz, que además, nos permite determinar ciertos valores especiales de las funciones L de Dirichlet. Y son precisamente estos valores, que ahora caracterizamos de un modo más detallado, haciendo uso de la ecuación funcional de las funciones L, y del hecho de no nulidad de estas cuando $\mathrm{Re}(s) > 1$.

Para extender $\zeta(s,x)$ más allá de la línea $\sigma = 1$ de manera clásica, se deriva una representación de esta función en términos de una integral de contorno. El contorno C (Figura. 3.1) es un lazo al rededor del eje negativo real, el cual esta compuesto de tres partes C_1, C_2, y C_3. C_2 es un círculo orientado positivamente de radio $0 < c < 2\pi$ al rededor del origen, y C_1, C_3 son los caminos inferior y superior de una "cortadura" en el plano complejo a lo largo del eje negativo real. Esto significa que usaremos la parametrización $z = re^{-\pi i}$ en C_1 y $z = re^{\pi i}$ en C_3 donde r varía de c hasta ∞.

No presentaremos la extensión analítica utilizando el método de la integral de contorno, pero si utilizaremos algunos teoremas que involucran esta continuación para deducir la fórmula de Hurwitz de la función $\zeta(s,x)$, que nos proporcionará la ecuación funcional de la funciones L de Dirichlet que buscamos.

Teorema 3.10. *Si $0 < a \leq 1$, la función definida por la integral de contorno:*

$$\mathfrak{I}(s,a) = \frac{1}{2\pi i}\int_C \frac{z^{s-1}e^{az}}{1-e^z}dz, \tag{3.5}$$

es una función entera de s.

Demostración. Aquí z^s es igual a $r^s e^{-\pi i s}$ en C_1 e igual a $r^s e^{\pi i s}$ en C_3. Consideramos un disco compacto arbitrario $|s| \leq M$, y probaremos que las integrales a lo largo de C_1 y C_3 converge uniformemente en cada uno de tales discos. Dado que el integrando es una función entera de s, esto probará que $\mathfrak{I}(s,a)$ es entera.

A lo largo de C_1 tenemos, para $r \geq 1$:

$$|z^{s-1}| = r^{\sigma-1}|e^{-\pi i(\sigma-1+it)}| = r^{\sigma-1}e^{\pi t} \leq r^{M-1}e^{\pi M},$$

ya que $|s| \leq M$. Similarmente, a lo largo de C_3 tenemos que para $r \geq 1$:

$$|z^{s-1}| = r^{\sigma-1}|e^{\pi i(\sigma-1+it)}| = r^{\sigma-1}e^{-\pi t} \leq r^{M-1}e^{\pi M}.$$

Por tal motivo, en C_1 o C_3, tenemos para $r \geq 1$:

$$\left|\frac{z^{s-1}e^{az}}{1-e^z}\right| \leq \frac{r^{M-1}e^{\pi M}e^{-ar}}{1-e^{-r}} = \frac{r^{M-1}e^{\pi M}e^{(1-a)r}}{e^r-1},$$

ahora, como $e^r - 1 > e^r/2$ cuando $r > \log 2$, en efecto:

$$e^r > e^{\log 2} = 2 \implies \frac{e^r}{2} > 1, \text{ i.e., } -\frac{e^r}{2} < -1 \quad \therefore \frac{e^r}{2} < e^r - 1,$$

luego el integrando esta acotado por $Ar^{M-1}e^{-ar}$ donde A es una constante dependiendo de M pero no de r, en efecto:

$$\frac{r^{M-1}e^{\pi M}e^{(1-a)r}}{e^r-1} < \frac{r^{M-1}e^{\pi M}e^r e^{-ar}}{e^r/2} = 2e^{\pi M}r^{M-1}e^{-ar}, \text{ tomando } A = 2e^{\pi M}.$$

Dado que

$$\int_c^\infty r^{M-1}e^{-ar}dr < +\infty, \quad \text{siempre que } c > 0,$$

esto muestra que las integrales a lo largo de C_1 y C_2 convergen uniformemente en cada disco compacto $|s| \leq M$, de manera que $\mathfrak{I}(s,a)$ es una función entera de s.

□

Observación 3.11. *La continuación analítica de la función zeta de Hurwitz utilizando integral de contorno, depende de la ecuación (ver [1], Teorema 12.3, p. 253)*

$$\zeta(s,a) = \Gamma(1-s)\mathfrak{I}(s,a) \quad si\ \sigma > 1 \quad y \quad 0 < a \leq 1. \tag{3.6}$$

Luego, como $\mathfrak{I}(s,a)$ es entera, la ecuación (3.6) define la continuación analítica de $\zeta(s,a)$ para $\sigma \leq 1$, (ver [1], Teorema 12.4, p. 255) haciendo uso de una ecuación integral.

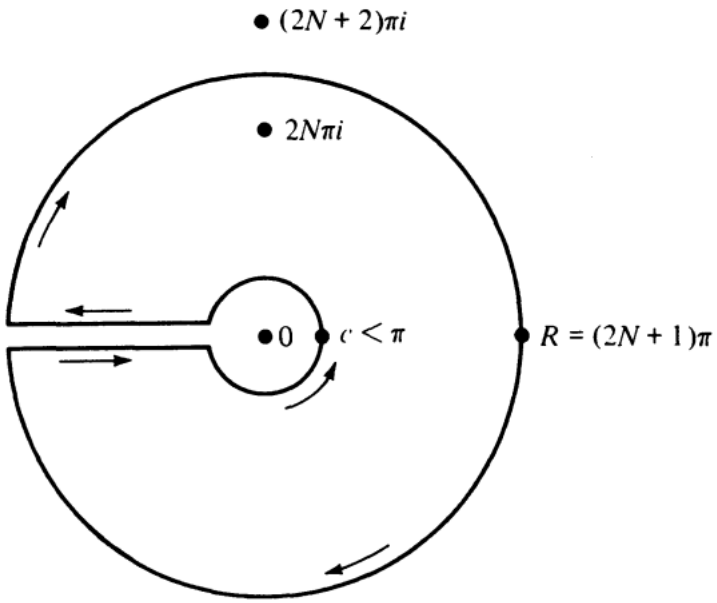


Figura 3.2: Contorno de Integración $C(N)$

Lema 3.12. *Sea $S(r)$ la región que queda cuando removemos del plano complejo todos los discos abiertos de radio r, $0 < r < \pi$, con centros en $z = 2n\pi i$, $n = 0, \pm 1, \pm 2, \cdots$. Entonces si $0 < a \leq 1$ la función*

$$g(z) = \frac{e^{az}}{1 - e^z}$$

es acotada en $S(r)$. (La cota depende de r).

Demostración. ver [1], Lema 1. p. 256.

□

Definición 3.13. *Sea $x \in \mathbb{R}$ y $s = \sigma + it$, con $\sigma > 1$, definimos la **función zeta periódica**, como sigue:*

$$F(x, s) = \sum_{n=1}^{\infty} \frac{e^{2\pi i n x}}{n^s}.$$

Esta función es periódica de periodo 1 con respecto a x, y además $F(1, s) = \zeta(s)$. También la función zeta periódica converge absolutamente para $\sigma > 1$. Si x no es entero, la serie converge (condicionalmente) para $\sigma > 0$ ya que para cada x fijo no entero los coeficientes poseen sumas parciales acotadas (ver [1], p. 257).

Teorema 3.14. ***Fórmula de Hurwitz**. Si $0 < a \leq 1$ y $\sigma > 1$ tenemos*

$$\zeta(1 - s, a) = \frac{\Gamma(s)}{(2\pi)^s} \left[e^{-\pi i s/2} F(a, s) + e^{\pi i s/2} F(-a, s) \right].$$

si $a \neq 1$ esta representación es válida también para $\sigma > 0$.

Demostración. Consideremos la función

$$\mathfrak{I}_N(s,a) = \frac{1}{2\pi i}\int_{C(N)} \frac{z^{s-1}e^{az}}{1-e^z}dz,$$

donde $C(N)$ es el contorno de la Figura 3.2, $N \in \mathbb{Z}$.

Primero probaremos que

$$\lim_{N\to\infty} \mathfrak{I}_N(s,a) = \mathfrak{I}(s,a), \quad \text{si } \sigma > 0,$$

donde $\mathfrak{I}(s,a)$ es la función entera del Teorema 3.10. De manera que, mostraremos que la integral a lo largo del círculo exterior tiende a cero cuando $N \to \infty$.

En el círculo exterior tenemos $z = Re^{i\theta}$, $-\pi \le \theta \le \pi$, con $R = (2N+1)\pi$, por lo tanto

$$|z^{s-1}| = |R^{s-1}e^{i\theta(s-1)}| = R^{\sigma-1}e^{-t\theta} \le R^{\sigma-1}e^{\pi|t|}.$$

Como el círculo exterior está dentro del conjunto $S(r)$ del Lema 3.12, el integrando está acotado por $Ae^{\pi|t|}R^{\sigma-1}$, donde A es la cota para $|g(z)|$ del Lema 3.12, luego

$$\left|\int_{C(N)} z^{s-1}g(z)dz\right| \le \int_{C(N)} |z^{s-1}||g(z)|dz \le AR^{\sigma-1}e^{\pi|t|}\int_{-\pi}^{\pi} d\theta = 2\pi Ae^{\pi|t|}R^{\sigma},$$

y este último tiende a cero cuando $R \to \infty$ si $\sigma < 0$. Por consiguiente, reemplazando s por $1-s$ vemos que

$$\lim_{N\to\infty} \mathfrak{I}_N(1-s,a) = \mathfrak{I}(1-s,a), \quad \text{si } \sigma > 1. \tag{3.7}$$

Ahora calculamos $\mathfrak{I}_N(1-s,a)$ explícitamente por el Teorema del Residuo de Cauchy

$$\mathfrak{I}_N(1-s,a) = -\sum_{\substack{n=-N\\ n\neq 0}}^{N} R(n) = \sum_{n=1}^{N}[R(n)+R(-n)],$$

donde

$$R(n) = \mathrm{Res}_{z=2\pi ni}\left(\frac{z^{-s}e^{az}}{1-e^z}\right).$$

Ahora bien,

$$R(n) = \lim_{z\to 2n\pi i}(z-2n\pi i)\frac{z^{-s}e^{az}}{1-e^z} = \frac{e^{2n\pi ia}}{(2n\pi i)^s}\lim_{z\to 2n\pi i}\frac{z-2n\pi i}{1-e^z} = -\frac{e^{2n\pi ia}}{(2n\pi i)^s}.$$

De manera que

$$\mathfrak{I}_N(1-s,a) = \sum_{n=1}^{N}\frac{e^{2\pi nia}}{(2n\pi i)^s} + \sum_{n=1}^{N}\frac{e^{-2\pi nia}}{(-2n\pi i)^s},$$

y como $i^{-s} = e^{-\pi is/2}$ e $(-i)^{-s} = e^{\pi is/2}$, luego:

$$\mathfrak{I}_N(1-s,a) = \frac{e^{-\pi is/2}}{(2\pi)^s}\sum_{n=1}^{N}\frac{e^{2n\pi ia}}{n^s} + \frac{e^{\pi is/2}}{(2\pi)^s}\sum_{n=1}^{N}\frac{e^{-2n\pi ia}}{n^s}.$$

Tomando $N \to \infty$ y usando (3.7) obtenemos:

$$\mathfrak{I}(1-s,a) = \frac{e^{-\pi is/2}}{(2\pi)^s} F(a,s) + \frac{e^{\pi is/2}}{(2\pi)^s} F(-a,s).$$

Por lo tanto

$$\zeta(1-s,a) = \Gamma(s)\mathfrak{I}(1-s,a) = \frac{\Gamma(s)}{(2\pi)^s}\left[e^{-\pi is/2}F(a,s) + e^{\pi is/2}F(-a,s)\right].$$

□

A partir de la fórmula de Hurwitz podemos deducir una ecuación funcional para la función zeta de Hurwitz.

Teorema 3.15. *Si h y k son enteros, con $1 \le h \le k$, entonces para todo s tenemos*

$$\zeta(1-s,h/k) = \frac{2\Gamma(s)}{(2\pi k)^s} \sum_{r=1}^{k} \cos\left(\frac{\pi s}{2} - \frac{2\pi rh}{k}\right) \zeta(s,r/k) \tag{3.8}$$

Demostración. Análogamente a lo hecho en la Observación 3.4, la función $F(x,s)$ se puede expresar como una combinación lineal de funciones zeta de Hurwitz cuando $x \in \mathbb{Q}$. De hecho, si $x = h/k$, podemos reordenar los términos de la función zeta periódica en la Definición 3.13 con respecto a sus clases módulo k, escribiendo:

$$n = qk + r, \quad \text{donde} \quad 1 \le r \le k \quad \text{y} \quad q = 0,1,2,\cdots.$$

Como resultado, para $\sigma > 1$:

$$\begin{aligned} F\left(\frac{h}{k},s\right) &= \sum_{n=1}^{\infty} \frac{e^{2\pi inh/k}}{n^s} \\ &= \sum_{r=1}^{k}\sum_{q=0}^{\infty} \frac{e^{2\pi irh/k}}{(qk+r)^s} \\ &= \frac{1}{k^s}\sum_{r=1}^{k} e^{2\pi irh/k} \sum_{q=0}^{\infty} \frac{1}{(q+r/k)^s} \\ &= k^{-s}\sum_{r=1}^{k} e^{2\pi irh/k}\zeta(s,r/k). \end{aligned}$$

De manera que, tomando $a = r/k$ en la fórmula de Hurwitz (ver Teorema 3.14) obtenemos:

$$\begin{aligned} \zeta\left(1-s,\frac{h}{k}\right) &= \frac{\Gamma(s)}{(2\pi)^s}\left[e^{-\pi is/2}F(h/k,s) + e^{\pi is/2}F(-h/k,s)\right] \\ &= \frac{\Gamma(s)}{(2\pi)^s}\left[e^{-\pi is/2}k^{-s}\sum_{r=1}^{k} e^{2\pi irh/k}\zeta(s,r/k) + e^{\pi is/2}k^{-s}\sum_{r=1}^{k} e^{-2\pi irh/h}\zeta(s,r/k)\right] \\ &= \frac{\Gamma(s)}{(2\pi k)^s}\sum_{r=1}^{k}\left(e^{-\pi is/2}e^{2\pi irh/k} + e^{\pi is/2}e^{-2\pi irh/k}\right)\zeta(s,r/k) \\ &= \frac{\Gamma(s)}{(2\pi k)^s}\sum_{r=1}^{k}\left(e^{-\left(\frac{\pi s}{2}-\frac{2\pi r.h}{k}\right)i} + e^{\left(\frac{\pi s}{2}-\frac{2\pi rh}{k}\right)i}\right)\zeta(s,r/k) \\ &= \frac{2\Gamma(s)}{(2\pi k)^s}\sum_{r=1}^{k}\cos\left(\frac{\pi s}{2} - \frac{2\pi rh}{k}\right)\zeta(s,r/k). \end{aligned}$$

Lo cual prueba (3.8) para $\sigma > 1$. La conclusión del teorema se tiene para todo s por continuación analítica.

□

Observación 3.16. *Notemos que si hacemos $h = k = 1$, solo hay un término en (3.8) y obtenemos ecuación funcional para la función zeta de Riemann del Lema 1.7, a saber:*

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

La principal razón histórica del estudio de las funciones L, es la extracción de información aritmética que estas poseen con respecto a los números primos, debido a la conocida representación de las funciones L de Dirichlet como productos de Euler:

Teorema 3.17. *Sea χ carácter de Dirichlet, para $\sigma > 1$, tenemos*

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1-\chi(p)p^{-s}} \tag{3.9}$$

Demostración. Esta es la generalización del mismo resultado para la función zeta de Riemann, mostrado en la Proposición A.3. Procediendo análogamente se obtiene para las funciones L de Dirichlet (ver [1], Teorema 11.6, p. 230). □

El Teorema 3.17 asegura entre otras cosas que $L(s,\chi) \neq 0$ para $\mathrm{Re}(s) > 1$. También lo utilizamos, para saber que en la deducción de una ecuación funcional de las funciones L de Dirichlet, es suficiente considerar solo los caracteres primitivos módulo el conductor del carácter.

Teorema 3.18. *Sea χ carácter de Dirichlet módulo k, sea d cualquier módulo inductor, y escribimos: (ver Apéndice B, Teorema B.22)*

$$\chi(n) = \psi(n)\chi_1(n),$$

donde ψ es un carácter módulo d y χ_1 es el carácter principal módulo k. Entonces para todo s tenemos

$$L(s,\chi) = L(s,\psi) \prod_{p|k} \left(1 - \frac{\psi(p)}{p^s}\right).$$

Demostración. Pimero tomemos $\sigma > 1$ y usemos el producto de Euler (ver Teorema 3.17)

$$L(s,\chi) = \prod_p \left(\frac{1}{1-\chi(p)p^{-s}}\right).$$

Dado que $\chi(p) = \psi(p)\chi_1(p)$, y como $\chi_1(p) = 0$ si $p|k$ y $\chi_1(p) = 1$ si $p \nmid k$, encontramos que:

$$\begin{aligned} L(s,\chi) &= \prod_{p\nmid k}\left(\frac{1}{1-\psi(p)p^{-s}}\right) \\ &= \prod_{p}\left(\frac{1}{1-\psi(p)p^{-s}}\right)\cdot\prod_{p|k}\left(1-\psi(p)p^{-s}\right) \\ &= L(s,\psi)\prod_{p|k}\left(1-\frac{\psi(p)}{p^s}\right). \end{aligned}$$

Esto prueba el teorema para $\sigma > 1$ y lo extendemos a todo s por continuación analítica. □

Observación 3.19. *Si tomamos d en el teorema anterior como el conductor de χ, entonces ψ es un carácter primitivo módulo d. Esto muestra que cada serie L, $L(s,\chi)$, es igual a una serie L, $L(s,\psi)$, de un carácter primitivo, multiplicado por un número finito de factores.*

Definición 3.20. *Definimos la suma de Gauss como:*

$$\tau(\chi) = \sum_{b=1}^{f}\chi(b)e^{2\pi ib/f}.$$

Teorema 3.21. *Sea χ carácter primitivo módulo $f > 1$. Entonces para $\sigma > 1$, tenemos:*

$$\tau(\overline{\chi})L(s,\chi) = \sum_{a=1}^{f}\overline{\chi}(a)F(a/f,s). \tag{3.10}$$

Demostración. Tomando $x = a/f$ en la función zeta periódica (ver Definición 3.13), luego multiplicando por $\overline{\chi}(a)$ y sumando en a obtenemos:

$$\begin{aligned} \sum_{a=1}^{f}\overline{\chi}(a)F\left(\frac{a}{f},s\right) &= \sum_{a=1}^{f}\sum_{n=1}^{\infty}\overline{\chi}(a)\frac{e^{2\pi ina/f}}{n^s} \\ &= \sum_{n=1}^{\infty}\frac{1}{n^s}\sum_{a=1}^{f}\overline{\chi}(a)e^{2\pi ina/f}. \end{aligned}$$

Por otro lado, si m.c.d$(n,f) > 1$ concluimos que: (ver [1],Teorema 8.15(a), p.168)

$$\sum_{a=1}^{f}\overline{\chi}(a)e^{2\pi ina/f} = 0.$$

Por esta razón, basta considerar los casos donde m.c.d$(n,f) = 1$, luego:

$$\sum_{a=1}^{f}\overline{\chi}(a)e^{2\pi ina/f} = \chi(n)\tau(\overline{\chi}),$$

en efecto, como n y f son primos relativos, los números na recorren un sistema completo de residuos módulo f con $1 \leq a \leq f$. También $|\chi(n)|^2 = \chi(n)\overline{\chi}(n) = 1$, luego:

$$\overline{\chi}(a) = \chi(n)\overline{\chi}(n)\overline{\chi}(a) = \chi(n)\overline{\chi}(na).$$

De manera que:

$$\begin{aligned}\sum_{a=1}^{f} \overline{\chi}(a)e^{2\pi ina/f} &= \chi(n) \sum_{a \pmod f} \overline{\chi}(na)e^{2\pi ina/f} \\ &= \chi(n) \sum_{m \pmod f} \overline{\chi}(m)e^{2\pi im/f} \\ &= \chi(n)\tau(\overline{\chi}).\end{aligned}$$

De lo anterior, tenemos que:

$$\sum_{a=1}^{f} \overline{\chi}(a)F\left(\frac{a}{f}, s\right) = \tau(\overline{\chi}) \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \tau(\overline{\chi})L(s, \chi).$$

□

A continuación pasamos a deducir la ecuación funcional para las funciones L de Dirichlet a partir de la fórmula de Hurwitz.

Teorema 3.22. *Sea χ un carácter de Dirichlet módulo f entonces para todo s tenemos la siguiente ecuación funcional para las funciones L de Dirichlet*

$$L(1-s, \chi) = \frac{f^{s-1}\Gamma(s)}{(2\pi)^s}\left[e^{-\pi is/2} + \chi(-1)e^{\pi is/2}\right]\tau(\chi)L(s, \overline{\chi}) \tag{3.11}$$

Demostración. Tomamos $a = k/f$ en la fórmula de Hurwitz (ver Teorema 3.14), luego multiplicando por $\chi(k)$ y sumando en k, tenemos:

$$\sum_{k=1}^{f} \chi(k)\zeta\left(1-s, \frac{k}{f}\right) = \frac{\Gamma(s)}{(2\pi)^s}\left[e^{-\pi is/2}\sum_{k=1}^{f}\chi(k)F\left(\frac{k}{f}, s\right) + e^{\pi is/2}\sum_{k=1}^{f}\chi(k)F\left(-\frac{k}{f}, s\right)\right].$$

Dado que $F(x, s)$ es periódica en x con periodo 1 y $\chi(k) = \chi(-1)\chi(-k)$, podemos escribir

$$\begin{aligned}\sum_{k=1}^{f} \chi(k)F\left(-\frac{k}{f}, s\right) &= \chi(-1)\sum_{k=1}^{f}\chi(-k)F\left(-\frac{k}{f}, s\right) \\ &= \chi(-1)\sum_{k=1}^{f}\chi(f-k)F\left(\frac{f-k}{f}, s\right) \\ &= \chi(-1)\sum_{k=1}^{f}\chi(k)F\left(\frac{k}{f}, s\right).\end{aligned}$$

De manera que, al reemplazar en la ecuación anterior, tenemos:

$$\sum_{k=1}^{f} \chi(k)\zeta\left(1-s, \frac{k}{f}\right) = \frac{\Gamma(s)}{(2\pi)^s}\left[e^{-\pi is/2} + \chi(-1)e^{\pi is/2}\right]\sum_{k=1}^{f}\chi(k)F\left(\frac{k}{f}, s\right),$$

al multiplicar ambos lados de la igualdad por f^{s-1} de la Observación 3.4 y usando (3.10), obtenemos el teorema.

□

Corolario 3.23. *Si $\chi(-1) = 1$, i.e., χ es carácter par, entonces:*

$$L(1-s,\chi) = \frac{2}{f}\left(\frac{f}{2\pi}\right)^{s} \tau(\chi)\cos\left(\frac{\pi s}{2}\right)\Gamma(s)L(s,\overline{\chi}). \tag{3.12}$$

Si $\chi(-1) = -1$, i.e., χ es carácter impar, entonces:

$$L(1-s,\chi) = -\frac{2i}{f}\left(\frac{f}{2\pi}\right)^{s} \tau(\chi)\sin\left(\frac{\pi s}{2}\right)\Gamma(s)L(s,\overline{\chi}). \tag{3.13}$$

Demostración. Ambas ecuaciones provienen de reemplazar en la ecuación funcional (3.11) por:

$$\cos\left(\frac{\pi s}{2}\right) = \frac{e^{i\pi s}+e^{-i\pi s}}{2} \quad \text{ó} \quad \sin\left(\frac{\pi s}{2}\right) = \frac{e^{i\pi s/2}-e^{-i\pi s/2}}{2i},$$

según sea el caso.

□

Observación 3.24. *Tomemos χ carácter primitivo, luego del Corolario 3.9, sabemos que:*

$$L(1-n,\chi) = -\frac{B_{n,\chi}}{n}, \quad \forall\ n \geq 1.$$

Por otra parte, del Teorema 1.20, se sabe que:

$$(-1)^n B_{n,\chi} = \chi(-1)B_{n,\chi}.$$

De manera que

$$L(1-n,\chi) = (-1)^n\chi(-1)L(1-n,\chi),$$

Por lo tanto, si χ y n poseen paridades opuestas, entonces $L(1-n,\chi) = 0$. Si χ y n poseen la misma paridad, del Corolario 3.23, tenemos para $n \in \mathbb{Z}_+$, que

$$|\tau(\chi)| \cdot |L(n,\overline{\chi})| = \frac{f}{2}\left(\frac{2\pi}{f}\right)^{n}\left|\frac{B_{n,\chi}}{n!}\right|,$$

y como $\tau(\chi) \neq 0$ (ver [1], Teorema 8.15 (c), p. 168) y $L(n,\overline{\chi}) \neq 0$ para $n \geq 1$ por su representación como producto de Euler (ver Teorema 3.17), se sigue que $B_{n,\chi} \neq 0$ en este caso. Hemos demostrado entonces la siguiente proposición:

Proposición 3.25. *Sea χ carácter de Dirichlet primitivo, de conductor $f > 1$. Entonces si $n \geq 1$:*

$$L(1-n,\chi) \neq 0 \iff \chi(-1) = (-1)^n,$$

esto es, $L(1-n,\chi) \neq 0$ si y solo si χ y n tienen la misma paridad.

3.2. Funciones L p-ádicas y función zeta de Hurwitz p-ádica

De la Observación 3.4, sabemos que las funciones L de Dirichlet pueden ser escritas como una combinación lineal de funciones zeta de Hurwitz, a saber:

$$L(s,\chi) = \sum_{b=1}^{f} \chi(b) H(s,b,f),$$

donde χ es carácter de Dirichlet con conductor $f > 1$ y donde hemos definido la función:

$$H(s,b,f) = f^{-s}\zeta\left(s, \frac{b}{f}\right), \quad 1 \leq b \leq f.$$

La idea es definir un análogo p-ádico a la función zeta de Hurwitz, digamos $H_p(s,b,f)$, con s variable p-ádica tal que esta función como en el caso clásico, nos permita expresar una función $L_p(s,\chi)$ en variable p-ádica como combinación lineal de estas funciones zeta de Hurwitz p-ádicas, es decir, que tenga la forma:

$$L_p(s,\chi) = \sum_{b=1}^{f} \chi(b) H_p(s,b,f).$$

Podemos sugerir a partir de ciertas observaciones, como podriamos formalizar la idea dada anteriormente. Recordemos que del Teorema 1.15, tenemos que:

$$B_{n,\chi} = f^{n-1} \sum_{b=1}^{f} \chi(b) B_n(b/f),$$

donde χ es carácter de Dirichlet con conductor $f > 1$ y $B_n(x)$ es el n-ésimo polinomio de Bernoulli, que por Definición 1.11 son de la forma:

$$B_n(x) = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} B_j,$$

dónde los B_j son números de Bernoulli (ver Capítulo 1), entonces:

$$B_n\left(\frac{b}{f}\right) = \sum_{j=0}^{n} \binom{n}{j} \left(\frac{b}{j}\right)^{n-j} B_j,$$

de tal manera que

$$B_{n,\chi} = f^{n-1} \sum_{b=1}^{f} \chi(b) \sum_{j=0}^{n} \binom{n}{j} \left(\frac{b}{f}\right)^{n-j} B_j,$$

debido a lo cual, del Corolario 3.9, a saber:

$$L(1-n,\chi) = -\frac{B_{n,\chi}}{n}, \quad \forall\ n \geq 1,$$

obtenemos para las funciones L de Dirichlet, la siguiente representación en sus valores enteros negativos

$$L(1-n,\chi) = -\frac{1}{f}\cdot\frac{1}{n}\sum_{b=1}^{f}\chi(b)b^n\sum_{j=0}^{n}\binom{n}{j}\left(\frac{f}{b}\right)^j B_j \tag{3.14}$$

De allí la importancia de la identidad presentada en el Corolario 3.9, la cual radica en el hecho que el lado derecho de (3.14) es esencialmente una combinación lineal de términos de la forma:

$$\sum_{j=0}^{n}\binom{n}{j}(f/b)^j B_j,$$

lo cual tiene sentido cuando n es reemplazada por una variable p-ádica y $p|f$.

3.2.1. La Función zeta de Hurwitz p-ádica

Definición 3.26. *Definimos la función zeta de Hurwitz p-ádica para $p|F$, $F\in\mathbb{Z}_+$ y $m.c.d(b,p)=1$, como sigue:*

$$H_p(s,b,F) = \frac{1}{s-1}\frac{1}{F}\langle b\rangle^{1-s}\sum_{k=0}^{+\infty}\binom{1-s}{k}(F/b)^k B_k, \quad con \quad 0<b\leq F,$$

donde $\langle b\rangle^{1-s}$ esta definido en la Observación 2.40.

Tomando nuevamente la convención

$$q = \begin{cases} p & \text{si} \quad p>2 \\ 4 & \text{si} \quad p=2. \end{cases}$$

El siguiente teorema establece la existencia de la función zeta de Hurwitz p-ádica, además de dar explícitamente su región de convergencia.

Teorema 3.27. *Supongamos que $q|F$, $F\in\mathbb{Z}_+$, y $m.c.d(a,p)=1$. Entonces $H_p(s,a,F)$ es una función meromorfa p-ádica en*

$$\{s\in\mathbb{C}_p:\ |s|_p < qp^{-1/(p-1)}\}$$

tal que

$$H_p(1-n,a,F) = \omega^{-n}(a)H(1-n,a,F), \quad n\geq 1.$$

En particular, cuando $n\equiv 0$ (mód $p-1$), ó (mód 2) si $p=2$, entonces

$$H_p(1-n,a,F) = H(1-n,a,F).$$

La función H_p es analítica, menos en el punto $s=1$ donde posee un polo simple con residuo igual a $1/F$.

Demostración. Asumamos la convergencia de $H_p(s,a,F)$ por el momento, luego:

$$\begin{aligned}
H_p(1-n,a,F) &= -\frac{1}{nF}\langle a\rangle^n \sum_{k=0}^{n}\binom{n}{k}\left(\frac{F}{a}\right)^k B_k \\
&= -\frac{1}{nF}a^n\omega^{-n}(a)\sum_{k=0}^{n}\binom{n}{k}\left(\frac{F}{a}\right)^k B_k \\
&= -\frac{F^{n-1}\omega^{-n}(a)}{n}\left(\frac{a}{F}\right)^n \sum_{k=0}^{n}\binom{n}{k}\left(\frac{F}{a}\right)^k B_k \\
&= -\frac{F^{n-1}\omega^{-n}(a)}{n}\sum_{k=0}^{n}\binom{n}{k}\left(\frac{a}{F}\right)^{n-k} B_k \\
&= -\frac{F^{n-1}\omega^{-n}(a)}{n}B_n\left(\frac{a}{F}\right) \\
&= \omega^{-n}(a)H(1-n,a,F),
\end{aligned}$$

$$\therefore \quad H_p(1-n,a,F) = \omega^{-n}(a)H(1-n,a,F), \quad n \geq 1.$$

La penúltima igualdad se obtiene debido a la Proposición 3.7.

Ahora bien por definición de $H_p(s,a,F)$, en $s=1$ existe un polo, cuyo residuo calculamos a continuación:

$$\begin{aligned}
\lim_{s\to 1}(s-1)H_p(s,a,F) &= \lim_{s\to 1}\frac{1}{F}\langle a\rangle^{1-s}\sum_{k=0}^{\infty}\binom{1-s}{k}\left(\frac{F}{a}\right)^k B_k \\
&= \frac{1}{F}\langle a\rangle^0 \sum_{k=0}^{\infty}\binom{0}{k}\left(\frac{F}{a}\right)^k B_k \\
&= \frac{1}{F}.
\end{aligned}$$

Demostremos ahora la convergencia de $H_p(s,a,F)$. Para hacer esto, aplicamos el Teorema 2.30 a la serie

$$\sum_{k=0}^{+\infty}\binom{s}{k}(F/a)^k B_k. \tag{3.15}$$

Del Teorema de von Staudt-Clausen (ver Teorema 1.26) con $B_k = U_k/V_k$, tenemos para p-primo impar que:

Si $(p-1)|k$ entonces $p|V_k$ de modo que $\nu_p(V_k)=1$ (ya que V_k es libre de cuadrados), entonces

$$\nu_p((F/a)^k B_k) = k\nu_p(F) - k\nu_p(a) + \nu_p(U_k) - \nu_p(V_k) \geq k - \nu_p(V_k) = k-1.$$

Si $(p-1)\nmid k$, entonces $p\nmid V_k$ por lo tanto $\nu_p(V_k)=0$, por tal motivo

$$\nu_p((F/a)^k B_k) = k\nu_p(F) - k\nu_p(a) + \nu_p(U_k) - \nu_p(V_k) \geq k - \nu_p(V_k) = k > k-1.$$

En ambos casos podemos concluir que

$$|(F/a)^k B_k|_p \leq p^{-(k-1)} = p\left(\frac{1}{p}\right)^k.$$

Al tomar $r = 1/p$ y $M = p$ en el Teorema 2.30, tenemos que $R = (p^{-1} \cdot p^{1/(p-1)})^{-1}$. Si $p = 2$ podemos obtener una mejor estimativa, en efecto:

$$\nu_2((F/a)^k B_k) = k\nu_2(F) - k\nu_2(a) + \nu_2(U_k) - \nu_2(V_k) \geq 2k - 1,$$

ya que por hipótesis en este caso $q = 4$ y $q|F$, entonces $\nu_2(F) \geq 2$. Luego

$$|(F/a)^k B_k|_2 \leq 2^{-2k+1} = 2\left(\frac{1}{4}\right)^k.$$

Entonces, al tomar $r = 1/q$ y $M = 2$ en el Teorema 2.30, tenemos que $R = (q^{-1} \cdot p^{1/(p-1)})^{-1} = 2 > 1$. De todo lo anterior, podemos concluir que (3.15) define una función analítica en el conjunto

$$D = \{s \in \mathbb{C}_p : |s|_p < qp^{-1/(p-1)}\}.$$

Por otra parte, dado que $1 \in D$ y como en los discos p-ádicos cualquier punto es centro, tenemos que:

$$D = \{s \in \mathbb{C}_p : |1 - s|_p < qp^{-1/(p-1)}\},$$

esto prueba que

$$\sum_{k=0}^{+\infty} \binom{1-s}{k} (F/a)^k B_k$$

es analítica en D. Por Observación 2.40 la función $\langle a\rangle^s$ es analítica en D, por tanto $\langle a\rangle^{1-s}$ también lo es.

□

3.2.2. Funciones L p-ádicas

Observación 3.28. *Sea χ un carácter de Dirichlet de conductor f y sea ω carácter de Teichmüller de conductor q (ver Definición 2.39). Sea $f_{\chi\omega^{-n}}$ el conductor del producto $\chi\omega^{-n}$ de estos caracteres, tal como se define en el Apéndice B, Sección B.1, entonces $f_{\chi\omega^{-n}}|fq$. Pero dado que $\chi = \chi\omega^{-n} \cdot \omega^n$, tenemos que $f|qf_{\chi\omega^{-n}}$. De manera que $f_{\chi\omega^{-n}}$ y f difieren solo por un factor la potencia del primo p. En efecto,*

$$\begin{aligned} & f_{\chi\omega^{-n}}|fq \ y \ f|qf_{\chi\omega^{-n}} \ \Rightarrow \ fq = k_1 \cdot f_{\chi\omega^{-n}}; \quad k_1 \in \mathbb{Z} \ \ y \ \ qf_{\chi\omega^{-n}} = fk_2; \quad k_2 \in \mathbb{Z} \\ & \Rightarrow \quad (ff_{\chi\omega^{-n}})q^2 = (ff_{\chi\omega^{-n}})k_1k_2 \quad \therefore \ q^2 = k_1k_2 \\ & \Rightarrow \quad k_1 = p^j \quad con \ \ 0 \leq j \leq 3 \quad si \ \ p = 2 \ \ y \ \ 0 \leq j \leq 2 \quad si \ \ p > 2. \end{aligned}$$

Se sigue que si $a \in \mathbb{Z}$, con $m.c.d(a, p) = 1$, entonces

$$m.c.d(a, f_{\chi\omega^{-n}}) = m.c.d(a, f) \quad y \quad \chi\omega^{-n}(a) = \chi(a)\omega^{-n}(a),$$

resta probar la segunda afirmación, como $m.c.d(a,p)=1$, *entonces* $m.c.d(a,q)=1$. *Si* $m.c.d(a,fq)=1$ *por definición del producto de carácteres* $\chi\omega^{-n}(a)=\chi(a)\omega^{-n}(a)$, *si* $d=m.c.d(a,fq)>1$, *luego* $d|a$ *y* $d|fq$, *como* $m.c.d(a,q)=1$, *podemos concluir que* $m.c.d(d,q)=1$, *así por Lema de Euclides* $d|f$, *con lo cual* $m.c.d(a,f)>1$, *de manera que* $m.c.d(a,f_{\chi\omega^{-n}})>1$, *y así concluimos que* $\chi\omega^{-n}(a)=0$ *y* $\chi(a)=0$, *por lo tanto* $\chi\omega^{-n}(a)=\chi(a)\omega^{-n}(a)$.

Ahora finalmente estamos listos para construir las funciones L p-ádicas.

Teorema 3.29. *Sea* χ *carácter de Dirichlet de conductor* f *y sea* F *un múltiplo de* q *y* f, *i.e.,* $F=Kqf$ *con* $K\in\mathbb{Z}$. *Entonces existe una función meromorfa p-ádica (analítica si* $\chi\neq\chi_1$) $L_p(s,\chi)$ *definida en*

$$D=\{s\in\mathbb{C}_p : |s|_p < qp^{-1/(p-1)}\}$$

tal que

$$L_p(1-n,\chi)=-(1-\chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n},\quad n\in\mathbb{Z}_+ \tag{3.16}$$

donde ω *es el carácter de Teichmüller. Si* $\chi=\chi_1$, *entonces* $L_p(s,\chi_1)$ *es analítica en* D *excepto para el polo simple en* $s=1$ *con residuo* $(1-1/p)$. *De hecho, tenemos la fórmula*

$$L_p(s,\chi)=\frac{1}{F}\frac{1}{s-1}\sum_{\substack{a=1\\(a,p)=1}}^{F}\chi(a)\langle a\rangle^{1-s}\sum_{k=0}^{+\infty}\binom{1-s}{k}(F/a)^k B_k. \tag{3.17}$$

Demostración. Definamos $L_p(s,\chi)$ como sigue:

$$L_p(s,\chi)=\sum_{\substack{a=1\\(a,p)=1}}^{F}\chi(a)H_p(s,a,F).$$

$L_p(s,\chi)$ es analítica en D por el Teorema 3.27, excepto en $s=1$. Calculemos el residuo de la función $L_p(s,\chi)$ en $s=1$

$$\begin{aligned}\lim_{s\to1}(s-1)L_p(s,\chi)&=\sum_{\substack{a=1\\(a,p)=1}}^{F}\chi(a)\lim_{s\to1}(s-1)H_p(s,a,F)\\&=\frac{1}{F}\sum_{\substack{a=1\\(a,p)=1}}^{F}\chi(a).\end{aligned}$$

$$\therefore\quad \mathrm{Res}_{s=1}L_p(s,\chi)=\frac{1}{F}\sum_{\substack{a=1\\(a,p)=1}}^{F}\chi(a).$$

Si $\chi=\chi_1$ es el carácter principal, la suma es igual a $(1-1/p)$, en efecto:

$$\frac{1}{F}\sum_{\substack{a=1\\(a,p)=1}}^{F}\chi_1(a)=\frac{1}{F}\sum_{\substack{a=1\\(a,p)=1}}^{F}1=\frac{1}{F}\left(F-\left[\frac{F}{p}\right]\right)=1-\frac{1}{F}\left[\frac{F}{p}\right],$$

notemos que:

$$\left[\frac{F}{p}\right] = \left[\frac{Kqf}{p}\right] = \begin{cases} Kf & \text{si} \quad q = p, \\ 2Kf & \text{si} \quad q = 4. \end{cases}$$

De manera que

$$\frac{1}{F}\sum_{\substack{a=1\\(a,p)=1}}^{F} \chi_1(a) = 1 - \frac{1}{p}, \quad \forall\ p\text{-primo},$$

como se quería demostrar.

Si $\chi \neq \chi_1$, la suma puede ser reescrita como

$$\frac{1}{F}\sum_{\substack{a=1\\(a,p)=1}}^{F} \chi(a) = \frac{1}{F}\sum_{a=1}^{F}\chi(a) - \frac{1}{F}\sum_{b=1}^{F/p}\chi(pb)$$

la primera suma es cero por Observación 1.19. Por otro lado, si $p|f$ entonces $\chi(pb) = 0$ para todo b y la segunda suma es 0. Si m.c.d$(p, f) = 1$, como $f|(F/p)$ ya que $F = Kqf$, la segunda suma nuevamente es 0. Más aún,

$$\begin{aligned} L_p(1-n,\chi) &= \sum_{\substack{a=1\\(a,p)=1}}^{F} \chi(a) H_p(1-n,a,F) \\ &= \sum_{\substack{a=1\\(a,p)=1}}^{F} \chi(a)\left[-\frac{1}{n}\frac{1}{F}\langle a\rangle^n \sum_{k=0}^{+\infty}\binom{n}{k}(F/a)^k B_k\right] \\ &= -\frac{1}{nF}\sum_{\substack{a=1\\(a,p)=1}}^{F} \chi(a)\langle a\rangle^n \sum_{k=0}^{n}\binom{n}{k}(F/a)^k B_k. \end{aligned}$$

La suma interior puede ser reescrita como

$$\begin{aligned} \sum_{k=0}^{n}\binom{n}{k}(F/a)^k B_k &= \sum_{k=0}^{n}\binom{n}{k}(F/a)^{n-k} B_{n-k} \\ &= (F/a)^n \sum_{k=0}^{n}\binom{n}{k}(a/F)^k B_{n-k}. \end{aligned}$$

Dado que estamos sumando sobre los a primos relativos a p, por la Observación 3.28, al usar el carácter de Teichmüller, podemos reescribir a la función $L_p(1-n,\chi)$ como:

$$\begin{aligned} L_p(1-n,\chi) &= -\frac{F^{n-1}}{n}\sum_{\substack{a=1\\(a,p)=1}}^{F} \chi\omega^{-n}(a) B_n(a/F) \\ &= -\frac{F^{n-1}}{n}\sum_{a=1}^{F}\chi\omega^{-n}(a)B_n(a/F) + \frac{F^{n-1}}{n}\sum_{b=1}^{F/p}\chi\omega^{-1}(pb)B_n(b/(F/p)). \end{aligned}$$

Si $p|f_{\chi\omega^{-n}}$ el conductor del carácter $\chi\omega^{-n}$ entonces $\chi\omega^{-n}(pb) = 0$ para todo b. Por otro lado, si $p \nmid f_{\chi\omega^{-n}}$, tenemos que $f_{\chi\omega^{-n}}|(F/p)$, en efecto, dado que $F = Kqf$, entonces

$f_{\chi\omega^{-n}}|F = Kqf$ y como m.c.d$(p, f_{\chi\omega^{-n}}) = 1$, entonces m.c.d$(q, f_{\chi\omega^{-n}}) = 1$, por Lema de Euclides $f_{\chi\omega^{-n}}|Kf$, y como $Kf|(F/p)$, se concluye la afirmación.

Ahora bien, por Teorema 1.15, tenemos que:

$$-\frac{F^{n-1}}{n}\sum_{a=1}^{F}\chi\omega^{-n}(a)B_n(a/F) = -\frac{B_{n,\chi\omega^{-n}}}{n}$$

y para el segundo término, tenemos que:

$$\begin{aligned}\frac{F^{n-1}}{n}\sum_{b=1}^{F/p}\chi\omega^{-1}(pb)B_n(b/(F/p)) &= \frac{\chi\omega^{-n}(p)}{n}F^{n-1}\sum_{b=1}^{F/p}\chi\omega^{-n}(b)B_n(b/(F/p)) \\ &= \frac{\chi\omega^{-n}(p)p^{n-1}}{n}\left(\frac{F}{p}\right)^{n-1}\sum_{b=1}^{F/p}\chi\omega^{-n}(b)B_n(b/(F/p)) \\ &= \chi\omega^{-n}(p)p^{n-1}\frac{B_{n,\chi\omega^{-n}}}{n}\end{aligned}$$

De donde concluimos

$$L_p(1-n,\chi) = -(1-\chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n}.$$

Lo cual completa la demostración del Teorema.

□

Observación 3.30.

- *El factor $(1-\chi\omega^{-n}(p)p^{n-1})$ es el inverso del factor de Euler en p para $L(s,\chi\omega^{-n})$ (ver Teorema 3.17). Es un principio general que para obtener un análogo p-ádico de una función de variable compleja, la p-parte debe ser removida, ya que intuitivamente por ejemplo, $\sum 1/n^s$ posee términos arbitrariamente grandes en forma p-ádica si consideramos los términos n divisibles entre p; por otra parte, los términos n que no son divisibles entre p, al menos están acotados en forma p-ádica.*

- *En general, $\chi\omega^{-n}(p) \neq \chi(p)\omega^{-n}(p)$. Por ejemplo, si $\chi = \omega^n \neq \chi_1$, entonces $\chi\omega^{-n}(p) = 1$, mientras que $\chi(p) = \omega^n(p) = 0$.*

- *$L_p(s,\chi)$ interpola los números*

$$(1-\chi\omega^{-n}(p)p^{n-1})L(1-n,\chi\omega^{-n}).$$

- *Notemos que la ecuación que define una función L p-ádica $L_p(s,\chi)$ (3.17) es esencialamente un intento de emular la ecuación (3.14) para $L(1-n,\chi)$.*

- *Si χ es un carácter impar, entonces n y $\chi\omega^{-n}$ tienen paridad opuesta y $L_p(s,\chi)$ es identicamente cero.*

  Esto se debe en principio a que ω es carácter impar, en efecto, si $p = 2$, entonces $\omega(a) \in V = \{\pm 1\}$, si $\omega(-1) = 1$, entonces $\omega(3) = 1$ y ω sería carácter principal, y tal cosa no puede ocurrir ya que $q > 1$ es su conductor, (ver Teorema B.16).

Si $p > 2$ y $\omega(-1) = 1$ entonces $\omega(-1) \equiv -1$ (mód p), i.e., $1 \equiv -1$ (mód p), lo que es contradictorio. De lo anterior:

$$\chi\omega^{-n}(-1) = \chi(-1)\omega^{-n}(-1) = (-1)(-1)^n = (-1)^{n+1},$$

lo cual implica que n y $\chi\omega^{-n}$ poseen paridad opuesta, de manera que por Proposición 3.25, y del hecho que:

$$L_p(1-n, \chi\omega^{-n}) = (1 - \chi\omega^{-n}(p)p^{n-1})L(1-n, \chi\omega^{-n}) = 0,$$

y al ser $\mathbb{Z}$ denso en $\mathbb{Z}_p$, entonces $L_p(s, \chi) = 0$ para todo $s \in \mathbb{Z}_p \subset D$, luego $L_p(s, \chi) = 0$ en D.

Si χ es carácter par, entonces n y $\chi\omega^{-n}$ poseen la misma paridad, luego $B_{n,\chi\omega^{-n}} \neq 0$. En efecto:

$$\chi\omega^{-n}(-1) = \chi(-1)\omega^{-n}(-1) = (-1)^n,$$

lo que implica que n y $\chi\omega^{-n}$ poseen la misma paridad. De manera que, $L_p(s, \chi)$ no es la función cero en este caso.

3.2.3. Congruencias de Kummer II

En esta sección se dará otra demostración de las congruencias de Kummer, la cual es consecuencia de una representación en serie de potencias de las funciones L p-ádicas, y que por tanto, se aleja del enfoque original empleado por Kummer.

Teorema 3.31. *Sea χ carácter de Dirichlet de conductor f_χ, supongamos $\chi \neq \chi_1$ y $pq \nmid f_\chi$. Entonces*

$$L_p(s, \chi) = a_0 + a_1(s-1) + a_2(s-1)^2 + \cdots,$$

con $|a_0|_p \leq 1$ y $\nu_p(a_j) \geq 1$ para $j \geq 1$.

Observación 3.32. *Notemos que, como $L_p(s, \chi)$ posee radio de convergencia mayor que 1, $a_j \to 0$ cuando $j \to \infty$; luego a priori tenemos que $\nu_p(a_j) \geq 1$ para j suficientemente grande.*

Demostración. Tomamos F como en el Teorema 3.29 tal que $q|F$ pero $pq \nmid F$. Asumimos además que χ es carácter par, ya que de lo contrario $L_p(s, \chi) = 0$ (ver Observación 3.30). Notemos que:

- Si $q \neq 4$ tenemos que $q = p$, en consecuencia $\nu_p(F) \geq 1$, así $|F|_p \leq 1/p$, de donde concluimos que $|F^{j-1}|_p \leq 1/p^{j-1}$.
- Si $q = 4$ tenemos que $p = 2$, en consecuencia $\nu_p(F) \geq 2$, luego $|F|_2 \leq 1/4$, de manera que $|F^{j-1}|_2 \leq 1/4^{j-1}$.

En cualquier caso, deducimos que:

$$|F^{j-1}|_p \leq \frac{1}{q^{j-1}}, \quad j > 1.$$

- Sea $a \in \mathbb{Z}_+$, con m.c.d$(a,p) = 1$, i.e., $p \nmid a$, de lo cual $\nu_p(a) = 0$, esto es, $|a|_p = 1$.
- Sea $B_j = U_j/V_j$, j-ésimo número de Bernoulli, entonces

$$\nu_p(B_j) = \nu_p(U_j) - \nu_p(V_j) \geq -\nu_p(V_j)$$

por ello $|B_j|_p \leq p^{\nu_p(V_j)}$, pero como $\nu_p(V_j) \leq 1$, tenemos que $p^{\nu_p(V_j)} \leq p$, de manera que $|B_j|_p \leq p$.

- Por último, como $\nu_p(j!) \leq j/(p-1)$ (ver Lema C.9 (i)), entonces $|j!|_p = p^{-\nu_p(j!)} \geq p^{-j/(p-1)}$, por lo tanto

$$\frac{1}{|j!|_p} \leq p^{j/(p-1)}, \quad j \geq 1.$$

De todo lo anterior, tenemos que:

$$\left|\frac{B_j}{j!} \cdot \frac{F^{j-1}}{a^j}\right|_p = \frac{|B_j|_p}{|j!|_p} \cdot \frac{|F^{j-1}|_p}{|a^j|_p} \leq p \cdot p^{j/(p-1)} \cdot \frac{1}{q^{j-1}}.$$

Ahora, notemos que:

- Si $q = 4$, entonces $p = 2$ por lo tanto para m.c.d$(a,2) = 1$ tenemos que:

$$\left|\frac{B_j}{j!} \cdot \frac{F^{j-1}}{a^j}\right|_2 \leq 2^j \cdot \left(\frac{2}{4^{j-1}}\right) = 2^j \cdot 2^{1-2j+2} = \frac{1}{2^{j-3}} \leq \frac{1}{4}, \quad \forall\, j \geq 5.$$

  Si $j = 3$, como $B_3 = 0$ tenemos que:

$$\left|\frac{B_3}{3!} \cdot \frac{F^{3-1}}{a^3}\right|_2 = |0|_2 \leq \frac{1}{4}.$$

  Si $j = 4$, como $B_4 = -1/30$, tenemos que:

$$\left|\frac{B_4}{4!} \cdot \frac{F^{4-1}}{a^4}\right|_2 = \frac{|-1/30|_2}{|4!|_2} \cdot \frac{|F^3|_2}{(|a|_2)^4} \leq \frac{2}{2^{-3}} \cdot 2^{-6} = 2^{-2} = \frac{1}{4}.$$

  De forma que:

$$\left|\frac{B_j}{j!} \cdot \frac{F^{j-1}}{a^j}\right|_2 \leq \frac{1}{4}, \quad \forall\, j \geq 3.$$

- Si $q = p$, entonces $p > 2$ luego si $j \geq 3$ tenemos que:

$$\begin{aligned} \frac{j}{p-1} - j + 2 &= j\left(\frac{1}{p-1} - 1\right) + 2 \\ &= j\left(\frac{2-p}{p-1}\right) + 2 \\ &\leq -j + 2 \leq -3 + 2 = -1, \end{aligned}$$

  por lo tanto para m.c.d$(a,p) = 1$ tenemos que:

$$\left|\frac{B_j}{j!} \cdot \frac{F^{j-1}}{a^j}\right|_p \leq p^{j/(p-1)} \cdot \left(\frac{p}{q^{j-1}}\right) = p^{j/(p-1)} \cdot p^{2-j} \leq \frac{1}{p}, \quad j \geq 3.$$

De todo lo anterior concluimos que

$$\therefore \quad \left|\frac{B_j}{j!}\cdot\frac{F^{j-1}}{a^j}\right|_p \leq p^{j/(p-1)}\cdot\left(\frac{p}{q^{j-1}}\right) \leq \frac{1}{q}, \quad j\geq 3.$$

De modo que todos los coeficientes de la serie de potencias

$$\frac{1}{F}\sum_{j\geq 3}\binom{1-s}{j}\left(\frac{F}{a}\right)^j B_j,$$

son divisibles por p. Similarmente, (ver Observación 2.40 y Definición 2.8)

$$\langle a\rangle^{1-s} = \exp_p((1-s)\log_p\langle a\rangle) = \sum_{j=0}^{\infty}\frac{(1-s)^j}{j!}(\log_p\langle a\rangle)^j,$$

tiene todos sus coeficientes en $\mathbb{Z}_p$ y estos son divisibles por pq para $j\geq 2$, dado que $q|\log_p\langle a\rangle$.

En efecto, como $\langle a\rangle \in 1+q\mathbb{Z}_p$ (ver Observación 2.40) tenemos que $|1-\langle a\rangle|_p < p^{-1/(p-1)}$ y así (ver Lema 2.16):

$$|\log_p\langle a\rangle|_p = |\log_p(1+(\langle a\rangle-1)|_p = |1-\langle a\rangle|_p < p^{-1/(p-1)} < 1, \tag{3.18}$$

de esta manera, si $q=p$ tenemos que $\nu_p(\log_p\langle a\rangle)>0$, i.e., $p|\log_p\langle a\rangle$, por otro lado si $q=4$, entonces $p=2$ y así $|\log_2\langle 2\rangle|_2 < 2^{-1}$, i.e., $\nu_2(\log_2\langle a\rangle)>1$, esto es, $4|\log_2\langle a\rangle$. Ahora bien, si $j\geq 2$ tenemos que:

$$\left|\frac{(\log_p\langle a\rangle)^j}{j!}\right|_p \leq q^{-j}\cdot p^{j/(p-1)} = (qp^{-1/(p-1)})^{-j},$$

Notemos que:

- Si $q=4$, tenemos que $p=2$, por lo tanto:

$$\left|\frac{(\log_2\langle a\rangle)^j}{j!}\right|_2 \leq (2^2\cdot 2^{-1})^{-j} = \frac{1}{2^j},$$

de tal modo, $\nu_2((\log_2\langle a\rangle)^j/j!)\geq j$. Así si $j>2$ se cumple que $pq=2^3$ divide a los coeficientes de la serie (3.18). Si $j=2$, entonces, $\nu_2((\log_2\langle a\rangle)^2/2)\geq 4-1=3$. De manera que si $j\geq 2$, concluimos que:

$$pq = 2^3\left|\frac{(\log_2\langle a\rangle)^j}{j!}\right.$$

- Si $q=p$, entonces:

$$\left|\frac{(\log_p\langle a\rangle)^j}{j!}\right|_p \leq (p\cdot p^{-1/(p-1)})^{-j},$$

luego

$$\nu_p\left(\frac{\log_p\langle a\rangle)^j}{j!}\right) \geq j\left(\frac{p-2}{p-1}\right) > 1, \quad j > 2.$$

Si $j = 2$ entonces $\nu_p((\log_p\langle a\rangle)^2/2!) = \nu_p((\log_p\langle a\rangle)^2) \geq 2$. De manera que, si $j \geq 2$, concluimos que:

$$pq = p^2 \left| \frac{(\log_p\langle a\rangle)^j}{j!} \right.$$

Por lo tanto solo necesitamos considerar la suma

$$\frac{1}{s-1}\sum_{\substack{a=1\\ p\nmid a}}^{F} \chi(a)(1+(1-s)\log_p\langle a\rangle)\left(\frac{1}{F} - \frac{1-s}{2a} + \frac{(1-s)(-s)F}{12a^2}\right),$$

notemos que:

$$\frac{1}{s-1}(1+(1-s)\log_p\langle a\rangle)\left(\frac{1}{F} - \frac{1-s}{2a} + \frac{(1-s)(-s)F}{12a^2}\right)$$

es igual a:

$$\begin{aligned} &= \left(\frac{1}{s-1} - \log_p\langle a\rangle\right)\left(\frac{1}{F} + \frac{s-1}{2a} + \frac{(1-s)((1-s)-1)F}{12a^2}\right) \\ &= \left(\frac{1}{s-1} - \log_p\langle a\rangle\right)\left(\frac{1}{F} + \frac{s-1}{2a} + \frac{(1-s)^2F - (1-s)F}{12a^2}\right), \end{aligned}$$

efectuando el producto nos queda como primer término

$$\frac{1/F}{s-1},$$

y como $\chi \neq \chi_1$, entonces (ver Teorema B.13 (iii)):

$$\frac{1}{F}\sum_{a=1}^{F}\chi(a) = 0.$$

Con lo cual la representación en serie de potencias p-ádica de $L_p(s,\chi)$ al rededor de $s = 1$, comienza en a_0. De modo que solo consideramos la siguiente expresión, resultado del producto hecho anteriormente:

$$\left(\frac{1}{2a} + \frac{F}{12a^2} - \frac{1}{F}\log_p\langle a\rangle\right) + \left(\frac{F}{12a^2} - \frac{\log_p\langle a\rangle}{2a} - \frac{F}{12a^2}\log_p\langle a\rangle\right)(s-1) - \frac{\log_p\langle a\rangle F}{12a^2}(s-1)^2.$$

De manera que:

$$a_0 \equiv -\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\left(\frac{1}{F}\log_p\langle a\rangle - \frac{1}{2a} - \frac{F}{12a^2}\right) \pmod{p}.$$

Ahora, $(1/F)\log_p\langle a\rangle$ y $F/12$ pertenecen a $\mathbb{Z}_p$ ya que $\nu_p(\log_p\langle a\rangle) \geq 1$ si $p > 2$, y $\nu_2(\log_2\langle a\rangle) \geq 2$ si $p = 2$, también $\nu_p(F) = 1$, si $p > 2$ y $\nu_2(F) = 2$ si $p = 2$, entonces:

$$\nu_p\left(\frac{1}{F}\log_p\langle a\rangle\right) = \nu_p(\log_p\langle a\rangle) - \nu_p(F) \geq 1 - 1 = 0, \quad \text{si } p > 2$$

y

$$\nu_2\left(\frac{1}{F}\log_2\langle a\rangle\right) = \nu_2(\log_2\langle a\rangle) - \nu_2(F) \geq 2 - 2 = 0, \quad \text{si } p = 2$$

Por otra parte si $q = 4$, entonces $\nu_2(F/12) = \nu_2(F) - \nu_2(12) = 2 - 2 = 0$, si $q = p > 2$ tenemos que $\nu_p(F/12) = \nu_p(F) - \nu_p(12) = 1 - \nu_p(12) \geq 0$. Lo que demuestra la afirmación hecha anteriormente.

Dado que para m.c.d$(a, p) = 1$ se cumple que $\omega(a) \equiv a \pmod q$, por tal motivo $a^{-1} \equiv \omega^{-1}(a) \pmod q$ razón por la cual (ver Observación 3.28):

$$\frac{\chi(a)}{a} \equiv \chi(a)\omega^{-1}(a) = \chi\omega^{-1}(a) \pmod q.$$

Así concluimos que:

$$\sum_{\substack{a=1\\ p\nmid a}}^{F} \frac{\chi(a)}{a} \equiv \sum_{\substack{a=1\\ p\nmid a}}^{F} \chi\omega^{-1}(a) \pmod q$$

Sea f' el conductor del carácter $\chi\omega^{-1}$, como χ es par y ω es impar tenemos que $\chi\omega^{-1} \neq \chi_1$. Con lo cual

$$\sum_{a=1}^{f'} \chi\omega^{-1}(a) = 0.$$

Por otro lado, como $f'|qf$ entonces $f'|F$, luego

$$\sum_{\substack{a=1\\ p\nmid a}}^{F} \chi\omega^{-1}(a) = \sum_{a=1}^{F} \chi\omega^{-1}(a) - \sum_{b=1}^{F/p} \chi\omega^{-1}(pb),$$

la primera suma es 0 ya que $f'|F$. Para la segunda suma, si $p|f'$ tenemos que $\chi\omega^{-1}(pb) = 0$, y la segunda suma es 0. Si $p \nmid f'$ entonces $f'|(F/p)$ dado que $F = Kqf$, de forma que $f'|F = Kqf$, por Lema de Euclides (ya que m.c.d$(f', q) = 1$) $f'|Kf$ y como $Kf|(F/p)$, se sigue la afirmación. De esta manera, concluimos que la segunda suma también es igual a cero.

De todo lo anterior, deducimos que:

$$\frac{1}{2}\sum_{\substack{a=1\\ p\nmid a}}^{F} \frac{\chi(a)}{a} \equiv \frac{1}{2}\sum_{\substack{a=1\\ p\nmid a}}^{\chi} \omega^{-1}(a) = 0 \pmod p,$$

esto demuestra que $|a_0|_p \leq 1$. Por último, para $p \geq 5$ tenemos que:

$$\sum_{\substack{a=1\\ p\nmid a}}^{F} \frac{F\chi(a)}{12a^2} \equiv\ 0 \pmod p,$$

ya que:

$$\nu_p\left(\frac{F\chi(a)}{12a^2}\right) = \nu_p(\chi(a)) + \nu_p(F) - \nu_p(12) - 2\nu_p(a) = \nu_p(F) = 1,$$

dado que $|\chi(a)|_p = 1$, $p|F$ pero $p^2 \nmid F$, $p \nmid 12$ y m.c.d$(a,p) = 1$. Si $p = 2$ ó $p = 3$, tenemos que $a^2 \equiv 1$ (mód p) para $p \nmid a$ y $F/12 \in \mathbb{Z}_p^\times$, luego solo basta considerar la suma:

$$\sum_{\substack{a=1\\ p\nmid a}}^{F} \chi(a) = \sum_{a=1}^{F} \chi(a) - \sum_{b=1}^{F/p} \chi(pb),$$

la primera suma es 0, ya que $f|F$. Si $p|f$ entonces $\chi(pb) = 0$, y la segunda suma es 0, si $p \nmid f$, entonces $f|(F/p)$ y así tenemos que la segunda suma es 0. Luego

$$\sum_{\substack{a=1\\ p\nmid a}}^{F} \chi(a)a^{-2} \equiv \sum_{\substack{a=1\\ p\nmid a}}^{F} \chi(a) = 0 \text{ (mód } p).$$

Después tenemos:

$$a_1 \equiv \sum_{\substack{a=1\\ p\nmid a}}^{f} \chi(a)\left(\frac{F}{12a^2} - \frac{\log_p\langle a\rangle}{2a} - \frac{F\log_p\langle a\rangle}{12a^2}\right) \text{ (mód } p).$$

Por todo lo dicho hasta el momento, $F\log_p\langle a\rangle/12a^2$ y $\log_p\langle a\rangle/2a$ son divisibles entre p y análogamente al caso anterior, basta considerar para los términos que involucran a $F/12a^2$ la suma de los $\chi(a)a^{-2}$, que como ya vimos es igual a 0 módulo p. De lo anterior $p|a_1$.

Finalmente tenemos que:

$$a_2 \equiv -\sum_{\substack{a=1\\ p\nmid a}}^{F} \chi(a)\frac{\log_p\langle a\rangle F}{12a^2} \equiv 0 \text{ (mód } p),$$

ya que todos lo términos de la suma son divisibles entre p. Y así finalmente completamos la demostración. □

La mayoría de las congruencias para lo números de Bernoulli y los números de Bernoulli generalizados se siguen del teorema anterior.

Corolario 3.33. *Si $\chi \neq \chi_1$, entonces*

$$L_p(1,\chi) \equiv -\frac{1}{F}\sum_{\substack{a=1\\ p\nmid a}}^{F} \chi(a)\log_p\langle a\rangle \text{ (}\textit{mód } p\text{)}$$

Demostración. Se sigue de los razonamientos dados en la congruencia:

$$a_0 \equiv -\sum_{\substack{a=1\\ p\nmid a}}^{F} \chi(a)\left(\frac{1}{F}\log_p\langle a\rangle - \frac{1}{2a} - \frac{F}{12a^2}\right) \text{ (mód } p),$$

en el Teorema 3.31. □

Corolario 3.34. *Supongamos $\chi \neq \chi_1$, $pq \nmid f$. Sean $m, n \in \mathbb{Z}$, entonces:*

$$L_p(m, \chi) \equiv L_p(n, \chi) \ (mód\ p)$$

y ambos son p-enteros.

Demostración. Por Teorema 3.31, tenemos que $L_p(m, \chi) \equiv a_0 \pmod{p}$ y también $L_p(n, \chi) \equiv a_0 \pmod{p}$ de donde se sigue el resultado por transitividad de la congruencia.

□

Corolario 3.35. ***Congruencias de Kummer -1851-*** *Supongamos que para $m, n \in \mathbb{Z}_+$, números pares, se cumple que $m \equiv n \not\equiv 0$ (mód $p-1$), entonces:*

$$\frac{B_m}{m} \equiv \frac{B_n}{n} \ (mód\ p).$$

De manera general, si m, n son enteros positivos pares con $m \equiv n$ (mód $\varphi(p^a)$) y $n \not\equiv 0$ (mód $p-1$), entonces:

$$(1 - p^{m-1})\frac{B_m}{m} \equiv (1 - p^{n-1})\frac{B_n}{n} \ (mód\ p^a).$$

Demostración. Como $n \equiv m \not\equiv 0 \pmod{\varphi(p^a)}$, entonces $n - m = K(p-1)p^{a-1}$ con $k \neq 0$, luego $\omega^{m-n}(b) = \omega^{K(p-1)p^{a-1}}(b) = 1$ para todo b con $p \nmid b$, esto es $\omega^{m-n} = \chi_1$, por lo tanto $\omega^m = \omega^n$.

Consideremos pues $L_p(s, \omega^m) = L_p(s, \omega^n)$, entonces

$$L_p(1 - m, \omega^m) = -(1 - p^{m-1})\frac{B_m}{m}, \quad \text{y} \quad L_p(1 - n, \omega^n) = -(1 - p^{n-1})\frac{B_n}{n}.$$

También, como $p|a_j$ para $j \geq 1$ (ver Teorema 3.31), tenemos:

$$\begin{aligned} L_p(1 - m, \omega^m) &= a_0 + a_1(-m) + a_2(-m)^2 + \cdots \\ &\equiv a_0 + a_1(-n) + a_2(-n)^2 + \cdots \pmod{p^a} \\ &= L_p(1 - n, \omega^n), \end{aligned}$$

de manera que

$$L_p(1 - m, \omega^m) \equiv L_p(1 - n, \omega^n) \pmod{p^a}.$$

De donde se sigue el resultado.

□

Corolario 3.36. *Supongamos n es entero impar con $n \not\equiv -1$ (mód $p-1$), entonces:*

$$B_{1,\omega^n} \equiv \frac{B_{n+1}}{n+1} \ (mód\ p).$$

Demostración. Dado que $n \not\equiv -1 \pmod{p-1}$, tenemos que $\omega^{n+1} \neq \chi_1$. También, $\omega^n(p) = 0$ ya que ω^n no es el carácter trivial. De modo que, por Corolario 3.34, tenemos que:

$$\begin{aligned} B_{1,\omega^n} &= (1-\omega^n(p))B_{1,\omega^n} = -L_p(0,\omega^{n+1}) \\ &\equiv -L_p(1-(n+1),\omega^{n+1}) = (1-p^n)\frac{B_{n+1}}{n+1} \\ &\equiv \frac{B_{n+1}}{n+1} \pmod{p}. \end{aligned}$$

□

Recordemos del Capítulo 1 Definición 1.34, que un primo es llamado regular si no divide el numerador de los números de Bernoulli B_k con k entero par y menor o igual a $p-3$. Podemos caracterizar el valor $L_p(1,\chi)$ cuando p es primo regular y χ es un carácter específico, como vemos en el siguiente teorema:

Teorema 3.37. *Si p es un primo regular y k es entero par con $k \not\equiv$ (mód $p-1$), entonces $L_p(1,\omega^k) \not\equiv 0$ (mód p). En particular $L_p(1,\omega^k) \neq 0$.*

Demostración. Por Teorema 3.31, tenemos que:

$$L_p(1-k,\omega^k) = -(1-p^{k-1})\frac{B_k}{k},$$

y por Corolario 3.34, tenemos que:

$$L_p(1,\omega^k) \equiv -(1-p^{k-1})\frac{B_k}{k} \pmod{p}.$$

Como $(p-1) \nmid k$ por Congruencia de Adams (ver Teorema 1.31) concluimos que $B_k/k \in \mathbb{Z}_{(p)}$, (en particular $L_p(1,\omega^k)$ es p-entero) y por Definición C.22, tenemos que $\nu_p(B_k/k) \geq 0$. Si $\nu_p(B_k/k) > 0$, entonces para $B_k = U_k/V_k$ tenemos que:

$$1 \leq \nu_p\left(\frac{B_k}{k}\right) = \nu_p(U_k) - \nu_p(V_k k),$$

Ahora como $\nu_p(V_k k) = 0$ (ver Lema C.23 (i)), concluimos que $\nu_p(U_k) \geq 1$, i.e., $p \nmid U_k$, lo que no puede ocurrir ya que p es primo regular. Por lo tanto

$$-(1-p^{k-1})\frac{B_k}{k} \not\equiv 0 \pmod{p},$$

de donde se concluye que $L_p(1,\omega^k) \not\equiv 0 \pmod{p}$, con lo cual $|L_p(1,\omega^k)|_p = 1$, i.e., $L_p(1,\omega^k) \neq 0$.

□

Podemos decir un poco más acerca de $L_p(1,\chi)$, lo cual presentamos en el siguiente teorema, para un estudio más detallado de $L_p(1,\chi)$ (ver [14], c. 5).

Teorema 3.38. *Sea χ carácter de Dirichlet de conductor $f > 1$ y sea F múltiplo de q y f, entonces:*

$$L_p(1,\chi) = \frac{1}{F}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\left(-\log_p\langle a\rangle + \sum_{j=1}^{\infty}\frac{B_j}{j}\left(-\frac{F}{a}\right)^j\right) \tag{3.19}$$

Demostración. Haciendo el cambio de variable $1-s$ por s en (3.17) en el Teorema 3.29, nos da:

$$L_p(1-s,\chi) = -\frac{1}{F}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\frac{1}{s}\langle a\rangle^s\sum_{j=0}^{\infty}\binom{s}{j}\left(\frac{F}{a}\right)^j B_j.$$

Notemos que:

$$\frac{1}{s}\langle a\rangle^s = \frac{1}{s} + \log_p\langle a\rangle + G(s,a),$$

donde

$$G(s,a) = \sum_{j=2}^{\infty}\frac{s^{j-1}}{j!}(\log_p\langle a\rangle)^j,$$

por lo tanto $L_p(1-s,\chi)$ es igual a:

$$-\frac{1}{F}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\left(\frac{1}{s} + \frac{1}{s}J(s,a) + \log_p\langle a\rangle + \log_p\langle a\rangle J(s,a) + G(s,a) + G(s,a)J(s,a)\right),$$

donde

$$J(s,a) = \sum_{j=1}^{\infty}\binom{s}{j}\left(\frac{F}{a}\right)^j B_j.$$

Notemos que en la demostración del Teorema 3.29, establecimos para $\chi \neq \chi_1$ que $L_p(1-s,\chi)$ era analítica en su dominio de convergencia y además que en este caso:

$$-\frac{1}{F}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a) = 0,$$

En consecuencia se puede prescindir del término en $1/s$ de la serie que define a la función $L_p(1-s,\chi)$. Por otra parte:

$$\frac{1}{s}J(s,a) = \sum_{j=1}^{\infty}\frac{(s-1)\cdots(s-j+1)}{j!}\left(\frac{F}{a}\right)^j B_j \longrightarrow -\sum_{j=1}^{\infty}\frac{(-1)^j}{j}\left(\frac{F}{a}\right)^j B_j,$$

cuando $s \to 0$, luego podemos definir:

$$\frac{1}{s}J(s,a) = -\sum_{j=1}^{\infty}\frac{B_j}{j}\left(-\frac{F}{a}\right)^j, \quad \text{en } s = 0.$$

Ahora, como $J(0,a) = 0$ y $G(0,a) = 0$, entonces:

$$L_p(1,\chi) = -\frac{1}{F}\sum_{\substack{a=1 \\ p\nmid a}}^{F} \chi(a)\left(\log_p\langle a\rangle - \sum_{j=1}^{\infty}\frac{B_j}{j}\left(-\frac{F}{a}\right)^j\right).$$

Como se quería demostrar.

□

Una de las áreas de investigación moderna con las funciones L p-ádicas es determinar sus valores en los enteros positivos. Avances en esta dirección están dados en [7], donde Jack Diamond en 1979 obtiene fórmulas de los valores $L_p(r,\chi)$ para r entero positivo, en términos de la función log gamma p-ádica. En 1992, Hideo Imai en [12], generaliza el resultado dado por Diamond y obtiene fórmulas de estos valores en términos de la función log gamma múltiple p-ádica. Aunque se espera que la ecuación que determine los valores $L_p(r,\chi)$ para r entero mayor igual que dos, no involucren series infinitas.

Apéndice A

Función Zeta de Riemann

La intención de este apéndice es definir la función zeta de Riemann ζ. A continuación realizamos su extensión meromorfa al plano complejo y presentamos una de sus ecuaciones funcionales, la demostración depende de una fórmula integral de la función $\zeta(s)$ que involucra a la función *gamma* Γ, razón por la cuál introducimos un breve estudio de la función Γ y damos algunas de sus propiedades, solo haciendo un bosquejo de sus demostraciones. En el camino también encontramos algunos conceptos ligados a la serie *theta* ϑ de *Jacobi*, de la cual solo utilizaremos su ecuación funcional tanto como sus leyes de crecimiento y decaimiento.

Definición A.1. *Sea $s \in \mathbb{C}$, definimos la serie* ***Zeta de Riemann*** *como*

$$\zeta(s) = \sum_{n=1}^{+\infty} n^{-s}.$$

Mostraremos ahora que esta serie define una función holomorfa para todo $s \in \mathbb{C}$ con $\mathrm{Re}(s) > 1$.

Proposición A.2. *La serie $\zeta(s)$ converge absolutamente para $Re(s) > 1$, esto implica que ζ es una función holomorfa en el semiplano $Re(s) > 1$.*

Demostración. Basta demostrar que la serie ζ converge uniformemente en todo disco cerrado en $A = \{s \in \mathbb{C} : \mathrm{Re}(s) > 1\}$. Sea $\delta > 0$ la distancia entre el disco cerrado $D \subset A$ y la recta $\mathrm{Re}(s) = 1$. Notemos que $n^{-s} = e^{-s\log(n)}$, donde $\log(n)$ es el logaritmo usual en los número reales. Ahora

$$|n^{-s}| = |e^{-s\log(n)}| = e^{-\mathrm{Re}(s)\log(n)} = n^{-\mathrm{Re}(s)}.$$

Si $s \in D$, entonces $\sigma = \mathrm{Re}(s) \geq 1 + \delta$, y así tenemos que

$$|n^{-s}| = n^{-\sigma} \leq n^{-(1+\delta)},$$

por lo tanto, si $M_n = n^{-(1+\delta)}$, por el test M de Weirstrass $\sum_{n\geq 1} |n^{-s}|$, converge absolutamente en D.

□

Ahora presentamos la conocida relación que existe entre la serie ζ y los números primos.

Proposición A.3. ***Identidad de Euler****. La función ζ admite la siguiente representación:*

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

para $Re(s) > 1$, donde p recorre todos lo números primos.

Demostración. Sea $\sigma = Re(s)$ y demostremos que el producto de la derecha converge para $\sigma > 1$. Para esto, primero demostramos que la sucesión de los productos parciales de la derecha convergen a un límite diferente de cero, esto pasa si y solo si la serie de los logaritmos de cada termino converge, donde el logaritmo es definido en la rama principal.

Sea entonces

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

$$\begin{aligned} \therefore \quad \log E(s) &= \sum_p \log[(1 - p^{-s})^{-1}] \\ &= \sum_p (-1) \log(1 - p^{-s}) \\ &= \sum_p \sum_{n \geq 1} (np^{ns})^{-1}, \end{aligned}$$

donde hemos utilizado la expansión en serie de potencias de la rama principal del logaritmo complejo, ya que $|p^{-s}| < 1$.

Esta serie converge absolutamente para $\sigma \geq 1 + \delta$, para todo $\delta > 0$. De hecho, dado que $|p^{ns}| = p^{n\sigma} \geq p^{n(1+\delta)}$, tenemos que

$$\begin{aligned} \sum_p \sum_{n \geq 1} |(np^{ns})^{-1}| &\leq \sum_p \sum_{n \geq 1} n^{-1} p^{-n(1+\delta)} \\ &\leq \sum_p \sum_{n \geq 1} p^{-n(1+\delta)} \\ &= \sum_p \left(p^{1+\delta} - 1\right)^{-1} \\ &< 2 \sum_p p^{-(1+\delta)} < \infty, \end{aligned}$$

donde hemos utilizado la convergencia de la serie geometrica para $\left|p^{-(1+\delta)}\right| < 1$ y la última desigualdad se da ya que, $p^{1+\delta} > p \geq 2$ luego $p^{1+\delta} > 2$, esto es, $p^{1+\delta} \cdot 2^{-1} > 1$, por tanto $p^{1+\delta} - 1 > p^{1+\delta} - \frac{p^{1+\delta}}{2} = \frac{p^{1+\delta}}{2}$.

La convergencia absoluta de la serie anterior implica la convergencia absoluta del producto para $\sigma = \mathrm{Re}(s) > 1$, tenemos entonces

$$E(s) = \prod_p (1 - p^{-s})^{-1} = \exp\left(\sum_p \sum_{n\geq 1} (np^{ns})^{-1}\right).$$

En este producto expandimos cada factor

$$\frac{1}{1-p^{-s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots$$

para los primos $p_1, ..., p_r \leq N$, y obtenemos

$$\prod_{p\leq N} (1 - p^{-s})^{-1} = \sum_{\nu_1,\ldots,\nu_r=0}^{+\infty} (p_1^{\nu_1} \cdots p_r^{\nu_r})^{-s} = \sum_{\substack{n \\ p_k | n \\ 1\leq k\leq r}} n^{-s}. \tag{A.1}$$

Dado que la última suma contiene en particular a los terminos correspondientes a los $n \leq N$, así podemos también escribir

$$\prod_{p\leq N} (1 - p^{-s})^{-1} = \sum_{n\leq N} n^{-s} + \sum_{\substack{n>N \\ p_k | n \\ 1\leq k\leq r}} n^{-s}.$$

Comparando ahora la suma en (A.1) con la serie $\zeta(s)$, tenemos

$$\left| \prod_{p\leq N} (1 - p^{-s})^{-1} - \zeta(s) \right| \leq \sum_{\substack{n>N \\ p_k \nmid n \\ 1\leq k\leq r}} |n^{-s}| \leq \sum_{n>N} n^{-(1+\delta)},$$

donde la serie de la derecha tiende a cero cuando N tiende a infinito, ya que es la cola de una serie convergente.

□

Definición A.4. ***Función Gamma****. Sea $s \in \mathbb{C}$ tal que $Re(s) > 0$, definimos la función gamma como*

$$\Gamma(s) = \int_0^\infty e^{-t} t^{s-1} dt. \tag{A.2}$$

Para la demostración detallada del siguiente hecho (ver [23], cap. 6). La expresión (A.2) define una función holomorfa en el semiplano $\mathrm{Re}(s) > 0$, ya que para cada $\epsilon > 0$, las funciones

$$F_\epsilon(s) = \int_\epsilon^{\frac{1}{\epsilon}} e^{-t} t^{s-1} dt,$$

definen una función holomorfa en cada banda $S_{\delta,M} = \{s \in \mathbb{C} : \delta < \mathrm{Re}(s) < M\}$, con $\delta > 0$ (ver [23], teorema 5.4, cap. 2), y dado que

$$\lim_{\epsilon\to 0} F_\epsilon(s) = \Gamma(s)$$

y esta convergencia es uniforme en $S_{\delta,M}$, se obtiene el resultado.

A pesar del hecho que la integral definida en (A.2) que a su vez define a Γ no es absolutamente convergente para otros valores de s, se puede demostrar que existe una función meromorfa al plano complejo, cuyos polos se encuentran en los valores $s = 0, -1, -2, -3, \cdots$. La unicidad de la extensión meromorfa nos permite seguir denotanado a la nueva funcióm por Γ.

Proposición A.5. *(i) La función gamma admite una extensión meromorfa a* $\mathbb{C}$.

(ii) Las únicas singularidades de la función gamma son polos simples en los enteros $s = 0, -1, -2, \cdots$, *donde* $Res_{s=-n} = (-1)^n/n!$.

(iii) Algunas ecuaciones funcionales de la función gamma son

(1) $\Gamma(s+1) = s\Gamma(s)$,

(2) $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s}$,

(iv) $\Gamma(1/2) = \sqrt{\pi}$, $\Gamma(1) = 1$, $\Gamma(n+1) = n!$ *para todo* $n \in \mathbb{N}$.

A continuación se realiza un bosquejo de la demostración de la proposición anterior. Empezamos con la observación que para $\mathrm{Re}(s) > 0$, se tiene que $\Gamma(s+1) = s\Gamma(s)$, en efecto,

$$\int_\epsilon^{1/\epsilon} \frac{d}{dt}\left(e^{-t}t^s\right) dt = -\int_\epsilon^{1/\epsilon} e^{-t}t^s dt + s\int_\epsilon^{1/\epsilon} e^{-t}t^{s-1}dt,$$

donde la integral finita de la izquierda tiende a cero cuando $\epsilon \to 0$, a su vez de la fórmula (A.2) para Γ se obtiene el resultado deseado. A partir de este hecho, primero concluimos de (A.2) que

$$\Gamma(1) = \int_0^\infty e^{-t}dt = \lim_{\epsilon\to 0}\int_\epsilon^{1/\epsilon} e^{-t}dt = \lim_{\epsilon\to 0} -e^{-t}|_\epsilon^{1/\epsilon} = 1,$$

y dado que para $n \in \mathbb{N}$, $\Gamma(n+1) = n\Gamma(n)$, procediendo inductivamente, deducimos que $\Gamma(n+1) = n!$.

Ahora bien, para demostrar la extensión meromorfa de Γ, es suficiente extender Γ a cada semiplano $\mathrm{Re}(s) > -m$, donde $m \in \mathbb{Z}_+$. Luego para $\mathrm{Re}(s) > -1$, se define la función

$$F_1(s) = \frac{\Gamma(s+1)}{s},$$

la cual es define una función meromorfa, con un polo simple en $s = 0$, y dado que si $\mathrm{Re}(s) > 0$, entonces $F_1(s) = \Gamma(s)$, luego F_1 es una extensión meromorfa de Γ en el semiplano $\mathrm{Re}(s) > -1$. Procediendo inductivamente, para $\mathrm{Re}(s) > -m$, se define

$$F_m(s) = \frac{\Gamma(s+m)}{(s+m-1)(s+m-2)\cdots s},$$

la cual es meromorfa en el semiplano $\mathrm{Re}(s) > -m$, y posee polos simples en los valores $s = 0, -1, -2, \cdots, -(m-1)$, además, $F_m(s) = \Gamma(s)$ en el semiplano $\mathrm{Re}(s) > 0$. Por

unicidad de las extensiones, esto también implica que $F_m = F_k$ para $1 \leq k \leq m$, en el dominio de definición de F_k. Así se obtiene la continuación analítica de Γ.

Para obtener la segunda ecuación funcional, hacemos uso del lema (ver [23], ej. 2, sec. 2.1, cap. 3).

Lema A.6. *Para* $0 < a < 1$

$$\int_0^\infty \frac{v^{a-1}}{1+v} dv = \frac{\pi}{\sin \pi a}.$$

Así, primero notando que para $0 < s < 1$ podemos escribir

$$\Gamma(1-s) = \int_0^\infty e^{-u} u^{-s} du = t \int_0^\infty e^{-vt} (-vt)^{-s} dv,$$

donde para $t > 0$ se hizo el cambio de variable $vt = u$. Luego

$$\begin{aligned}
\Gamma(1-s)\Gamma(s) &= \int_0^\infty e^{-t} t^{s-1} \Gamma(1-s) dt \\
&= \int_0^\infty e^{-t} t^{s-1} \left(t \int_0^\infty e^{-vt} (vt)^{-s} dv \right) dt \\
&= \int_0^\infty \int_0^\infty e^{-t(1+v)} v^{-s} dv dt \\
&= \int_0^\infty \int_0^\infty e^{-t(1+v)} v^{-s} dt dv \\
&= \int_0^\infty \frac{v^{-s}}{1+v} dv = \frac{\pi}{\sin \pi(1-s)} \\
&= \frac{\pi}{\sin \pi s}.
\end{aligned}$$

En particular, tomando $s = 1/2$, tenemos que

$$\begin{aligned}
\Gamma(1/2)^2 &= \frac{\pi}{\sin \pi/2} = \pi \\
\therefore \Gamma(1/2) &= \sqrt{\pi}.
\end{aligned}$$

Otra ecuación funcional (ver [22], c.1, pág. 23.) que enventualmente se usará es

$$\Gamma(s)\Gamma(s+\frac{1}{2}) = \frac{2\sqrt{\pi}}{2^{2s}} \Gamma(2s) \quad (\textbf{Fórmula de duplicación de Legendre}). \tag{A.3}$$

Definición A.7. ***Función Theta de Jacobi.*** *Para $t \in \mathbb{R}$ con $t > 0$, definimos*

$$\vartheta(t) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 t} \tag{A.4}$$

Como una aplicación de la fórmula de sumación de Poisson (ver [23], teorema 2.4, cap.4) se obtiene la ecuación funcional

$$\vartheta(t) = t^{-1/2}\vartheta(1/t). \tag{A.5}$$

Notemos ahora que

$$|\vartheta(t) - 1| \leq Ce^{-\pi t} \quad \text{para algún } C > 0, \text{ y todo } t \geq 1. \tag{A.6}$$

En efecto, por (A.4)

$$\vartheta(t) = 1 + 2\sum_{n\geq 1} e^{-\pi n^2 t}, \tag{A.7}$$

por otro lado, dado que $-\pi n^2 t \leq -\pi n t$ para todo $t \geq 1$, entonces

$$\sum_{n\geq 1} e^{-\pi n^2 t} \leq \sum_{n\geq 1} e^{-\pi n t} = e^{-\pi t}\sum_{n\geq 1} e^{-\pi(n-1)t} \leq C_1 e^{-\pi t}; \quad \text{con} \quad C_1 > 0,$$

ya que la serie $\sum_{n\geq 1} e^{-\pi(n-1)t}$ es convergente para $t \geq 1$ (se puede utilizar el criterio de la integral para verificarlo), por tanto de (A.7), tenemos que

$$|\vartheta(t) - 1| \leq 2\sum_{n\geq 1} e^{-\pi n^2 t} \leq 2C_1 e^{-\pi t} = Ce^{-\pi t}.$$

Para relacionar la función gamma con la función zeta, hacemos la sustitución $t = \pi n^2 y$ en la definición de la función gamma, luego $dt = \pi n^2 dy$, y así

$$\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}dt = \pi^s n^{2s}\int_0^\infty e^{-\pi n^2 y}y^{s-1}dy,$$

por tanto

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

y al sumar sobre $n \geq 1$, tenemos que

$$\sum_{n\geq 1}\pi^{-s}\Gamma(s)n^{-2s} = \sum_{n\geq 1}\int_0^\infty e^{-\pi n^2 y}y^{s-1}dy$$
$$\pi^{-s}\Gamma(s)\sum_{n\geq 1} n^{-2s} = \sum_{n\geq 1}\int_0^\infty e^{-\pi n^2 y}y^{s-1}dy.$$

Por otro lado, para la serie del lado derecho, haciendo $\mathrm{Re}(s) = \sigma$ tenemos que

$$\sum_{n\geq 1}\int_0^\infty |e^{-\pi n^2 y}y^{s-1}|dy = \sum_{n\geq 1}\int_0^\infty e^{-\pi n^2 y}y^{\sigma-1}dy.$$

Sea $x = \pi n^2 y$, luego $dx = \pi n^2 dy$, y por tanto

$$\begin{aligned}\sum_{n\geq 1}\int_0^\infty e^{-\pi n^2 y} y^{\sigma-1} dy &= \sum_{n\geq 1}\int_0^\infty e^{-x}\frac{x^{\sigma-1}}{(\pi n^2)^{\sigma-1}}\frac{dx}{\pi n^2}\\ &= \sum_{n\geq 1}\int_0^\infty e^{-x}\frac{x^{\sigma-1}}{\pi^\sigma n^{2\sigma}}dx\\ &= \frac{1}{\pi^\sigma}\sum_{n\geq 1}\frac{1}{n^{2\sigma}}\left(\int_0^\infty e^{-x}x^{\sigma-1}dx\right)\\ &= \pi^{-\sigma}\zeta(2\sigma)\Gamma(\sigma) < +\infty, \quad \text{si} \quad \sigma > \frac{1}{2}.\end{aligned}$$

Luego por teorema 2.25 de [9], tenemos que

$$\sum_{n\geq 1}\int_0^\infty e^{-\pi n^2 y} y^{s-1} dy = \int_0^\infty \sum_{n\geq 1} e^{-\pi n^2 y} y^{s-1} dy.$$

Así concluimos que

$$\pi^{-s}\Gamma(s)\zeta(2s) = \int_0^\infty \sum_{n\geq 1} e^{-\pi n^2 y} y^{s-1} dy,$$

notemos además que la serie bajo la integral, por (A.7) se puede ver como

$$\sum_{n\geq 1} e^{-\pi n^2 y} = \frac{1}{2}(\vartheta(y) - 1).$$

Definición A.8. ***Función Xi.*** *Sea $s \in \mathbb{C}$, con $Re(s) > 1$, definimos*

$$\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s) \tag{A.8}$$

Por lo hecho anteriormente, tenemos entonces que

Proposición A.9. *La función $\xi(s)$, para $Re(s) > 1$ admite la represetación integral*

$$\xi(s) = \frac{1}{2}\int_0^\infty (\vartheta(y) - 1) y^{s-1} dy. \tag{A.9}$$

Ahora podemos hacer la extensión analítica de la función ξ, y encontrar cierta ecuación funcional.

Proposición A.10. *La función ξ es holomorfa para $Re(s) > 1$ y tiene continuación analítica a todo $\mathbb{C}$ como función meromorfa con polos simples en $s = 0$ y $s = 1$. Más aún, sastisface la siguiente ecuación funcional*

$$\xi(s) = \xi(1 - s) \quad \forall s \in \mathbb{C} \tag{A.10}$$

Demostración. Sea $\psi(u) = [\vartheta(u) - 1]/2$. La ecuación funcional para la función theta en (A.5), implica

$$\begin{aligned}\psi(u) &= \frac{1}{2}\vartheta(u) - \frac{1}{2} \\ &= \frac{u^{-1/2}}{2}\vartheta(1/u) - \frac{1}{2} \\ &= \frac{u^{-1/2}}{2}\vartheta(1/u) - \frac{u^{-1/2}}{2} + \frac{u^{-1/2}}{2} - \frac{1}{2} \\ &= u^{-1/2}\frac{[\vartheta(1/u) - 1]}{2} + \frac{1}{2u^{1/2}} - \frac{1}{2}\end{aligned}$$

$$\therefore\ \ \psi(u) = u^{-1/2}\psi(1/u) + \frac{1}{2u^{1/2}} - \frac{1}{2}.$$

Luego para $\mathrm{Re}(s) > 1$, tenemos

$$\begin{aligned}\pi^{-s/2}\Gamma(s/2)\zeta(s) &= \int_0^\infty u^{(s/2)-1}\psi(u)du \\ &= \int_0^1 u^{(s/2)-1}\psi(u)du + \int_1^\infty u^{(s/2)-1}\psi(u)du \\ &= \int_0^1 u^{(s/2)-1}\left[u^{-1/2}\psi(1/u) + \frac{1}{2u^{1/2}} - \frac{1}{2}\right]du + \int_1^\infty u^{(s/2)-1}\psi(u)du,\end{aligned}$$

resolviendo la primera integral con detalle, vemos que es igual a

$$\begin{aligned}&\int_0^1 \left[u^{(s/2)-\frac{3}{2}}\psi(1/u) + \frac{1}{2}u^{(s/2)-\frac{3}{2}} - \frac{1}{2}u^{(s/2)-1}\right]du \\ &= \int_0^1 u^{(s/2)-\frac{3}{2}}\psi(1/u)du + \int_0^1 \frac{1}{2}u^{(s/2)-\frac{3}{2}}du - \int_0^1 \frac{1}{2}u^{(s/2)-1}du \\ &= \frac{1}{s-1} - \frac{1}{s} + \int_0^1 u^{(s/2)-\frac{3}{2}}\psi(1/u)du.\end{aligned}$$

Ahora, haciendo un cambio de variable $v = 1/u$, tenemos que $-u^2dv = du$. Por tanto

$$\int_0^1 u^{(s/2)-\frac{3}{2}}\psi(1/u)du = -\int_\infty^1 v^{-s/2-1/2}\cdot u^{-2}\cdot\psi(v)\cdot u^2 dv = \int_1^\infty v^{(-s/2)-1/2}\psi(v)dv.$$

Así las cosas, tenemos que solo por cuestiones de notación, esto es haciendo $u = v$

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \frac{1}{s-1} - \frac{1}{s} + \int_1^\infty \left(v^{(-s/2)-1/2} + v^{(s/2)-1}+\right)\psi(v)dv, \qquad (A.11)$$

por el decaimiento exponencial de ψ, introducido en (A.6), la integral (ver [23], teorema 5.4, cap. 2) define una función entera, esto implica que ψ posee una continuación analítica a todo $\mathbb{C}$ como función meromorfa, con polos simples en $s = 0$ y $s = 1$, como la expresión permanece invariante si reemplazamos s por $1 - s$, concluimos entonces la ecuación funcional

$$\xi(s) = \xi(1-s)\ \ \forall s \in \mathbb{C}.$$

□

Directamente de la proposición anterior, tenemos la extensión meromorfa deseada para la función zeta.

Proposición A.11. *La función zeta de Riemann ζ posee una continuación analítica a todo $\mathbb{C}$ como función meromorfa con un polo simple en $s = 1$. Más aún, se satisface la siguiente ecuación funcional*

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \pi^{-(1-s)/2}\Gamma((1-s)/2)\zeta(1-s) \quad \forall s \in \mathbb{C}^{\times} \tag{A.12}$$

Demostración. Como $\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$, entonces

$$\zeta(s) = \pi^{s/2}\frac{\xi(s)}{\Gamma(s/2)},$$

ahora como $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s}$, entonces tenemos que

$$\frac{1}{\Gamma(s)} = \Gamma(1-s)\frac{\sin \pi s}{\pi},$$

luego los polos simples de $\Gamma(1-s)$, los cuales se encuentran en los valores $s = 1, 2, 3, \cdots$ son cancelados por los ceros simples de $\sin \pi s$ en estos mismos valores, y por tanto $1/\Gamma$ es entera con ceros simples en los valores $s = 0, -1, -2, -3, \cdots$. Con lo cual, la función $1/\Gamma(s/2)$ es entera con ceros simples en $s = 0, -2, -4, \cdots$, por tanto el polo simple de $\xi(s)$ en $s = 0$ es cancelado. Y por la proposición anterior dado que ξ posee una continuación analítica a todo $\mathbb{C}$ de manera holomorfa con polo simple en $s = 1$, se sigue el resultado. La ecuación funcional no es mas que la relación $\xi(s) = \xi(1-s)$ para todo $s \in \mathbb{C}$ de la proposición anterior. □

Apéndice B

Carácter de Dirichlet

Los caracteres de Dirichlet son utilizados en la definición de las funciones L de Dirichlet y las funciones L p-ádicas. La idea es presentar el concepto de carácter de Dirichlet basado en la teoría de caracteres de grupos abelianos finitos, además de dar ciertos resultados relevantes sobre ellos que serán utilizados de manera usual a lo largo del texto, y que son indispensables en la definición del grupo de caracteres primitivos, objetivo principal de este apéndice.

Definición B.1. *Sea G un grupo. Una función $f : G \to \mathbb{C}^\times$, es llamada* ***carácter*** *de G si f es homomorfismo de grupos con respecto a la multiplicación compleja, es decir*

$$f(ab) = f(a)f(b) \quad \forall\ a, b \in G,$$

Teorema B.2. *Si f es un carácter de un grupo finito G con elemento identidad e, entonces $f(e) = 1$ y cada valor $f(a)$ con $a \in G$ es una raíz de la unidad. De hecho, si $a^n = e$ para algún $n \in \mathbb{Z}_+$, entonces $f(a)^n = 1$.*

Demostración. La primera afirmación se tiene ya que f es homomorfismo. Por otro lado, al ser G grupo finito, para $a \in G$ existe $n \in \mathbb{Z}_+$ tal que $a^n = e$, entonces $1 = f(e) = f(a^n) = f(a)^n$.

□

Cada grupo G posee al menos un carácter, a saber la función que es identicamente 1 en G.

Definición B.3. *Sea G grupo, llamamos* ***carácter principal*** *con respecto a G al carácter f tal que $f(g) = 1$ para todo $g \in G$.*

Aunque ciertamente este no es el único carácter que existe para un grupo abeliano finito de orden mayor que 1. A saber tenemos

Teorema B.4. *Un grupo abeliano finito G de orden n, tiene exactamente n caracteres distintos.*

Demostración. (Ver [1], cap. 6, teorema 6.8, pág. 138).

□

Observación B.5. *Sea G grupo abeliano finito de orden n, al carácter principal de G lo denotamos por f_1, los otros caracteres denotados por $f_2, ..., f_n$ son llamados caracteres no principales. Estos últimos tienen la propiedad que $f_k(a) \neq 1$ para algún $a \in G$, $1 < k \leq n$.*

Teorema B.6. *Definamos la multiplicación de caracteres por la relación*

$$(f_j f_k)(a) = f_j(a) f_k(a) \quad \forall\ a \in G, \tag{B.1}$$

entonces el conjunto de caracteres de G forma un grupo abeliano de orden n. Denotamos a este grupo por $\hat{G}$. El elemento identidad de $\hat{G}$ es el carácter principal f_1. El inverso de f_j es el recíproco $1/f_j$.

Demostración. (1) *Cerradura:* Sean f_j, f_k caracteres de G, grupo abeliano finito con $|G| = n$. Probemos que $(f_j f_k)$ es carácter de G. Sean $a, b \in G$, entonces si $a = b$:

$$(f_j f_k)(a) = f_j(a) f_k(a) = f_j(b) f_k(b) = (f_j f_k)(b),$$

ya que f_j y f_k son funciones, esto demuestra que $f_j f_k$ definida en (B.1) es función de G a $\mathbb{C}^\times$.

Por otro lado, tenemos:

$$\begin{aligned}(f_j f_k)(ab) &= f_j(ab) f_k(ab) \\ &= f_j(a) f_k(a) f_j(b) f_k(b) \\ &= (f_j f_k)(a)(f_j f_k)(b),\end{aligned}$$

ya que f_j y f_k son homomorfismos de G a $\mathbb{C}^\times$, esto demuestra que $f_j f_k$ definida en (B.1) es homormorfismo de G a $\mathbb{C}^\times$. De lo anterior $f_j f_k$ es carácter de G.

(2) *Asociatividad:* Sean f_j, f_k, f_l caracteres de G. Debemos demostrar que $(f_j f_k) f_l = f_j(f_k f_l)$. Sea $a \in G$, luego:

$$\begin{aligned}[(f_j f_k) f_l](a) &= (f_j f_k)(a) f_l(a) \\ &= [f_j(a) f_k(a)] f_l(a) \\ &= f_j(a)[f_k(a) f_l(a)] \\ &= f_j(a)(f_k f_l)(a) = [f_j(f_k f_l)](a)\end{aligned}$$

$\therefore$ La multiplicación es asociativa.

(3) *Elemento Neutro:* Sea f_1 el carácter principal de G. Debemos demostrar que $f_j f_1 = f_1 f_j = f_j$, sea $a \in G$, luego:

$$\begin{aligned}(f_j f_1)(a) &= f_j(a) f_1(a) = f_j(a) \cdot 1 = f_j(a) \\ (f_1 f_j)(a) &= f_1(a) f_j(a) = 1 \cdot f_j(a) = f_j(a)\end{aligned}$$

$\therefore (f_j f_1)(a) = (f_1 f_j)(a) = f_j(a)$, para todo $a \in G$.

(4) *Elemento inverso:* Sea f_j carácter de G. Debemos demostrar que existe $f_k \in \hat{G}$ tal que $f_j f_k = f_1$, sea $f_k = 1/f_j$, definido para $a \in G$ de la siguiente manera $f_k(a) = 1/f_k(a)$, el inverso de $f_j(a)$ en $\mathbb{C}^\times$, que es carácter de G. En efecto, para todo $a, b \in G$ tenemos que si $a = b$, entonces:

$$f_k(a) = \frac{1}{f_j(a)} = \frac{1}{f_j(b)} = f_k(b),$$

ya que f_j es función de G a $\mathbb{C}^\times$, esto demuestra que $f_k = 1/f_j$ define una función de G a $\mathbb{C}^\times$. Por otro lado:

$$f_k(ab) = 1/f_j(ab) = \frac{1}{f_j(a)}\frac{1}{f_j(b)} = f_k(a)f_k(b),$$

esto demuestra que $f_k = 1/f_j$ define un homomorfismo de G a $\mathbb{C}^\times$. De lo anterior $f_k = 1/f_j$ es un carácter de G, i.e., $f_k \in \hat{G}$. Notemos también que:

$$(f_j f_k)(a) = f_j(a)f_k(a) = f_j(a)\frac{1}{f_j(a)} = 1.$$

Para todo $a \in G$. Luego $f_k \in \hat{G}$, así definido es tal que $f_j f_k = f_1$, el carácter prinicipal.

(5) *Conmutatividad:* $(\hat{G}, \cdot)$ es grupo abeliano por ser $\mathbb{C}^\times$ abeliano con respecto al producto.

□

Observación B.7. *Para cada carácter f en un grupo G finito, tenemos $|f(a)| = 1$ (ver, Teorema B.2). Por lo tanto el recíproco $1/f(a)$ es igual al conjungado complejo $\overline{f(a)}$. Por lo tanto, la función $\overline{f}$ definida por $\overline{f}(a) = \overline{f(a)}$ es también un carácter de G. Más aún, tenemos*

$$\overline{f}(a) = \frac{1}{f(a)} = f(a^{-1})$$

para cada $a \in G$. Luego, para $f \in \hat{G}$, con G grupo finito, por Teorema B.6 parte (3), el inverso de f es $\overline{f}$.

Observación B.8. *Sea $k \in \mathbb{Z}_+$ y sea el grupo abeliano multiplicativo $(\mathbb{Z}/k\mathbb{Z})^\times$ para el cual $[a] \in (\mathbb{Z}/k\mathbb{Z})^\times$ si y solo si $m.c.d(a, k) = 1$. Si f es un carácter de $(\mathbb{Z}/k\mathbb{Z})^\times$, podemos tomar la extensión por 0, la cual denotamos por $\hat{f}$:*

$$(\mathbb{Z}/k\mathbb{Z})^\times \hookrightarrow (\mathbb{Z}/k\mathbb{Z}) \xrightarrow{\hat{f}} \mathbb{C}$$

tal que $\hat{f}(n) = f(n)$ si $n \in (\mathbb{Z}/k\mathbb{Z})^\times$ y $\hat{f}(n) = 0$, si este no es el caso. Por otro lado, si π es la proyección de $\mathbb{Z}$ sobre $\mathbb{Z}/k\mathbb{Z}$, tenemos:

$$\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/k\mathbb{Z} \xrightarrow{\hat{f}} \mathbb{C}$$

con lo cual al tomar $\chi_f = \hat{f} \circ \pi$ ésta define una función multiplicativa de $\mathbb{Z}$ a $\mathbb{C}$.

Definición B.9. ***Carácter de Dirichlet mód k.*** *Sea* $(\mathbb{Z}/k\mathbb{Z})^\times$*, al hacer corresponder cada carácter* f *de* $(\mathbb{Z}/k\mathbb{Z})^\times$ *a una función aritmética* $\chi = \chi_f : \mathbb{Z} \to \mathbb{C}$ *como sigue:*

$$\chi(n) = \begin{cases} f(n \text{ mód } k) & si \quad m.c.d(n,k) = 1, \\ 0 & si \quad m.c.d(n,k) > 1 \end{cases}$$

Definimos la función χ*, la cual es llamada carácter de Dirichlet módulo* $k \in \mathbb{Z}_+$*.*

Observación B.10. *El* ***carácter principal mód k*** χ_1 *es aquel con la propiedad* $\chi_1 : \mathbb{Z} \to \mathbb{C}$

$$\chi_1(n) = \begin{cases} 1 & si \quad m.c.d(n,k) = 1, \\ 0 & si \quad m.c.d(n,k) > 1 \end{cases}$$

Observación B.11. *Un carácter de Dirichlet* χ *puede tomar dos valores en el entero* $n = -1$*, estos son* $\chi(-1) = 1$ *ó* $\chi(-1) = -1$*, por lo tanto sea*

$$\delta_\chi = \begin{cases} 0 & si \quad \chi(-1) = 1, \\ 1 & si \quad \chi(-1) = -1. \end{cases}$$

Decimos que χ *es* ***par*** *si* $\delta_\chi = 0$ *e* ***impar*** *si* $\delta_\chi = 1$*.*

Teorema B.12. *Existen* $\varphi(k)$ *caracteres de Dirichlet módulo* $k \in \mathbb{Z}_+$*, donde* φ *es la función indicatriz de Euler, cada uno de los cuales es completamente multiplicativo y periódico con periodo* k*. Esto es, tenemos*

$$\chi(mn) = \chi(m)\chi(n) \quad \forall\ m, n \in \mathbb{Z}, \tag{B.2}$$

y

$$\chi(n+k) = \chi(n) \quad \forall\ n \in \mathbb{Z}. \tag{B.3}$$

Recíprocamente, si χ *es completamente multiplicativo y periódico con periodo* k*, y si* $\chi(n) = 0$ *para* $m.c.d(n,k) > 1$*, entonces* χ *es uno de los caracteres de Dirichlet módulo* k*.*

Demostración. Existen $\varphi(k)$ caracteres f para el grupo $(\mathbb{Z}/k\mathbb{Z})^\times$ por Teorema B.4, luego existen $\varphi(k)$ caracteres χ_f de Dirichlet módulo k. La propiedad multiplicativa (B.2) de χ_f se sigue de la propiedad multiplicativa de f cuando ambos m y n son primos relativos a k. Si alguno de los dos m ó n no es primo relativo a k entonces también mn, por tanto ambos lados de la igualdad en (B.2) son cero. La propiedad en (B.3) se sigue del hecho que $\chi_f(n) = f(n \text{ mód } k)$ y que $a \equiv b \pmod{k}$ implica que m.c.d(a,k) =m.c.d(b,k).

Para probar el recíproco notamos que la función f definida en el grupo $(\mathbb{Z}/k\mathbb{Z})^\times$ por la ecuación

$$f(n \text{ mód } k) = \chi(n) \quad \text{si} \quad \text{m.c.d}(n,k) = 1,$$

es un carácter de G, entonces χ es un carácter de Dirichlet.

□

Demostraremos a continuación propiedades básicas de los caracteres de Dirichlet.

Teorema B.13. *Sea χ carácter de Dirichlet mód k, entonces*

(i) Si $a \equiv 1$ (mód k), entonces $\chi(a) = 1$,

(ii) Si m.c.d$(a,k) = 1$, entonces $\chi(a)^{\varphi(k)} = 1$,

(iii)

$$\sum_{a \pmod{k}} \chi(a) = \begin{cases} \varphi(k) & si \quad \chi = \chi_1, \\ 0 & si \quad \chi \neq \chi_1. \end{cases}$$

Demostración. (i) Como χ es carácter de Dirichlet, entonces por propiedad multiplicativa B.2, $\chi(a) = \chi(a \cdot 1) = \chi(a)\chi(1)$. Si $a \equiv 1$ (mód k), entonces $\chi(a) \neq 0$, ya que m.c.d$(a,k) = 1$. Luego $\chi(1) = 1$, entonces por la periocidad B.3 tenemos que $\chi(a) = 1$.

(ii) Sea m.c.d$(a,k) = 1$, del teorema de Euler-Fermat tenemos $a^{\varphi(k)} \equiv 1$ (mód k). Por lo tanto

$$\chi(a)^{\varphi(k)} = \chi(a^{\varphi(k)}) = 1.$$

Por lo visto en (i).

(iii) Dado que $\varphi(k) = |(\mathbb{Z}/k\mathbb{Z})^\times|$, la afirmación se confirma si $\chi \neq \chi_1$. Si $\chi \neq \chi_1$, existe b tal que $\chi(b) \neq 0, 1$. Sea

$$S = \sum_{a \pmod{k}} \chi(a),$$

entonces

$$\chi(b)S = \sum_{a \pmod{k}} \chi(b)\chi(a) = \sum_{a \pmod{k}} \chi(ba) = S,$$

ya que ba recorre $(\mathbb{Z}/k\mathbb{Z})^\times$, por ser m.c.d$(b,k) = 1$, esto implica que $(1 - \chi(b))S = 0$ y como $1 - \chi(b) \neq 0$ entonces $S = 0$.

□

Definición B.14. ***Módulo Inductor.*** *Sea χ un carácter de Dirichlet módulo k y sea d un divisor positivo de k. El número d es llamado un módulo inductor para χ si se cumple la siguiente condición*

$$\chi(a) = 1 \quad \textit{siempre que} \quad m.c.d(a,k) = 1 \quad y \quad a \equiv 1 (\textit{mód } d) \tag{B.4}$$

Observación B.15. *Notemos que k mismo es un inductor para χ.*

Teorema B.16. *Sea χ un carácter de Dirichlet módulo k. Entonces 1 es un inductor para χ si y solamente si $\chi = \chi_1$ es el carácter principal.*

Demostración. Si $\chi = \chi_1$ entonces $\chi(a) = 1$ para todo $a \in \mathbb{Z}$ con m.c.d$(a, k) = 1$. Por otro lado, dado que $a \equiv 1$ (mód 1) el número 1 es un módulo inductor para χ_1. Recíprocamente, si 1 es un módulo inductor para χ entonces

$$\chi(a) = 1 \quad \text{para } a \text{ con m.c.d}(a, k) = 1 \text{ y } a \equiv 1(\text{mód } 1),$$

esto es, $\chi(a) = 1$ para todo $a \in \mathbb{Z}$ con m.c.d$(a, k) = 1$, i.e., $\chi = \chi_1$.

□

Definición B.17. ***Carácter Primitivo.*** *Un carácter de Dirichlet χ módulo k se dice* ***primitivo*** *módulo k si no posee un módulo inductor $d < k$. En otras palabras, χ es primitivo módulo k si y solo si para cada divisor d de k, $0 < d < k$, existe un entero $a \equiv 1$ (mód d) con m.c.d$(a, k) = 1$ tal que $\chi(a) \neq 1$.*

Observación B.18. *Si $k > 1$ el carácter principal χ_1 módulo k no es primitivo, ya que tiene a 1 como módulo inductor.*

Teorema B.19. *Cada carácter no principal χ módulo un primo p es un carácter primitivo módulo p.*

Demostración. Los únicos divisores positivos de p son 1 y p, luego estos son los únicos candidatos para ser módulos inductores. Pero si $\chi \neq \chi_1$ el divisor 1 no es un módulo inductor por teorema B.16. Por tanto χ es primitivo. □

El siguiente teorema se refiere a como se comporta χ en números que son congruentes módulo n un inductor.

Teorema B.20. *Sea χ un carácter de Dirichlet módulo k y asumamos que $d|k$, $d > 0$. Entonces d es un inductor para χ, si y solo si:*

$$\chi(a) = \chi(b) \text{ siempre que m.c.d}(a, k) = \text{m.c.d}(b, k) = 1 \text{ y } a \equiv b(\text{mód } d) \tag{B.5}$$

Demostración. Si (B.5) se cumple entonces d es un inductor ya que podemos escoger $b = 1$, por (B.4) se satisface la afirmación.

Recíprocamente, escojamos a y b tales que m.c.d(a, k) =m.c.d$(b, k) = 1$ y $a \equiv b$ (mód d), debemos mostrar que $\chi(a) = \chi(b)$. Sea a' el inverso de a mód k en $(\mathbb{Z}/k\mathbb{Z})^\times$, i.e., $aa' \equiv 1$ (mód k). Ahora $aa' \equiv 1$ (mód d) ya que $d|k$, en efecto, tenemos $k = dq_1$ luego $aa' - 1 = kq_0 = dq$, con $q = q_0q_1$. Por tanto $\chi(aa') = 1$ ya que d es inductor para χ. Pero $aa' \equiv ba' \equiv 1$ (mód d) ya que $a \equiv b$ (mód d), por tanto $\chi(aa') = \chi(ba')$ luego

$$\chi(a)\chi(a') = \chi(b)\chi(a'),$$

y como $\chi(a') \neq 0$ ya que $\chi(a)\chi(a') = 1$. Cancelando $\chi(a')$, vemos que $\chi(a) = \chi(b)$.

□

Observación B.21. *La ecuación (B.5) nos dice que χ es periódica módulo d en todos los enteros a primos relativos a k. Por tanto χ actúa mucho más como un carácter módulo d.*

En lo siguiente daremos dos equivalencias más para que un entero positivo sea inductor de un carácter de Dirichlet.

Teorema B.22. *Sea χ un carácter de Dirichlet módulo k y asumamos que $d|k$, con $d > 0$. Entonces las siguientes afirmaciones son equivalentes:*

(i) d es un inductor para χ,

(ii) Existe un carácter de Dirichlet ψ módulo d tal que:

$$\chi(n) = \psi(n)\chi_1(n) \quad \forall\ n \in \mathbb{Z}, \tag{B.6}$$

donde χ_1 es el carácter principal módulo k.

Demostración. Asumamos que (ii) se cumple. Elegimos n tal que m.c.d$(n, k) = 1$, $n \equiv 1$ (mód d). Entonces $\chi_1(n) = \psi(n) = 1$, luego $\chi(n) = 1$ y así d es un inductor para χ. Luego (ii) implica (i).

Asumamos ahora que (i) se cumple. Exhibimos un carácter de Dirichlet ψ módulo d para el cual (B.6) se cumple. Definimos $\psi(n)$ como sigue; si m.c.d$(n, d) > 1$ sea $\psi(n) = 0$. En este caso tenemos también m.c.d$(n, k) > 1$, en efecto, sea $d_0 =$m.c.d(n, d) entonces $d_0|n$ y $d_0|d$, como $d|k$ tenemos que $d_0|n$ y $d_0|k$, por tanto $d_0|$m.c.d(n, k). Así (B.6) se satisface ya que ambas partes son iguales a cero.

Ahora supongamos que m.c.d$(n, d) = 1$. Entonces existe m tal que $m \equiv n$ (mód d) con m.c.d$(m, k) = 1$. En efecto, sea $m = n + qd$ donde q es el producto de los primos que dividen a k pero no dividen a n. Si tales primos no existen, entonces para p primo con $p|k$ también $p|n$, por tanto $p \nmid d$, al hacer $m = n + d$, tenemos que $p \nmid m$, por tanto en este caso ningún primo que divide a k divide a m, i.e., m.c.d$(m, k) = 1$ y como $m - n = d$, entonces $m \equiv n$ (mód d). Por otro lado, si $q > 1$, tenemos que m.c.d$(m, d) = 1$, ya que:

$$1 = nx + dy = (m - qd)x + dy = mx + d(y - qx),$$

supongamos que m.c.d$(m, k) > 1$, luego existe un primo p con $p|k$ y $p|m$.

- Si $p|n$ entonces $p|(m - n) = qd$, como $p \nmid q$. Si no, por definición de q, p sería factor de n, entonces, por el Lema de Euclides $p|d$, luego $p|$m.c.d$(m, d) = 1$. Lo cual es absurdo.

- Si $p \nmid n$, entonces $p|q$ por definición de q, por lo tanto $p|(m - qd) = n$. Lo cual es contradictorio.

De lo anterior m.c.d$(m, k) = 1$ y como $m - n = qd$ entonces $m \equiv n$ (mód d).

Al tener el m, definimos $\psi(n) = \chi(m)$. El número $\psi(n)$ está bien definido ya que por Teorema B.20, χ toma los mismos valores en los números que son congruentes módulo d y que son primos relativos a k. Continuamos mostrando que ψ es en efecto, un carácter de Dirichlet módulo d.

(1) Sean $a, b \in \mathbb{Z}$ tales que $a \equiv b \pmod{d}$ y m.c.d$(a, d) =$ m.c.d$(b, d) = 1$, entonces existen $m_1, m_2 \in \mathbb{Z}$, tales que:

$$a \equiv m_1 \pmod{d} \quad \text{y} \quad b \equiv m_2 \pmod{d} \;\Rightarrow\; m_1 \equiv m_2 \pmod{d}$$

con m.c.d$(m_1, d) =$m.c.d$(m_2, d) = 1$, por tanto $\psi(a) = \chi(m_1) = \chi(m_2) = \psi(b)$.

(2) Sean $a, b \in \mathbb{Z}$. Demostremos que $\psi(ab) = \psi(a)\psi(b)$, al tomar m.c.d$(a, d) > 1$ ó m.c.d$(b, d) > 1$, tenemos que $\psi(a) = 0$ ó $\psi(b) = 0$, y además m.c.d$(ab, d) > 1$, por lo tanto $\psi(ab) = 0$, así $\psi(ab) = \psi(a)\psi(b)$.

Por otro lado, si m.c.d$(a, d) =$m.c.d$(b, d) = 1$, entonces:

$$\begin{aligned}
&\psi(ab) = \chi(m_0) \quad \text{para algún } m_0 \equiv ab \pmod{d} \text{ y m.c.d}(m_0, k) = 1,\\
&\psi(a) = \chi(m_1) \quad \text{para algún } m_1 \equiv a \pmod{d} \text{ y m.c.d}(m_1, k) = 1,\\
&\psi(b) = \chi(m_2) \quad \text{para algún } m_2 \equiv b \pmod{d} \text{ y m.c.d}(m_2, k) = 1.
\end{aligned}$$

Luego, $\chi(m_1 m_2) = \chi(m_1)\chi(m_2)$, y como $m_1 m_2 \equiv ab \pmod{d}$, esto implica que $m_0 \equiv m_1 m_2 \pmod{d}$, con lo cual $\chi(m_0) = \chi(m_1 m_2) = \chi(m_1)\chi(m_2)$. Por lo tanto $\psi(ab) = \psi(a)\psi(b)$.

Verificamos ahora que la ecuación (B.6), se cumple para todo n. Si m.c.d$(n, k) = 1$ entonces m.c.d$(n, d) = 1$, y así, $\psi(n) = \chi(m)$ para algún $m \equiv n \pmod{d}$. Luego por el Teorema B.20:

$$\chi(n) = \chi(m) = \psi(n) = \psi(n)\chi_1(n)$$

con χ_1 carácter principal mód k. Si m.c.d$(n, k) > 1$ entonces $\chi(n) = \chi_1(n) = 0$ y (B.6) se cumple.

□

Teorema B.23. *Sea χ carácter de Dirichlet módulo k. Sea $d|k$, $d > 0$. Entonces d es un inductor para χ, si solo si, χ se factoriza:*

$$(\mathbb{Z}/k\mathbb{Z})^\times \xrightarrow{\beta} (\mathbb{Z}/d\mathbb{Z})^\times \xrightarrow{\psi} \mathbb{C}, \tag{B.7}$$

con ψ carácter de Dirichlet módulo d y β definida tal que $(a \text{ mód } k) \mapsto (a \text{ mód } d)$.

Observación B.24. *En la afirmación anterior, estamos haciendo un poco de abuso de notación, ya que un carácter de Dirichlet esta definido sobre $\mathbb{Z}$, pero recordemos que estos quedan totalmente determinados según cierto módulo k, en particular por los caracteres del grupo $(\mathbb{Z}/k\mathbb{Z})^\times$, asi que podemos visualizarlos solo con los valores que toman en este grupo, y dando valor 0 a los $n \in \mathbb{Z}$ tales que m.c.d$(n, k) > 1$.*

Demostración. Supongamos que χ se factoriza como en (B.7), i.e., $\chi = \psi \circ \beta$, luego si $a \in \mathbb{Z}$ con m.c.d$(a, k) = 1$ y $a \equiv 1 \pmod{d}$, entonces $(a \text{ mód } k) \in (\mathbb{Z}/k\mathbb{Z})^\times$ y además $(a \text{ mód } d) = (1 \text{ mód } d)$ en $(\mathbb{Z}/d\mathbb{Z})^\times$, por tanto:

$$\chi(a) = \psi(\beta(a \text{ mód } k)) = \psi(a \text{ mód } d) = \psi(1 \text{ mód } d) = 1,$$

y por definición B.14, d es módulo inductor para χ.

Recíprocamente, si d es módulo inductor para χ, por Teorema B.22 parte (ii) existe un carácter de Dirichlet ψ módulo d tal que $\chi(n) = \psi(n)\chi_1(n)$ para todo $n \in \mathbb{Z}$, con χ_1 carácter principal módulo k. Demostremos que $\chi = \psi \circ \beta$, para hacer esto tomemos $(n \bmod k) \in (\mathbb{Z}/k\mathbb{Z})^\times$, entonces $(\psi \circ \beta)(n \bmod k) = \psi(n \bmod d) = \psi(n) = \psi(n)\chi_1(n)$, con χ_1 carácter principal módulo k (recuerde que estamos haciendo un poco de abuso de notación), por tanto $(\psi \circ \beta)(n) = \chi(n)$ para todo $n \in \mathbb{Z}$ con m.c.d$(n, k) = 1$.

□

Recordemos que si χ es un carácter de Dirichlet módulo k, este k es un módulo inductor para χ.

Definición B.25. *Sea χ un carácter de Dirichlet módulo k. El inductor d más chico para χ es llamado el* ***conductor*** *de χ.*

Teorema B.26. *Cada carácter de Dirichlet χ módulo k puede ser expresado como un producto,*

$$\chi(n) = \psi(n)\chi_1(n) \quad \forall\ n \in \mathbb{Z}, \tag{B.8}$$

donde χ_1 es el carácter principal módulo k y ψ es un carácter primitivo módulo el conductor de χ.

Demostración. Sea d el conductor de χ. Del Teorema B.22 sabemos que χ puede ser expresado como un producto de la forma (B.6), donde ψ es un carácter módulo d. Mostraremos que ψ es carácter primitivo módulo d.

Supongamos que no, si ψ no es primitivo módulo d existe un divisor q de d, $q < d$ que es módulo inductor para ψ. Probaremos que q el cual divide a k, es también módulo inductor para χ. Sea $n \equiv 1 \pmod q$, con m.c.d$(n, k) = 1$, entonces

$$\chi(n) = \psi(n)\chi_1(n) = \psi(n) = 1,$$

ya que m.c.d$(n, d) = 1$ y q es inductor para ψ. Por tanto, q es módulo inductor para χ, lo cual contradice que d sea el conductor de χ.

□

Observación B.27. *El Teorema B.26 junto al Teorema B.23 nos dice que si d es conductor de χ carácter de Dirichlet módulo k, existe ψ carácter primitivo módulo d tal que χ se factoriza*

$$(\mathbb{Z}/k\mathbb{Z})^\times \xrightarrow{\beta} (\mathbb{Z}/d\mathbb{Z})^\times \xrightarrow{\psi} \mathbb{C},$$

también, por Teorema B.26, si χ es carácter de Dirichlet primitivo módulo k, entonces χ no se puede factorizar de la forma anterior.

Observación B.28. *Por el Teorema B.26 todo carácter de Dirichlet χ, queda unívocamente determinado por un único carácter ψ, primitivo módulo f_χ el conductor de χ. En efecto, si ψ' es otro carácter de Dirichlet primitivo mód f_χ tal que satisface (B.8), tenemos que el siguiente diagrama conmuta:*

$$\begin{array}{ccc} (\mathbb{Z}/k\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/f_\chi\mathbb{Z})^\times \\ \downarrow & & \downarrow{\scriptstyle \psi'} \\ (\mathbb{Z}/f_\chi\mathbb{Z})^\times & \xrightarrow{\psi} & \mathbb{C}^\times \end{array}$$

como se satisface (B.8) para ψ y ψ', entonces $\psi \circ \pi = \chi = \psi' \circ \pi$, dónde π es la proyección natural de reducción módulo f_χ, la cual es sobreyectiva ya que $f_\chi | k$, entonces posee inversa a derecha, con lo cual concluimos que $\psi = \psi'$.

B.1. Grupo de Caracteres de Dirichlet Primitivos

Es conveniente por lo visto hasta el momento tomar a todos los caracteres que sean primitivos, ya que así se puede definir una multiplicación entre ellos sin ambigüedades.

Sean χ' y χ'' caracteres de Dirichlet primitivos con conductores d' y d'' respectivamente. Sea $m = d'd''$, definimos la función: $\gamma : \mathbb{Z} \to \mathbb{C}$ módulo m, tal que:

$$\gamma(n) = \begin{cases} \chi'(n)\chi''(n) & \text{si} \quad \text{m.c.d}(n,m) = 1, \\ 0 & \text{si} \quad \text{m.c.d}(n,m) > 1. \end{cases}$$

La función γ es un carácter de Dirichlet módulo m. En efecto:

(1) Sean $a, b \in \mathbb{Z}$ con m.c.d(a,m) =m.c.d$(b,m) = 1$ y $a \equiv b$(mód m), por tanto m.c.d$(a,d') =$ m.c.d$(b,d') = 1$ y, además, m.c.d$(a,d'') =$ m.c.d$(b,d'') = 1$, por otro lado también tenemos que $a \equiv b$(mód d') y $a \equiv b$(mód d''), todo lo anterior implica que:

$$\gamma(a) = \chi'(a)\chi''(a) = \chi'(b)\chi''(b) = \gamma(b).$$

(2) Sean $a, b \in \mathbb{Z}$ con m.c.d(a,m) =m.c.d$(b,m) = 1$, entonces:

$$\begin{aligned} \gamma(ab) &= \chi'(ab)\chi''(ab) \\ &= \chi'(a)\chi'(b)\chi''(a)\chi''(b) \\ &= \chi'(a)\chi''(a)\chi'(b)\chi''(b) = \gamma(a)\gamma(b). \end{aligned}$$

Si m.c.d$(a,m) > 1$ ó m.c.d$(b,m) > 1$ entonces m.c.d$(ab,m) > 1$, por tanto $\gamma(ab) = 0$, y por otro lado $\gamma(a) = 0$ o $\gamma(b) = 0$, asi $\gamma(ab) = \gamma(a)\gamma(b)$.

(3) $\gamma(n) \neq 0$ para todo $n \in \mathbb{Z}$ con m.c.d$(n,m) = 1$, ya que $\chi'(n) \neq 0$ y $\chi''(n) \neq 0$ en este caso.

Al tomar el conductor f_γ del carácter de Dirichlet γ definido anteriormente y reduciendolo a un carácter primitivo (el cual es único por Observación B.28), definimos la multiplicación $\chi' \cdot \chi''$ entre caracteres primitivos como el carácter primitivo asociado

a γ. Por otro lado, al tomar χ_1 como el carácter tal que es idénticamente 1 (carácter trivial) para todo $\mathbb{Z}$, este define un carácter de Dirichlet primitivo el cuál es el único con conductor 1.

Teorema B.29. *Con la multiplicación definida anteriormente, el conjunto de todos los caracteres primitivos de Dirichlet forman un grupo abeliano.*

Demostración. De la definición de la multiplicación sabemos que la operación es cerrada en el conjunto de los caracteres de Dirichlet primitivos:

(i) *Asociatividad*: Sean χ', χ'' y χ''' caracteres primitivos de Dirichlet, con conductores f_1, f_2 y f_3 respectivamente, queremos demostrar que:

$$(\chi'\chi'')\chi''' = \chi'(\chi''\chi'''),$$

sean f_γ y f_ψ los conductores de estos caracteres de la izquierda y derecha respectivamente de la identidad anterior, y sea $f_1 f_2 f_3 = f$, por lo tanto $f_\gamma | f$ y $f_\psi | f$. Notemos que si m.c.d$(n, f) = 1$, entonces:

$$((\chi'\chi'')\chi''')(n) = (\chi'(n)\chi''(n))\chi'''(n) = \chi'(n)(\chi''(n)\chi'''(n)) = (\chi'(\chi''\chi'''))(n).$$

De lo anterior:

$$\begin{array}{ccc} (\mathbb{Z}/f\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/f_\gamma\mathbb{Z})^\times \\ \downarrow & & \downarrow \\ (\mathbb{Z}/f_\psi\mathbb{Z})^\times & \longrightarrow & \mathbb{C}^\times \end{array}$$

el diagrama es conmutativo, ya que los caracteres primitivos $(\chi'\chi'')\chi'''$ y $\chi'(\chi''\chi''')$ inducen al carácter $\chi'\chi''\chi''' : (\mathbb{Z}/f\mathbb{Z}) \to \mathbb{C}^\times$ definido por:

$$(\chi'\chi''\chi''')(n) = \chi'(n)\chi''(n)\chi'''(n),$$

y por Observación B.28 estos caracteres son únicos, con lo cual se obtiene la identidad deseada.

(ii) *Conmutatividad*: Sean χ' y χ'' caracteres primitivos de Dirichlet con conductores f_1 y f_2 respectivamente, sea $f = f_1 f_2$, entonces si m.c.d$(n, f) = 1$, tenemos que

$$\gamma(n) = \chi'(n)\chi''(n) = \chi''(n)\chi'(n) = \psi(n)$$

luego, por definición de la multiplicación de caracteres, ambos son inducidos por el mismo carácter primitivo, i.e.

$$(\chi'\chi'')(n) = (\chi''\chi')(n) \quad \forall\ n \in \mathbb{Z}.$$

(iii) *Neutro*: Notemos que el elemento neutro es el carácter principal χ_1 definido como $\chi_1(n) = 1$ para todo $n \in \mathbb{Z}$. En efecto, para χ carácter primitivo con conductor f, tenemos que si m.c.d$(n, f) = 1$

$$\gamma(n) = \chi(n)\chi_1(n) = \chi(n),$$

al tomar el carácter primitivo asociado a γ, entonces $\chi\chi_1 = \chi$.

(iv) *Inverso*: El elemento inverso de χ es el carácter $\overline{\chi}$ el cual es el mapeo del conjugado complejo de χ, i.e., $\overline{\chi}(n) = \overline{\chi(n)}$, $n \in \mathbb{Z}$.

□

Apéndice C

Números p-ádicos

Kurt Hensel introdujo los números p-ádicos en 1897 como series de potencias con respecto al primo p, usando la analogía entre el anillo de enteros $\mathbb{Z}$ y su campo de cocientes $\mathbb{Q}$ y el anillo de polinomios $\mathbb{C}[X]$ y su campo de cocientes $\mathbb{C}(X)$. En este apéndice damos aspectos básicos sobre el campo de los números p-ádicos, campo en el cual van a estar definidas las funciones L p-ádicas, tema principal de esta tesina. Para un tratamiento más profundo del campo p-ádico (ver [11]).

Definición C.1. *Sea $\mathbb{F}$ un campo. Una norma (o valor absoluto) en $\mathbb{F}$ es una función $|\cdot| : \mathbb{F} \to \mathbb{R}_+$, tal que*

(i) $|x| = 0$ *si y solo si* $x = 0$,

(ii) $|xy| = |x||y|$, *para* $x, y \in \mathbb{F}$,

(iii) $|x + y| \leq |x| + |y|$, *para* $x, y \in \mathbb{F}$ *(Desigualdad Triangular).*

Definición C.2. *Una norma $|\cdot|$ es llamada no arquimediana (ó ultramétrica), si además satisface*

(iv) $|x + y| \leq máx\{|x|, |y|\}$, *para* $x, y \in \mathbb{F}$.

Observación C.3. *Notemos que* $|x+y| \leq máx\,\{|x|, |y|\} \leq |x|+|y|$, *i.e., (iv)* $\Longrightarrow$ *(iii).*

Observación C.4. *Podemos siempre definir la norma trivial en el campo $\mathbb{F}$ como*

$$|x| = \begin{cases} 1 & si \quad x \neq 0, \\ 0 & si \quad x = 0. \end{cases}$$

Aunque usualmente no se estudia este caso.

El valor absoluto usual el cual notaremos por $|\cdot|_\infty$ es una norma en $\mathbb{Q}$ y su métrica correspondiente es la función distancia usual, cuya completación nos da el cuerpo de los números reales $\mathbb{R}$. Por otro lado, podemos construir otras normas en $\mathbb{Q}$, que dependan de un primo p dado.

Primero, damos el concepto de valuación p-ádica y definimos el anillo $\mathbb{Z}_p$ de los enteros p-ádicos.

Definición C.5. *Sea p primo, y sea $a \in \mathbb{Z} - \{0\}$, luego $\nu_p(a)$ es el exponente de p en la factorización de a como producto de primos, es decir:*

$$a = p^{\nu_p(a)}b, \quad donde \quad p \nmid b,$$

$\nu_p(a)$ es la valuación p-ádica de a. Definimos $\nu_p(0) = +\infty$.

Podemos extender esta definición a los racionales de la siguiente manera, si $a/a' \in \mathbb{Q}$ con $m.c.d(a, a') = 1$, $a' > 0$, definimos $\nu_p(a/a') = \nu_p(a) - \nu_p(a')$. Entonces, el mapeo $\nu_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ es la valuación p-ádica de $\mathbb{Q}$.

Observación C.6. *Para cualquier $x \in \mathbb{Q}$, el valor de $\nu_p(x)$ no depende de su representación como cociente de dos enteros. En otras palabras, si $a/b = c/d$, entonces $\nu_p(a) - \nu_p(b) = \nu_p(c) - \nu_p(d)$, en efecto, tenemos que $ac = bd$ luego $\nu_p(ac) = \nu_p(bd)$, por teorema fundamental de la aritmética deducimos que*

$$\nu_p(a) + \nu_p(c) = \nu_p(b) + \nu_p(d),$$

donde se deduce el resultado.

La valuación p-ádica cumple las siguientes propiedades básicas (ver [11], cap. 2.)

Lema C.7. *Para todo a y $b \in \mathbb{Q}$, tenemos*

(i) $\nu_p(ab) = \nu_p(a) + \nu_p(b)$,

(ii) $\nu_p(a + b) \geq \min\{\nu_p(a), \nu_p(b)\}$,

(iii) Si $\nu_p(a) < \nu_p(b_1), \nu_p(b_2), ..., \nu_p(b_k)$, entonces $\nu_p(a + b_1 + \cdots + b_k) = \nu_p(a)$, con $b_i \in \mathbb{Q}$.

Observación C.8. *Si $\nu_p(x) = e \geq 1$, decimos que p^e es la potencia exacta de p que divide a x, escribimos $p^e \parallel x$.*

Más aún, si $x \in \mathbb{Q}^\times$, la valuación p-ádica es determinada por la fórmula

$$x = p^{\nu_p(x)} \cdot \frac{a}{b}, \quad p \nmid ab.$$

Lema C.9. *Sea $n = n_0 + n_1 p + n_2 p^2 + \cdots + n_r p^r$ representación de un entero $n \geq 1$ en base p-primo. Entonces, tenemos las siguientes afirmaciones acerca de las valuaciones p-ádicas.*

(i) La valuación p-ádica de $n!$ es

$$\nu_p(n!) = \sum_{k \geq 1} \left[\frac{n}{p^k} \right] = \frac{n - (n_0 + n_1 + \cdots + n_r)}{p - 1},$$

(ii) La valuación p-ádica del coeficiente binomial $\binom{n}{k}$ *es la suma de las "transferencias"que ocurren en la suma de* k *y* $n-k$.

(iii) La valuación p-ádica del coeficiente binomial $\binom{p^n}{k}$ *es igual a* $n-\nu_p(k)$, *para* $k \geq 1$.

Demostración. (i) Como $n = n_0 + n_1 p + \cdots + n_r p^r$. Tenemos $[n/p^k]$ enteros $m \leq n$ divisibles por p^k, en efecto, sea j el mayor entero tal que $jp^k \leq n$. De manera que, j es el número de elementos en $\{1, 2, \cdots, n\}$ que son divisibles por p^k.

$$\implies j \leq \frac{n}{p^k} < j+1 \quad \therefore \quad j = \left[\frac{n}{p^k}\right],$$

luego existen $[n/p^k] - [n/p^{k+1}]$ enteros $m \leq n$ de valuación p-ádica igual a k. Se sigue que:

$$\nu_p(n!) = \sum_{k\geq 1} k\left(\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right]\right) = \sum_{k\geq 1}\left[\frac{n}{p^k}\right].$$

Usando el hecho que

$$\left[\frac{n}{p^k}\right] = \sum_{i\geq k} n_i p^{i-k},$$

entonces

$$\begin{aligned}
\left[\frac{n}{p}\right] &= n_r p^{r-1} + n_{r-1}p^{r-2} + \cdots + n_1,\\
\left[\frac{n}{p^2}\right] &= n_r p^{r-2} + n_{r-1}p^{r-3} + \cdots + n_2,\\
&\vdots\\
\left[\frac{n}{p^r}\right] &= n_r.
\end{aligned}$$

Por lo tanto,

$$\nu_p(n!) = n_r(1 + \cdots + p^{r-2} + p^{r-1}) + n_{r-1}(1 + \cdots + p^{r-2}) + \cdots + n_1,$$

tenemos que

$$\begin{aligned}
\nu_p(n!) &= n_1 + n_2(1+p) + n_3(1+p+p^2) + \cdots + n_r(1 + \cdots + p^{r-1})\\
&= \frac{1}{p-1}[n_1 p + n_2 p^2 + \cdots + n_r p^r - (n_1 + \cdots + n_r)]\\
&= \frac{n - (n_0 + n_1 + \cdots + n_r)}{p-1}.
\end{aligned}$$

(ii) Sean $k = k_0 + k_1 p + \cdots + k_r p^r$ y $l = n - k = l_0 + l_1 p + \cdots + l_r p^r$. Con el algoritmo de la suma p-ádica

$$\begin{aligned}
&k_0 + l_0 = n_0 + \delta_0 p && \text{con} \quad \delta_0 \in \{0,1\},\\
&k_1 + l_1 + \delta_0 = n_1 + \delta_1 p && \text{con} \quad \delta_1 \in \{0,1\},\\
&\quad\vdots && \qquad\vdots\\
&k_r + l_r + \delta_{r-1} = n_r + \delta_r p && \text{con} \quad \delta_r \in \{0,1\},\\
&n_{r+1} = \delta_r.
\end{aligned}$$

donde los $\delta_0, \delta_1, \cdots, \delta_r$ son las "transferencias". Entonces por *(i)* tenemos

$$\begin{aligned}
\nu_p\left(\binom{n}{k}\right) &= \nu_p\left(\frac{n!}{k!\cdot l!}\right) \\
&= \nu_p(n!) - \nu_p(k!) - \nu_p(l!) \\
&= [n - (n_0 + n_1 + \cdots + n_{r+1}) - k + (k_0 + k_1 + \cdots + k_r) - l + (l_0 + l_1 + \cdots + l_r)] \cdot \frac{1}{p-1} \\
&= [(k_0 + l_0 - n_0) + (k_1 + l_1 - n_1) + \cdots + (k_r + l_r - n_r) - n_{r+1}] \cdot \frac{1}{p-1} \\
&= [(\delta_0 + \delta_1 + \cdots + \delta_r)p - (\delta_0 + \delta_1 + \cdots + \delta_r)] \cdot \frac{1}{p-1} \\
&= \delta_0 + \delta_1 + \cdots + \delta_r.
\end{aligned}$$

(iii) Sea $1 \leq j < p^n$, tenemos que $\nu_p(p^n - j) = \nu_p(j)$, en efecto, sea $\nu_p(p^n - j) = m$, entonces $p^n - j = p^m q$, con $p \nmid q$, por tanto $j = p^m(p^{n-m} - q)$, de donde se sigue que $\nu_p(j) = m$. Entonces:

$$\begin{aligned}
\nu_p\left(k!\binom{p^n}{k}\right) &= \nu_p(k!) + \nu_p\left(\binom{p^n}{k}\right) \\
&= \nu_p(p^n(p^n-1)(p^n-2)\cdots(p^n-(k-1))) \\
&= n + \sum_{j=1}^{k-1} \nu_p(p^n - j) \\
&= n + \sum_{j=1}^{k-1} \nu_p(j) \\
&= n + \nu_p((k-1)!).
\end{aligned}$$

$$\begin{aligned}
\therefore \quad \nu_p\left(\binom{p^n}{k}\right) &= n + \nu_p((k-1)!) - \nu_p(k!) \\
&= n - \nu_p(k).
\end{aligned}$$

□

Definición C.10. *Para $x \in \mathbb{Q}$, definimos la norma p-ádica de x, de la siguiente manera*

$$|x|_p = \begin{cases} p^{-\nu_p(x)} & si \quad x \neq 0 \\ 0 & si \quad x = 0. \end{cases}$$

Observación C.11. *La demostración que efectivamente $|\cdot|_p$ define una norma en $\mathbb{Q}$, más aún, una norma no arquimediana, se sigue del Lema C.7.*

Teorema C.12. ***Ostrowski-1916.*** *Cada norma no trivial en $\mathbb{Q}$ es equivalente a una de las normas p-ádicas $|\cdot|_p$, para algún p-primo, o a la norma $|\cdot|_\infty$.*

Demostración. Ver [11], cap. 3, Teorema 3.1.3.

□

Observación C.13. *El Teorema C.12 de Ostrowski, caracteriza todos los valores absolutos que se pueden definir sobre $\mathbb{Q}$, en esencia, existen solo de dos tipos. Por otro lado, es bien sabido que $(\mathbb{Q}, |\cdot|_\infty)$, es un espacio no completo, cuya completación, ya sea por cortaduras de Dedekind o succeciones de Cauchy origina el campo de los números reales $(\mathbb{R}, |\cdot|_\infty)$. Esto mismo ocurre para el caso no arquimediano.*

Observación C.14. *Notemos que si en $\mathbb{Q}$ trabajamos con la norma trivial, entonces sería completo, ya que si $(a_n)_n$ es una sucesión de Cauchy en $\mathbb{Q}$, para $0 < \varepsilon < 1$, existe $N \in \mathbb{N}$, tal que:*

$$|a_n - a_m| < \varepsilon < 1 \text{ siempre que } n, m \geq N$$

y como esta es la norma trivial, entonces $|a_n - a_m| = 0$, con lo cual, $a_n = a_m$ siempre que $n, m \geq N$, i.e., la sucesión se estaciona a partir de un término fijo, por lo tanto es sucesión convergente.

Lema C.15. *El campo $\mathbb{Q}$ de los números racionales no es completo respecto a cualquiera de sus normas no triviales.*

Demostración. Ver [11], cap. 3, Lema 3.2.2. □

Observación C.16. *Procediendo de manera clásica se puede obtener la completación de $(\mathbb{Q}, |\cdot|_p)$ vía sucesiones de Cauchy. Tenemos entonces el siguiente teorema*

Teorema C.17. *Para cada primo $p \in \mathbb{Z}_+$ existe un campo $\mathbb{Q}_p$ con norma no arquimediana $|\cdot|_p$, tal que:*

(i) Existe una inclusión $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, y la norma inducida por $|\cdot|_p$ en $\mathbb{Q}$ vía esta inclusión es el valor absoluto p-ádico.

(ii) La imagen de $\mathbb{Q}$ bajo esta inclusión es densa en $\mathbb{Q}_p$ (respecto al valor absoluto $|\cdot|_p$).

(iii) $\mathbb{Q}_p$ es completo respecto al valor absoluto $|\cdot|_p$.

El campo $\mathbb{Q}_p$ que satisface (i), (ii) y (iii) es único salvo isometrías.

Demostración. Ver [11], cap. 3, Teorema 3.2.13. □

Observación C.18. *Tanto como la norma p-ádica se puede extender de $\mathbb{Q}$ a $\mathbb{Q}_p$ bajo la inclusión mencionada anteriormente, lo mismo ocurre con la valuación p-ádica.*

Lema C.19. *Para cada $x \in \mathbb{Q}_p$, $x \neq 0$, existe un entero $\nu_p(x)$ tal que $|x|_p = p^{-\nu_p(x)}$.*

Demostración. Por Teorema C.17, $\mathbb{Q}$ es denso en $\mathbb{Q}_p$, luego, para $x \in \mathbb{Q}_p$ con $x \neq 0$, existe $(x_n)_n$ sucesión en $\mathbb{Q}$ tal que $x_n \to x$ en norma p-ádica. Por tanto, $(x_n)_n$ es sucesión de Cauchy que no converge a cero. De lo anterior, existen $c > 0$ y $N_1 \in \mathbb{Z}$, tal que

$$n \geq N_1 \implies |x_n|_p \geq c > 0.$$

Por otro lado, dado que $(x_n)_n$ es sucesión de Cauchy, existe $N_2 \in \mathbb{Z}$ para el cual

$$n, m \geq N_2 \implies |x_n - x_m|_p < c.$$

Sea $N = \text{máx}\{N_1, N_2\}$, entonces

$$n, m \geq N \implies |x_n - x_m|_p \leq \text{máx } \{|x_n|_p, |x_m|_p\},$$

por lo tanto, para $n, m \geq N$

$$|x_n|_p \leq \text{máx } \{|x_n - x_m|_p, |x_m|_p\} = |x_m|_p,$$

con lo cual $|x_n|_p \leq |x_m|_p$ si $n, m \geq N$, análogamente tenemos $|x_m|_p \leq |x_n|_p$, y por tanto $|x_n|_p = |x_m|_p = p^{-k}$, para todo $n, m \geq N$ y algún $k \in \mathbb{Z}$. Definamos $k = \nu_p(x)$, y dado que $x_n \to x$, entonces $|x_n|_p \to |x|_p$, y así $|x|_p = p^{-\nu_p(x)}$. □

Observación C.20. *Terminamos de realizar la extensión de ν_p a todo $\mathbb{Q}_p$, tomando $\nu_p(0) = +\infty$.*

Definición C.21. *El anillo de los enteros p-ádicos es el anillo de valuación*

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : \ |x|_p \leq 1\}.$$

Definición C.22. *Decimos que $r = a/a' \in \mathbb{Q}$ es p-entero si $\nu_p(r) \geq 0$. Claramente cada $a \in \mathbb{Z}$ es p-entero ($\forall$ p-primo). Notamos al conjunto de los racionales p-enteros por $\mathbb{Z}_{(p)}$ el cual es subanillo de $\mathbb{Q}$.*

Teorema C.23. *El anillo $\mathbb{Z}_p$ de los enteros p-ádicos es un anillo local cuyo ideal maximal es el ideal principal $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : \ |x|_p < 1\}$. Más aún,*

(i) $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\}$.

(ii) La inclusión $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ tiene imagen densa. En particular, dado $x \in \mathbb{Z}_p$ y $n \geq 1$, existe $\alpha \in \mathbb{Z}$, $0 \leq \alpha < p^n$, tal que $|x - \alpha|_p \leq p^{-n}$. El entero α con estas propiedades es único.

(iii) Para $x \in \mathbb{Z}_p$, existe una sucesión de Cauchy $(\alpha_n)_n$ de enteros que converge a x, del siguiente tipo:

- $0 \leq \alpha_n < p^n$
- *Para cada n tenemos $\alpha_n \equiv \alpha_{n-1}$ (mód p^{n-1}).*

La sucesión $(\alpha_n)_n$ con estas propiedades es única.

Demostración. Para una demostración completa (ver [11], cap. 3, Proposición 3.3.4). Solo demostraremos (i).

Explícitamente, necesitamos probar que $r \in \mathbb{Z}_{(p)}$ si y solo si $r = 0$ o $r = a/b$ con $b \neq 0$ y $p \nmid b$. En efecto, sea $r = a/b \in \mathbb{Z}_{(p)}$ con m.c.d$(a, b) = 1$, luego $\nu_p(r) \geq 0$, de manera que $\nu_p(a) \geq \nu_p(b)$, como $r \in \mathbb{Q}$, $b \neq 0$. Si $\nu_p(b) > 0$ entonces $p|b$ y $p|a$ y así m.c.d$(a, b) > 1$, lo cual es contradictorio, así $\nu_p(b) = 0$, esto es $p \nmid b$. Recíprocamente, si $r = 0$, entonces $\nu_p(r) = \infty > 0$, luego $r \in \mathbb{Z}_p$, por otro lado, si $r = a/b$ con $b \neq 0$ y $p \nmid b$, con lo cual $\nu_p(b) = 0$, entonces $\nu_p(r) = \nu_p(a) \geq 0$.

□

Observación C.24. *Un número racional r es entero si y solo si r es p-entero para cada primo p, i.e., Sea $r \in \mathbb{Q}$, entonces $r \in \mathbb{Z} \iff r \in \mathbb{Z}_{(p)}\ \forall$ p-primo. En efecto, la condición suficiente es clara, recíprocamente si $r = a/b \in \mathbb{Q}$ tal que $r \in \mathbb{Z}_{(p)}$ para todo p-primo, entonces por lema anterior tenemos dos opciones, si $r = 0$, entonces $r \in \mathbb{Z}$, por otro lado, $p \nmid b$, para todo p-primo, por teorema fundamental de la aritmética $b = 1$ ó $b = -1$ necesariamente, por lo tanto $r = a \in \mathbb{Z}$.*

Observación C.25. *Al ser $\mathbb{Z}_p$ la bola cerrada unitaria en $\mathbb{Q}_p$, una pregunta natural sería. ¿Es $\mathbb{Z}_p$ compacto? respuesta que es afirmativa (ver [11], cap. 3. Corolario 3.3.8.)*

A continuación, definimos una relación de equivalencia en $\mathbb{Q}_p$, que generaliza la relación de congruencia módulo p en $\mathbb{Z}$.

Lema C.26. *Sean $r, s \in \mathbb{Q}_p$, $e \in \mathbb{Z}_+$ entero fijo. Entonces $r \equiv s$ (mód p^e) si y solo si $\nu_p(r - s) \geq e$. Define una relación de equivalencia en $\mathbb{Q}_p$.*

Demostración. En efecto:

(i) *Reflexiva:* Sea $r \in \mathbb{Q}_p$, luego $r - r = 0$, y dado que $\nu_p(0) = +\infty$, entonces $\nu_p(r - r) > e$, i.e., $r \equiv r \pmod{p^e}$.

(ii) *Simétrica:* Sean $r, s \in \mathbb{Q}_p$ tales que $r \equiv s \pmod{p^e}$, esto es, $\nu_p(r - s) \geq e$. Como

$$\nu_p(r - s) = \nu_p((-1)(s - r)) = \nu_p(-1) + \nu_p(s - r) = \nu_p(s - r).$$

Entonces $\nu_p(s - r) \geq e$, por tanto $s \equiv r \pmod{p^e}$.

(iii) *Transitiva:* Sean r, s y t elementos en $\mathbb{Q}_p$, tales que $r \equiv s \pmod{p^e}$ y $s \equiv t \pmod{p^e}$, por tanto $\nu_p(r - s) \geq e$ y $\nu_p(s - t) \geq e$, luego

$$\nu_p(r - t) = \nu_p((r - s) + (s - t)) \geq \min\{\nu_p(r - s), \nu_p(s - t)\} \geq e,$$

por tanto $r \equiv t \pmod{p^e}$.

□

Lema C.27. ***Lema de Hensel****. Sea $f(x) \in \mathbb{Z}_p[X]$ polinomio con coeficientes en $\mathbb{Z}_p$. Denotamos por $f'(X)$ a su derivada formal. Si la congruencia $f(X) \equiv 0$ (mód p) tiene una solución a_1 tal que $f'(a_1) \not\equiv 0$ (mód p) entonces existe un único entero p-ádico a tal que $f(a) = 0$ y $a \equiv a_1$ (mód p).*

Demostración. Ver Murty [18], cap. 4, Teorema 4.1 □

Observación C.28. *Una consecuencia importante del Lema de Hensel es que resolver ecuaciones en $\mathbb{Z}_p$ es equivalente a resolver ecuaciones mód p^n para todo $n \in \mathbb{Z}_+$. Por ende, al tener los mapeos naturales (Proyecciones)*

$$\mathbb{Z}/p^{n+1}\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z},$$

podemos ver a $\mathbb{Z}_p$ como el límite inverso (o proyectivo) del sistema $\{\mathbb{Z}/p^n\mathbb{Z}\}_{n\in\mathbb{N}}$, i.e.,

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}.$$

Observación C.29. *También como consecuencia del Lema de Hensel, $\mathbb{Q}_p$ no es algebraicamente cerrado. Ya que con el se pueden caracterizar las raíces m-ésimas de la unidad que pertenecen a $\mathbb{Q}_p$ (Ver [11], cap. 3, Proposición 3.4.2.). Al extender la norma $|\cdot|_p$ a la cerradura algebraica $\overline{\mathbb{Q}}_p$ (ver Murty [18], cap. 4, pág 49-50), notamos que $\overline{\mathbb{Q}}_p$ pierde la completitud con respecto a la norma p-ádica (ver Murty [18], cap. 4, Teorema 4.4.)*

Al tomar $\mathbb{C}_p$, la completación vía suceciones de Cauchy de $(\overline{\mathbb{Q}}_p, |\cdot|_p)$, obtenemos el análogo p-ádico de los números complejos con la norma usual, ya que:

Teorema C.30. *$\mathbb{C}_p$ es algebraicamente cerrado y completo.*

Demostración. Ver Murty [18], cap. 4, Teorema 4.6. □

Epílogo

La teoría de números ocupa entre los matemáticos un estatus de grandeza justificado. No en vano Carl Gauss la llamaba "la reina de las matemáticas", no podría ser de otra manera, ya que es un área presente desde el nacimiento de esta ciencia formal y que a través de los años ha proporcionado una gran cantidad de retos a la comunidad matemática. Los matemáticos poco a poco han ido resolviendo estos problemas y al mismo tiempo han presenciado en el camino cómo el edificio matemático creció junto a ellos.

Hablar de matemáticas, específicamente de investigación en matemáticas como aprendí en estos dos años de maestría en el CIMAT, se refiere a las técnicas que se usan en el intento de resolver un problema en cuestión, la generalización de alguna teoría, la aplicación de un concepto en algún caso concreto y en particular en el desarrollo de ideas que puedan brindar un fundamento sólido para algún área de investigación. Esta tesina engloba ese último concepto, pues en su elaboración estudié las técnicas que se desarrollaron en el siglo XIX y XX en la construcción de las herramientas básicas de la teoría analítica de números que busca como objetivo final, entender el comportamiento de los objetos ariméticos, que surgen en la investigación del anillo de los números enteros.

A partir de aquí el objetivo a futuro será completar el camino iniciado en esta tesina, el cual es, entender la construcción algebraica hecha por Kenkichi Iwasawa en los años sesenta de las funciones L p-ádicas que inició la investigación de lo que hoy llamamamos Teoría de Iwasawa, cuya conjetura principal para $\mathbb{Q}$ fue demostrada en 1984 por Andrew Wiles y Barry Mazur y en donde se demuestra que los dos métodos de construcción, tanto el analítico vía interpolación como el algebraico definen el mismo objeto, que a su vez inicia una serie de generalizaciones que están presentes en la ivestigación moderna de la teoría números.

Bibliografía

[1] Apostol, T.M. *Introduction to Analytic Number Theory*. Springer-Verlag New York Inc, 1976.

[2] Arakawa, T., Ibukiyama, T. and Kaneko, M. *Bernoulli Numbers and Zeta Functions*, SMM, Springer-Verlag., Japan, 2014.

[3] Bernoulli, J. *Ars conjectandi, opus posthumum*. Accedit Tractatus de seriebus infinitis, et epistola gallicé scripta de ludo pilae reticularis, Basel: Thurneysen Brothers, OCLC 7073795, (1973).

[4] Bojanic, R. *A simple proof of Mahler's theorem on approximation of continuous functions of a p-adic variable by polynomials*, J. Number Theory, **6** (1974)pp.412-415.

[5] Clark, W.E. *The Aryabhatiya of Aryabhata*, University of Chicago Press, Chicago, Illinois, 1930.

[6] Clausen, T. *"Theorem"*, Astronomische Nachrichten, 17 (22): 351–352, (1840).

[7] Diamond, J. *On the values of p-adic L-functions at positive integers*, Acta Arith. 35 (1979), 223-237.

[8] Eissa, H. *Double Sequences and Double Series*, vol. 14, 2005.

[9] Folland, G.B. *Real Analysis: modern techniques and their applications*. John Wiley & Sons, Inc, 1999.

[10] Fröhlich, A. & Taylor, M.J. *Algebraic Number Theory*. Cambridge University Press, 1991.

[11] Gouvea, F.Q. *p-adic Numbers An Introduction*. Universitext, Springer-Verlag, 2003.

[12] Hideo, I. *Values of p-adic L-functions at positive integers and p-adic log multiple gamma functions*, Tohoku Math. J. 45 (1993), 505-510.

[13] Iwasawa, K. *On p-adic L-functions*, Ann. Math. 89 (1969), 198-205.

[14] Iwasawa, K. *Lectures on p-adic L-Functions*. Princeton University Press, 1972.

[15] Koblitz, N. *p-adic Numbers, p-adic Analysis and Zeta Functions*, Vol. 58, Springer-Verlag, 1977.

[16] Kubota, T. und Leopoldt, H.W. *Eine p-adische Theorie der Zetawerte. I. Einführung der p-adischen Dirichletschen L-funktionen.*, I, Jour, Reine und angew. Math., 214/215 (1964), 328-339.

[17] Mahler, K. *"An interpolation series for continuous functions of a p-adic variable"*, Journal für die reine und angewandte Mathematik, 199: 23–34, 1958.

[18] Murty, M.R. *Introduction to p-adic Analytic Number Theory.* AMS/IP studies in advanced mathematics, 2002.

[19] Murty, M. R. and Sinha, K. *Multiple Hurwitz Zeta Functions*, in Multiple Dirichlet series, automorphic forms, and analytic number theory, Proc. Symp. Pure Math., 75 (2006), 135-156.

[20] Neukirch, J. *Algebraic Number Theory.* Springer-Verlag Berlin Heidelberg New York, 1999.

[21] Robert, A. *A Course in p-adic Analysis*, GTM, Vol.198, Springer-Verlag, 2000.

[22] Srivastava, H.M. and Manocha, H.L. *A Treatise on Generating Functions.* Ellis Horwood Limited, 1984.

[23] Stein, E.M. and Shakarchi, R. *Complex Analysis.* Princeton University Press, 2003.

[24] Tao, T. *An Introduction to Measure Theory.* AMS Graduate Studies in Mathematics, 2011.

[25] von Staudt, K. *"Beweis eines Lehrsatzes, die Bernoullischen Zahlen betreffend"*, Journal für die Reine und Angewandte Mathematik, 21: 372–374, (1840).

[26] Weierstrass, K. *Über die analytische Darstellbarkeit sogenannter willkürlicher Functionen einer reellen Veränderlichen*, Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin, 1885 (II).

[27] Washington, L.C. *Introduction to Cyclotomic Fields.* GTM. Springer-Verlag, New York Inc. 1982.