INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE FÍSICA Y MATEMÁTICAS

Números de Bernoulli: Un estudio sobre su importancia, consecuencias y algunas aplicaciones en la Teoría de Números

T E S I S

QUE PARA OBTENER EL TÍTULO DE
LICENCIADO EN FÍSICA Y MATEMÁTICAS
CON ESPECIALIDAD EN MATEMÁTICAS

P R E S E N T A

DAVID JOSÉ FERNÁNDEZ BRETÓN

ASESOR DE TESIS
DR. PABLO LAM ESTRADA

MÉXICO, D. F. **29 DE MAYO DE 2008**

A mis padres David y Nora,

a mi hermano Maximiliano,

a mi prometida Rocio,

y a mi abuelito adoptivo, Bogdan.

Agradecimientos

En primer lugar, deseo agradecer a mis padres, David y Nora, que me soportaron tanto moral como económicamente durante todos mis estudios, y sin los cuales difícilmente habría llegado a buen término el presente trabajo; además de que fueron ellos quienes por primera vez me mostraron la majestuosa belleza de la matemática. También agradezco enormemente a mi hermano Maximiliano, quien en repetidas ocasiones soportó mis aburridos temas de conversación matemáticos. Cabe agradecer también a mi abuelo adoptivo, Bogdan, de quien aprendí a ser obsesivo, en justa medida, con el trabajo. Y desde luego, agradezco también a mi prometida Rocio, quien me acompañó, apoyó y soportó durante la entera realización del presente trabajo, lo cual no es poco, ni en modo alguno fácil.

Es también necesario recalcar mi agradecimiento a la biblioteca Jerzy Plebañsky del Centro de Investigación y Estudios Avanzados, que fue la que me proporcionó gran parte de los libros y artículos utilizados en el presente trabajo. Asimismo, agradezco enormemente a mi asesor de tesis, el dr. Pablo Lam Estrada, por orientarme y apoyarme durante el desarrollo de la presente tesis, así como por sus estimulantes cursos que me introdujeron en el maravilloso mundo del álgebra. Y, desde luego, a mis sinodales, la dra. Myriam Maldonado, el mtro. Rubén Mancio, el mtro. Abelardo Santaella y el lic. Manuel Robles, por tomarse el trabajo y el tiempo de leer esta tesis, corregirla, y presenciar el examen profesional.

Por último, deseo agradecer a todos mis compañeros y profesores de la Escuela Superior de Física y Matemáticas, quienes permitieron mi desarrollo en un entorno intelectualmente estimulante que me permitió cultivar mi gusto por las “ciencias exactas”. Todos ellos han desempeñado un papel crucial en mi desarrollo como estudiante, y es difícil imaginar la realización del presente trabajo sin ellos a mi alrededor.

Índice general

Introducción

El portentoso matemático alemán del siglo XVIII, Carl Friedrich Gauss, afirmó en cierta ocasión que "La Matemática es la reina de las Ciencias, y la Teoría de Números es la reina de la Matemática". En efecto, la Teoría de Números resulta ser una rama de las matemáticas que, a lo largo de los siglos (ya desde hace dos milenios, como en el caso de Diofanto de Alejandría) ha atraído y hechizado a los más brillantes matemáticos a lo largo de la historia. Con el objetivo de que el presente trabajo de tesis versara sobre Teoría de Números, pero sin haber definido aún un tema claro y bien delimitado, el autor del presente trabajo se dio a la tarea (instado a ello por su asesor de tesis) de revisar el magnífico libro de Ireland y Rosen [9]. El objetivo de dicha lectura era conseguir una visión del panorama que ofrece la Teoría de Números, sus subramas y los problemas interesantes que plantea, tanto resueltos como por resolver. El capítulo acerca de números de Bernoulli que contiene el mencionado libro sorprende por la belleza de los problemas matemáticos que pueden resolverse elegantemente apelando a dichos números, así como la diversidad de los mismos. Resulta asimismo sugestivo el hecho de que dichos problemas recorren toda la gama de dificultad, desde lo elemental hasta lo que requiere conocimientos teóricos profundos. Además, varios de los teoremas importantes de este capítulo no son demostrados, sino sólo mencionados (junto con la alusión al hecho de que la demostración correspondiente involucra números de Bernoulli) en el libro en cuestión. De esta forma, la tarea de buscar, comprender y explicar estas demostraciones, resulta ser en un legítimo tema de tesis.

En base a lo anterior, el objetivo de la presente tesis es (como su título indica) ofrecer un panorama claro y amplio acerca de lo que son los números de Bernoulli, y de cuál es el papel que juegan dentro de la Teoría de Números. Esto incluye reseñar y explicar sus aplicaciones y consecuencias, dentro de las demostraciones de importantes teoremas de esta rama de las matemáticas. Es bien sabido que las tesis de licenciatura en una disciplina como lo es la matemática van orientadas a la asimilación profunda de conocimiento ya existente, seguida de una exposición clara del mismo. De esta forma, lo que se hizo en el presente trabajo es recopilar, en una diversidad de fuentes bibliográficas, las demostraciones de varios teoremas sumamente importantes dentro

de la Teoría de Números, que involucren de una u otra forma, tanto directa como indirectamente, a los números de Bernoulli. Posteriormente, dichas demostraciones, según sea el caso, se detallaron, se clarificaron o inclusive (en algunas ocasiones) se reformularon, de modo que el todo del trabajo ofrezca al lector la posibilidad de comprender la importancia de los números de Bernoulli en la Teoría de Números.

El orden de exposición es de lo más elemental, a lo que requiere más teoría. De esta forma, el primer capítulo trabaja las nociones más sencillas (sin que ello signifique que los resultados expuestos sean poco profundos) y, en teoría, resulta comprensible para cualquiera que conozca de manera somera los principios básicos de álgebra elemental y cálculo diferencial. El segundo capítulo, por contraste, ofrece resultados que, para ser comprendidos, requieren tener conocimientos de Teoría de Grupos y de Teoría de Anillos. Por último, el tercer capítulo involucra conceptos mucho más complejos y, aunque en este caso no todos los resultados son rigurosamente demostrados (en unas ocasiones debido a que dichos resultados se exponen en los cursos estándar de la licenciatura, y en otras debido a que la dificultad excedía los objetivos del presente trabajo), sí se requiere, como mínimo, conocer la Teoría de Extensiones de Campos y la Teoría de Galois.

El primer capítulo se subdivide en cuatro secciones, siendo la primera una introducción de corte histórico acerca del surgimiento de los números de Bernoulli y los problemas matemáticos que estos números permitieron resolver. La segunda sección expone la definición de los números de Bernoulli, además del problema que condujo a su definición: determinar la suma de las n primeras k-ésimas potencias, para $n, k \in \mathbb{N}$. Asimismo, se deducen algunas propiedades básicas de los números de Bernoulli, que se siguen de manera natural como corolarios. La tercera sección introduce la noción de polinomios de Bernoulli (misma que se encuentra estrecha e indisolublemente ligada a la de los números de Bernoulli), y expone varios resultados importantes que involucran a estos polinomios, incluyendo la conocida fórmula de suma de Euler-MacLaurin. Por último, la cuarta sección habla acerca de la función zeta de Riemann, y de cómo los números de Bernoulli sirven para encontrar los valores de dicha función cuando el argumento correspondiente es o bien un entero positivo par, o bien un entero negativo. El segundo capítulo contiene, más que aplicaciones, teoremas que versan sobre los mismos números de Bernoulli, los cuales a la sazón han obtenido importancia por sí mismos y, por consiguiente, han cobrado vida propia. Este capítulo se subdivide en tres secciones, de las cuales la primera introduce la noción de p-entero y muestra numerosos resultados acerca de qué combinaciones de números de Bernoulli dan lugar a p-enteros, lo cual resulta de gran importancia al determinar cuáles son los factores primos de los denominadores de los números de Bernoulli. Esta sección finaliza con el célebre teorema de Clausen y von-Staudt. La segunda sección muestra una gran cantidad de congruencias que involucran a los números de Bernoulli, tanto en el anillo $\mathbb{Z}$ como en el anillo de p-enteros, incluyendo

las célebres congruencias de Voronoi y las congruencias de Kummer. Estas últimas congruencias se interpretan en términos de continuidad de la función zeta p-ádica, bajo la métrica p-ádica. Y finalmente, la tercera sección versa acerca de los números primos regulares, proporcionándose su definición, ofreciendo la demostración de que existe una infinidad de números primos irregulares, y finalmente mostrando heurísticamente que los números primos regulares muy probablemente son más de la mitad de todos los números primos. Para esto último, se introducen todas las nociones de probabilidad necesarias, de modo que no se requiere ningún conocimiento previo de probabilidad por parte del lector. Por último, el tercer capítulo, que se divide en cinco secciones, está enteramente dedicado a una importantísima aplicación de los números de Bernoulli: demostrar un caso particular del último teorema de Fermat. Esta demostración es tan compleja, que sólo aparece hasta la quinta sección, siendo las cuatro primeras únicamente una introducción de la teoría necesaria para comprenderla. Así, la primera sección constituye un recordatorio acerca de campos y anillos ciclotómicos, mientras que la segunda sirve como repaso acerca de los dominios Dedekind y campos numéricos. La tercera sección introduce las nociones de caracter de Dirichlet y de L-serie, necesarias para el resultado principal de este capítulo, pero sin demostrar todos los resultados, ya que algunos de ellos requieren conocimientos teóricos más profundos de lo que permitiría la extensión del trabajo. Incidentalmente, junto con las L-series, que generalizan a la función zeta de Riemann, se introduce la definición de los números de Bernoulli generalizados, mismos que proporcionan ciertos valores de las L-series en argumentos enteros negativos, con lo cual se generaliza uno de los resultados de la cuarta sección del primer capítulo acerca de ciertos valores de la función zeta de Riemann. La cuarta sección muestra el camino (nuevamente, sin demostrar todo lo que aparece en dicho camino) para demostrar un importante teorema que relaciona a los números primos regulares con cierta propiedad en determinados anillos ciclotómicos, y que será pieza fundamental para comprender cómo se relacionan los números de Bernoulli con este caso particular del último teorema de Fermat. Por último, en la quinta sección se expone la demostración de la primera parte de este caso particular (pues la segunda parte del mismo exige, nuevamente, exceder la cantidad de teoría permisible dentro del presente trabajo), ilustrando con ello una de las más bonitas e importantes aplicaciones de los números de Bernoulli en Teoría de Números.

La realización del presente trabajo involucró variadas dificultades; desde las obvias, como puede ser intentar comprender una demostración particularmente difícil, hasta las más inesperadas, tales como las dificultades relativas al tiempo y al espacio. En efecto, los números de Bernoulli resultan ser fundamentales, no sólo para la Teoría de Números sino para una gran cantidad de ramas de las matemáticas, y sus aplicaciones tan sólo en la Teoría de Números son tantas, tan variadas, y todas ellas tan hermosas, que se hizo particularmente difícil seleccionar de entre ellas, las que no

hicieran que el presente trabajo excediera la longitud permisible; así como aquellas que no provocaran que el tiempo de realización de esta tesis rebasara los límites de lo admisible. Sin embargo, considero que el resultado final ha sido satisfactorio, y que el lector encontrará en el presente trabajo una interesante y amplia introducción a los números de Bernoulli, que mostrará en manera clara y comprensible la enorme importancia que tienen estos números en el corazón mismo de la Teoría de Números.

Capítulo 1

Números de Bernoulli

El presente capítulo da cuenta de propiedades básicas de los números de Bernoulli, a saber, aquellas que no requieren álgebra especialmente avanzada. En la primera sección se justifica la importancia histórica de los números de Bernoulli, en la segunda y tercera sección se introducen los conceptos de número de Bernoulli y polinomio de Bernoulli, junto con algunas de sus características principales y aplicaciones básicas. Finalmente, en la cuarta sección se establece una interesante relación entre los números de Bernoulli y la función zeta de Riemann.

1.1. Introducción histórica

Comenzaremos por mencionar tres problemas, cada uno de los cuales tiene un importante interés histórico.

El primero de ellos tiene que ver con la búsqueda de fórmulas para la suma de las k-ésimas potencias de los primeros n enteros positivos. Jacob Bernoulli (1654-1705) conocía las siguientes fórmulas:

$$\begin{aligned} 1+2+3+\cdots+(n-1) &= \frac{n(n-1)}{2}, \\ 1^2+2^2+3^2+\cdots+(n-1)^2 &= \frac{n(n-1)(2n-1)}{6}, \\ 1^3+2^3+3^3+\cdots+(n-1)^3 &= \frac{n^2(n-1)^2}{4}. \end{aligned}$$

También conocía otras fórmulas menos famosas, análogas a las anteriores, correspondientes a mayores exponentes, hasta el 10. Esto es, para cada exponente k la

suma $1^k + 2^k + \cdots + (n-1)^k$ resultaba ser un polinomio sobre la variable n de grado $k+1$. Mientras se dedicaba a determinar los coeficientes de estos polinomios para un k arbitrario, Bernoulli se vió obligado a definir los números que llevan su nombre. Finalmente, Bernoulli tuvo éxito al encontrar satisfactoriamente dichos coeficientes, y en su libro *Ars Conjectandi* (una obra póstuma que data de 1713) menciona orgullosamente haber podido sumar las décimas potencias de los primeros mil enteros en menos de un cuarto de hora.

Otro problema importante de aquella época era encontrar la suma

$$\zeta(2) = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \frac{1}{25} + \cdots$$

así como, de manera más general, $\zeta(2m)$, en donde $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ es la función zeta de Riemann. Después de un prolongado esfuerzo, Leonhard Euler (1707-1783) logró mostrar en 1734 que $\zeta(2) = \pi^2/6$. Posteriormente determinó $\zeta(2m)$ para todos los enteros positivos $m \in \mathbb{N}$.

El tercer problema es el célebre último teorema de Fermat. Pierre de Fermat (1601-1665) afirmó que la ecuación $x^n + y^n = z^n$ no tiene solución en enteros positivos para $n \geq 3$. Antes de que Andrew John Wiles (1953-) lograra demostrar este teorema*, se habían logrado ciertos resultados parciales relacionados con él; más concretamente, en 1847 Ernst Eduard Kummer (1810-1893) demostró que, en efecto, lo afirmado por Fermat se verifica en el caso cuando n pertenece a un subconjunto particular del conjunto de números primos, los llamados primos regulares. Más aún, Kummer descubrió un bonito criterio elemental para la regularidad de un primo p, que involucra propiedades de divisibilidad de los primeros $(p-3)/2$ números no cero de Bernoulli. Mientras desarrollaba sus resultados, Kummer realizó grandes avances en teoría de anillos, introduciendo varios conceptos importantes, entre ellos el de ideal.

Los primeros dos problemas serán discutidos en las siguientes secciones, el tercero se tratará con detalle en el capítulo 3.

1.2. Números de Bernoulli

Comenzaremos por atacar el problema de calcular la sumatoria de las primeras $n-1$ m-ésimas potencias. Con ese objetivo, definimos para cada $n, m \in \mathbb{N}$, la cantidad

*Sin el afán de menospreciar el trabajo de Wiles, ni quitarle absolutamente ningún mérito, cabe mencionar que su demostración no es algebraica.

$S_m(n) := 1^m + 2^m + \cdots + (n-1)^m$. Por otro lado, debido al teorema del binomio de Newton, se tiene que para cada $k, m \in \mathbb{Z}$, con k y m no negativos,

$$(k+1)^{m+1} = 1 + \binom{m+1}{1}k + \binom{m+1}{2}k^2 + \cdots + \binom{m+1}{m}k^m + k^{m+1}.$$

Restando k^{m+1} a ambos lados de la ecuación anterior, y sustituyendo en dicha ecuación los valores de $k = 0, 1, \ldots, n-1$, obtenemos las siguientes ecuaciones:

$$\begin{aligned}
1^{m+1} - 0^{m+1} &= 1 + \binom{m+1}{1}0 + \cdots + \binom{m+1}{m}0^m, \\
2^{m+1} - 1^{m+1} &= 1 + \binom{m+1}{1}1 + \cdots + \binom{m+1}{m}1^m, \\
3^{m+1} - 2^{m+1} &= 1 + \binom{m+1}{1}2 + \cdots + \binom{m+1}{m}2^m, \\
\vdots \qquad\qquad & \quad \vdots \qquad\qquad\qquad\qquad \vdots \\
n^{m+1} - (n-1)^{m+1} &= 1 + \binom{m+1}{1}(n-1) + \cdots + \binom{m+1}{m}(n-1)^m.
\end{aligned}$$

Sumando todas estas ecuaciones miembro a miembro, obtenemos

$$n^{m+1} = n + \binom{m+1}{1}S_1(n) + \binom{m+1}{2}S_2(n) + \cdots + \binom{m+1}{m}S_m(n). \qquad (1.2.1)$$

De modo que, si se tienen fórmulas para $S_1(n), S_2(n), \ldots, S_{m-1}(n)$, entonces la ecuación (1.2.1) nos permite encontrar una fórmula para $S_m(n)$. Bernoulli observó que $S_m(n)$ es un polinomio de grado $m+1$ en n cuyo término principal es $n^{m+1}/(m+1)$. Esto se demuestra fácilmente por inducción, a partir de la ecuación (1.2.1). Además, el término independiente resulta ser siempre cero, lo cual también se sigue con facilidad de la ecuación (1.2.1) y el principio de inducción. Los valores de los otros coeficientes son menos obvios. Así, por ejemplo, se tiene que

$$\begin{aligned}
S_1(n) &= -\frac{1}{2}\cdot n + \frac{1}{2}\cdot n^2, \\
S_2(n) &= \frac{1}{6}\cdot n - \frac{1}{2}\cdot n^2 + \frac{1}{3}\cdot n^3, \\
S_3(n) &= \frac{1}{4}\cdot n^2 - \frac{1}{2}\cdot n^3 + \frac{1}{4}\cdot n^4.
\end{aligned}$$

Por cálculo directo, se puede encontrar que los coeficientes de n son $-\frac{1}{2}$, $\frac{1}{6}$, 0, $-\frac{1}{30}$, 0, $\frac{1}{42}$, 0, $-\frac{1}{30}$, 0, $\frac{5}{66}$, para $m = 1, 2, \ldots, 10$. La observación empírica de todas estas fórmulas condujo a Bernoulli a la siguiente definición.

Definición 1.2.1. *Se define la sucesión de números $\{B_n\}_{n\in\mathbb{N}\cup\{0\}}$ de manera inductiva como sigue: $B_0 := 1$, y*

$$B_m := -\frac{1}{m+1}\sum_{k=0}^{m-1}\binom{m+1}{k}B_k, \tag{1.2.2}$$

para cada $m \in \mathbb{N}$.

Observación. *Los números B_n que conforman la sucesión de la definición 1.2.1, reciben el nombre de **números de Bernoulli**, en virtud de que fue, como se ha dicho, Jacob Bernoulli quien los definió y utilizó por primera vez.*

Multiplicando ambos lados de la ecuación (1.2.2) por $\binom{m+1}{m} = m+1$, tenemos que dicha ecuación es equivalente a la siguiente:

$$\sum_{k=0}^{m}\binom{m+1}{k}B_k = 0. \tag{1.2.3}$$

Si expresamos la ecuación (1.2.3) para cada $m \in \mathbb{N}$, el resultado es un sistema de ecuaciones que exhibe la siguiente apariencia:

$$\begin{aligned} 2B_1 + 1 &= 0 \\ 3B_2 + 3B_1 + 1 &= 0 \\ 4B_3 + 6B_2 + 4B_1 + 1 &= 0 \\ 5B_4 + 10B_3 + 10B_2 + 5B_1 + 1 &= 0 \\ \vdots \qquad\qquad\qquad & \vdots \end{aligned}$$

Por ejemplo, realizando los cálculos para los primeros doce números de Bernoulli, tenemos que

$$\begin{aligned} B_1 &= -\frac{1}{2}, & B_2 &= \frac{1}{6}, & B_3 &= 0, \\ B_4 &= -\frac{1}{30}, & B_5 &= 0, & B_6 &= \frac{1}{42}, \\ B_7 &= 0, & B_8 &= -\frac{1}{30}, & B_9 &= 0, \\ B_{10} &= \frac{5}{66}, & B_{11} &= 0, & B_{12} &= -\frac{691}{2730}. \end{aligned}$$

Más adelante demostraremos que los números de Bernoulli no cero tienen signos alternados. Además, también se verá que todos los números de Bernoulli con índice impar mayor que 1 son cero.

Lema 1.2.1. *Supongamos que se expande la función $t/(e^t-1)$ en serie de potencias alrededor del origen, es decir, que se busca una expresión de la forma* $\dfrac{t}{(e^t-1)} = \displaystyle\sum_{m=0}^{\infty} b_m t^m$. *Entonces, se tiene que* $b_m = B_m/m!, \quad \forall\ m \in \mathbb{N} \cup \{0\}$.

Demostración: En la expansión $\dfrac{t}{(e^t-1)} = \displaystyle\sum_{m=0}^{\infty} b_m t^m$, multiplicamos ambos miembros por $e^t - 1 = \displaystyle\sum_{n=1}^{\infty} \frac{t^n}{n!}$, y de este modo obtendremos que

$$t = \left(\sum_{n=1}^{\infty} \frac{t^n}{n!}\right)\left(\sum_{m=0}^{\infty} b_m t^m\right) = \left(t\sum_{n=0}^{\infty} \frac{t^n}{(n+1)!}\right)\left(\sum_{m=0}^{\infty} b_m t^m\right).$$

Por consiguiente, si se dividen ambos lados de la ecuación anterior entre t, se observará que

$$1 = \left(\sum_{n=0}^{\infty} \frac{t^n}{(n+1)!}\right)\left(\sum_{m=0}^{\infty} b_m t^m\right) = \sum_{m=0}^{\infty}\left(\sum_{k=0}^{m} \frac{b_k}{[(m-k)+1]!}\right) t^m.$$

Si en esta última expresión se igualan los coeficientes a ambos lados, obtenemos que $b_0 = 1 = B_0/0!$, mientras que, para $m \in \mathbb{N}$,

$$0 = \sum_{k=0}^{m} \frac{b_k}{(m+1-k)!} = \sum_{k=0}^{m} \frac{k! b_k}{k!(m+1-k)!},$$

y, al multiplicar ambos lados por $(m+1)!$, se obtiene que

$$0 = \sum_{k=0}^{m} \frac{(m+1)!(k!b_k)}{k![(m+1)-k]!} = \sum_{k=0}^{m} \binom{m+1}{k}(k!b_k), \quad \forall\ m \in \mathbb{N}.$$

Comparando este sistema de ecuaciones con el sistema determinado por la ecuación (1.2.3), se nota que esta última expresión, junto con la "condición inicial" $0!b_0 = B_0 = 1$, implica que $m!b_m = B_m, \ \ \forall\ m \in \mathbb{N}$. □

Con la ayuda del lema 1.2.1, estamos capacitados para responder aquella pregunta que se hizo Bernoulli respecto de las sumas $S_m(n)$.

Teorema 1.2.1. *Para $m, n \in \mathbb{N}$, las sumas $S_m(n)$ vienen dadas por:*

$$S_m(n) = \frac{1}{m+1} \sum_{k=0}^{m} \binom{m+1}{k} B_k \ n^{m+1-k}.$$

Demostración: Para cada $k \in \mathbb{N} \cup \{0\}$, se tiene la igualdad $e^{kt} = \displaystyle\sum_{m=0}^{\infty} \frac{k^m t^m}{m!}$ (en donde utilizamos la convención, bastante útil, de que $0^0 = 1$); de donde, si se sustituyen los valores $k = 0, 1, 2, \ldots, n-1$, resulta:

$$\begin{aligned}
1 &= \sum_{m=0}^{\infty} \frac{0^m t^m}{m!} = 1, \\
e^t &= \sum_{m=0}^{\infty} \frac{t^m}{m!} = \sum_{m=0}^{\infty} \frac{1^m t^m}{m!}, \\
e^{2t} &= \sum_{m=0}^{\infty} \frac{2^m t^m}{m!}, \\
\vdots &\quad \vdots \qquad\quad \vdots \\
e^{(n-1)t} &= \sum_{m=0}^{\infty} \frac{(n-1)^m t^m}{m!}.
\end{aligned}$$

Si sumamos todas estas ecuaciones, el resultado es

$$1 + e^t + e^{2t} + \cdots + e^{(n-1)t} = 1 + \sum_{m=0}^{\infty} S_m(n) \frac{t^m}{m!},$$

pero el miembro izquierdo de esta expresión, es igual a

$$\begin{aligned}\frac{e^{nt}-1}{e^t-1} &= \frac{e^{nt}-1}{t}\cdot\frac{t}{e^t-1} = \left(\sum_{k=1}^{\infty}\frac{n^k t^{k-1}}{k!}\right)\left(\sum_{j=0}^{\infty}B_j\frac{t^j}{j!}\right)\\ &= \left(\sum_{k=0}^{\infty}\frac{n^{k+1}t^k}{(k+1)!}\right)\left(\sum_{j=0}^{\infty}B_j\frac{t^j}{j!}\right)\\ &= \sum_{m=0}^{\infty}\left(\sum_{k=0}^{m}\frac{B_k n^{(m-k)+1}}{k![(m-k)+1]!}\right)t^m.\end{aligned}$$

Así pues, de las dos expresiones anteriores, se concluye que

$$1+\sum_{m=0}^{\infty}S_m(n)\frac{t^m}{m!} = \sum_{m=0}^{\infty}\left(\sum_{k=0}^{m}\frac{B_k n^{(m-k)+1}}{k![(m-k)+1]!}\right)t^m.$$

De modo que si en esta última expresión se igualan los coeficientes correspondientes a t^m, para $m\in\mathbb{N}$, se tendrá que:

$$\frac{S_m(n)}{m!} = \sum_{k=0}^{m}\frac{B_k n^{m+1-k}}{k!(m+1-k)!}.$$

Es por ello que

$$\begin{aligned}(m+1)S_m(n) &= \frac{(m+1)!}{m!}S_m(n) = \sum_{k=0}^{m}\frac{(m+1)!B_k n^{m+1-k}}{k!(m+1-k)!}\\ &= \sum_{k=0}^{m}\binom{m+1}{k}B_k n^{m+1-k}.\end{aligned}$$

□

Acto seguido, estableceremos una importante propiedad de la sucesión de números de Bernoulli, con la cual se concluye la presente sección.

Proposición 1.2.1. $B_{2k+1}=0, \quad \forall\ k\in\mathbb{N}.$

Demostración: Aplicando el lema 1.2.1, y tomando en cuenta que $B_1 = -\frac{1}{2}$, tenemos que

$$\frac{t}{e^t-1} = \sum_{k=0}^{\infty}\frac{B_k}{k!}t^k = 1-\frac{t}{2}+\sum_{k=2}^{\infty}\frac{B_k}{k!}t^k,$$

en consecuencia,

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

Obsérvese ahora que la función $\dfrac{t}{2}\cdot\dfrac{e^t+1}{e^t-1}$ es par, debido a que

$$\begin{aligned}\frac{(-t)}{2}\cdot\frac{e^{-t}+1}{e^{-t}-1} &= \frac{(-t)}{2}\cdot\frac{e^{-t}+1}{e^{-t}-1}\cdot\frac{e^t}{e^t}\\ &= \frac{(-t)}{2}\cdot\frac{1+e^t}{1-e^t} = \frac{(-t)}{2}\cdot\frac{e^t+1}{-(e^t-1)}\\ &= \frac{t}{2}\cdot\frac{e^t+1}{e^t-1};\end{aligned}$$

así pues, se llega a la relación siguiente:

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

Si se igualan los coeficientes de t^k en la última expresión, se tiene que $1=1$ y $B_k/k! = (-1)^k B_k/k!$, para $k\geq 2$, o, en otras palabras,

$$B_k = (-1)^k B_k, \quad \forall\ k\in\mathbb{N}\backslash\{1\}.$$

Cuando k es par, esta última ecuación no proporciona información alguna, aparte del hecho obvio de que $B_k = B_k$. Sin embargo, cuando k es impar y $k\geq 2$, se tiene que $B_k = -B_k$. De ahí que $B_k = 0$, si $k\geq 2$, con k impar. □

1.3. Polinomios de Bernoulli

Definición 1.3.1. *Para cada $m\in\mathbb{N}\cup\{0\}$, definimos el m-ésimo* ***polinomio de Bernoulli****, denotado por $B_m(X)$, como*

$$B_m(X) := \sum_{k=0}^{m}\binom{m}{k}B_k X^{m-k}.$$

De esta forma, se tiene que $B_0(X) = 1$, $B_1(X) = X - \frac{1}{2}$, $B_2(X) = X^2 - X + \frac{1}{6}$, etc. Observemos que, de acuerdo con el teorema 1.2.1,

$$\begin{aligned} B_{m+1}(n) &= \sum_{k=0}^{m+1} \binom{m+1}{k} B_k n^{m+1-k} \\ &= \sum_{k=0}^{m} \binom{m+1}{k} B_k n^{m+1-k} + \binom{m+1}{m+1} B_{m+1} \\ &= (m+1) S_m(n) + B_{m+1}, \end{aligned}$$

de aquí que podamos escribir el resultado del teorema 1.2.1 en la forma:

$$S_m(n) = \frac{1}{m+1}(B_{m+1}(n) - B_{m+1}). \tag{1.3.1}$$

Como consecuencia de la ecuación (1.3.1), tenemos algunas fórmulas interesantes, tal como las siguientes:

$$\sum_{k=n}^{m-1} k^q = S_q(m) - S_q(n) = \frac{1}{q+1} \left(B_{q+1}(m) - B_{q+1}(n) \right),$$

para cualesquiera $q, n, m \in \mathbb{N}$, con $m > n$. En particular, también se tiene que

$$n^q = \frac{1}{q+1} \left(B_{q+1}(n+1) - B_{q+1}(n) \right). \tag{1.3.2}$$

A continuación, enunciamos un par de propiedades importantes de los polinomios de Bernoulli.

Proposición 1.3.1.

(*i*) $\frac{1}{m+1} B'_{m+1}(X) = B_m(X)$, *para cualquier* $m \in \mathbb{N} \cup \{0\}$, *en donde por* B'_{m+1} *entendemos la derivada del polinomio* B_{m+1}.

(*ii*) $B_m(0) = B_m(1) = B_m$, *para todo* $m \in \mathbb{N} \cup \{0\}$, $m \neq 1$.

Demostración:

(*i*) Observemos que $\binom{m+1}{k}\frac{m+1-k}{m+1} = \binom{m}{k}$, lo cual se deduce con facilidad de la definición de los coeficientes binomiales. De manera que

$$\begin{aligned}
\frac{1}{m+1}B'_{m+1}(X) &= \frac{1}{m+1}\left\{\frac{d}{dX}\left(\sum_{k=0}^{m+1}\binom{m+1}{k}B_kX^{m+1-k}\right)\right\} \\
&= \frac{1}{m+1}\sum_{k=0}^{m}\binom{m+1}{k}B_k(m+1-k)X^{m-k} \\
&= \sum_{k=0}^{m}\binom{m+1}{k}\frac{m+1-k}{m+1}B_kX^{m-k} \\
&= \sum_{k=0}^{m}\binom{m}{k}B_kX^{m-k} \\
&= B_m(X).
\end{aligned}$$

(*ii*) Si $m = 0$, entonces el polinomio $B_0(X)$ es el polinomio constante con valor B_0. Ahora bien, cuando $m \geq 2$, entonces es claro que $B_m(0) = B_m$. Por otra parte, se tiene que

$$\begin{aligned}
B_m(1) &= \sum_{k=0}^{m}\binom{m}{k}B_k = B_m + mB_{m-1} + \sum_{k=0}^{m-2}\binom{m}{k}B_k \\
&= B_m + mB_{m-1} - m\left(-\frac{1}{m}\sum_{k=0}^{m-2}\binom{m}{k}B_k\right) \\
&= B_m + mB_{m-1} - mB_{m-1} = B_m.
\end{aligned}$$

□

En el caso del polinomio $B_1(X)$, se tiene que $B_1(0) = -1/2 = B_1$, mientras que $B_1(1) = 1 - 1/2 = 1/2 = -B_1$. Con esto completamos la información acerca de los $B_m(0)$ y $B_m(1)$. Ahora bien, con ayuda de la proposición 1.3.1, podremos generalizar la fórmula de la ecuación (1.3.2), de manera que no sólo resulte válida para $n \in \mathbb{N}$, sino para cualquier número real.

Proposición 1.3.2. *Sea $q \in \mathbb{N} \cup \{0\}$. Entonces, se tiene que*

$$X^q = \frac{1}{q+1}[B_{q+1}(X+1) - B_{q+1}(X)].$$

Demostración: Observemos que, para $q = 0$, se tiene que

$$\frac{1}{1}[B_1(X+1) - B_1(X)] = (X+1) - \frac{1}{2} - \left(X - \frac{1}{2}\right) = 1 = X^0.$$

Asimismo, para $q = 1$, observamos que

$$\begin{aligned}
\frac{1}{2}[B_2(X+1) - B_2(X)] &= \frac{1}{2}\left[(X+1)^2 - (X+1) + \frac{1}{6} - \left(X^2 - X + \frac{1}{6}\right)\right] \\
&= \frac{1}{2}\left[X^2 + 2X + 1 - X - 1 + \frac{1}{6} - X^2 + X - \frac{1}{6}\right] \\
&= \frac{1}{2}(2X) = X = X^1.
\end{aligned}$$

Procedemos ahora por inducción. Supóngase que, siendo $q > 1$, la fórmula se satisface para $q - 1$, es decir,

$$X^{q-1} = \frac{1}{q}[B_q(X+1) - B_q(X)].$$

Entonces, observemos que, debido a la hipótesis de inducción,

$$\frac{d}{dX}(X^q) = qX^{q-1} = B_q(X+1) - B_q(X).$$

En consecuencia, debido a la proposición 1.3.1 parte (i), se tiene que

$$\frac{d}{dX}(X^q) = \frac{1}{q+1}[B'_{q+1}(X+1) - B'_{q+1}(X)]$$

y esto último implica que, para cierta constante c,

$$c = X^q - \frac{1}{q+1}[B_{q+1}(X+1) - B_{q+1}(X)]. \tag{1.3.3}$$

Observemos cuál es el término independiente del polinomio $B_{q+1}(X+1)$. Para ello, desarrollamos el polinomio:

$$\begin{aligned} B_{q+1}(X+1) &= \binom{q+1}{0} B_0 (X+1)^{q+1} + \binom{q+1}{1} B_1 (X+1)^q + \cdots \\ &\quad \cdots + \binom{q+1}{q} B_q (X+1) + B_{q+1} \\ &= \binom{q+1}{0} B_0 \left[X^{q+1} + \binom{q+1}{1} X^q + \cdots + \binom{q+1}{q} X + 1 \right] + \\ &\quad + \binom{q+1}{1} B_1 \left[X^q + \binom{q}{1} X^{q-1} + \cdots + \binom{q}{q-1} X + 1 \right] + \cdots \\ &\quad \cdots + \binom{q+1}{q} B_q (X+1) + B_{q+1}. \end{aligned}$$

De ahí que, claramente, el término independiente de $B_{q+1}(X+1)$ sea igual a

$$\begin{aligned} \binom{q+1}{0} B_0 + \binom{q+1}{1} B_1 + \cdots + \binom{q+1}{q} B_q + B_{q+1} &= \sum_{k=0}^{q+1} \binom{q+1}{k} B_k \\ &= B_{q+1}(1). \end{aligned}$$

En consecuencia, la proposición 1.3.1 parte (ii) nos asegura que el término independiente del polinomio $B_{q+1}(X+1)$ es igual a B_{q+1}. Ahora bien, es claro que éste es también el término independiente del polinomio $B_{q+1}(X)$. Es por ello que el polinomio $[B_{q+1}(X+1) - B_{q+1}(X)]/(q+1)$ tiene término constante igual a cero. Asimismo, siendo por hipótesis $q > 1$, el polinomio X^q no es constante, y su término constante es igual a cero. Así pues, la ecuación (1.3.3) implica que $c = 0$ y la proposición se sigue. □

Con los resultados obtenidos hasta ahora, es posible deducir una interesante fórmula de multiplicación para los polinomios de Bernoulli.

Teorema 1.3.1. *Sea $q \in \mathbb{N} \cup \{0\}$. Entonces, para cualquier $k \in \mathbb{N}$,*

$$B_q(kX) = k^{q-1} \sum_{j=0}^{k-1} B_q \left(X + \frac{j}{k} \right).$$

Demostración: Dada la proposición 1.3.2, si evaluamos X^q en $X = n + j/k$ (para algunos $n \in \mathbb{N}$, $j \in \mathbb{N} \cup \{0\}$) y multiplicamos por k^q, obtenemos

$$(kn+j)^q = \frac{k^q}{q+1} \left[B_{q+1} \left(n + \frac{j}{k} + 1 \right) - B_{q+1} \left(n + \frac{j}{k} \right) \right].$$

Si $N, M \in \mathbb{N}$, con $N > M$ y sumamos la expresión anterior para n desde M hasta $N-1$, obtendremos que

$$\begin{aligned}
\sum_{n=M}^{N-1}(kn+j)^q &= \frac{k^q}{q+1}\sum_{n=M}^{N-1}\left[B_{q+1}\left(n+\frac{j}{k}+1\right)-B_{q+1}\left(n+\frac{j}{k}\right)\right] \\
&= \frac{k^q}{q+1}\Bigg\{B_{q+1}\left(M+\frac{j}{k}+1\right)-B_{q+1}\left(M+\frac{j}{k}\right)+ \\
&\quad +B_{q+1}\left(M+\frac{j}{k}+2\right)-B_{q+1}\left(M+\frac{j}{k}+1\right)+ \\
&\quad +\cdots+B_{q+1}\left(N+\frac{j}{k}\right)-B_{q+1}\left(N-1+\frac{j}{k}\right)\Bigg\} \\
&= \frac{k^q}{q+1}\left\{B_{q+1}\left(N+\frac{j}{k}\right)-B_{q+1}\left(M+\frac{j}{k}\right)\right\}.
\end{aligned}$$

En consecuencia, si ahora sumamos la expresión anterior para j desde 0 hasta $k-1$, obtenemos

$$\sum_{n=M}^{N-1}\sum_{j=0}^{k-1}(kn+j)^q = \frac{k^q}{q+1}\sum_{j=0}^{k-1}\left\{B_{q+1}\left(N+\frac{j}{k}\right)-B_{q+1}\left(M+\frac{j}{k}\right)\right\}.$$

Sin embargo, se tiene que

$$\sum_{n=M}^{N-1}\sum_{j=0}^{k-1}(kn+j)^q = \sum_{m=Mk}^{Nk-1}m^q = \frac{1}{q+1}[B_{q+1}(Nk)-B_{q+1}(Mk)],$$

de manera que

$$\frac{1}{q+1}[B_{q+1}(Nk)-B_{q+1}(Mk)] = \frac{k^q}{q+1}\sum_{j=0}^{k-1}\left\{B_{q+1}\left(N+\frac{j}{k}\right)-B_{q+1}\left(M+\frac{j}{k}\right)\right\},$$

multiplicando la expresión anterior por $q+1$ y despejando, observamos que

$$B_{q+1}(Nk)-k^q\sum_{j=0}^{k-1}B_{q+1}\left(N+\frac{j}{k}\right) = B_{q+1}(Mk)-k^q\sum_{j=0}^{k-1}B_{q+1}\left(M+\frac{j}{k}\right),$$

$\forall\ N \in \mathbb{N},\ N > M$; de donde, dejando M fijo y variando $N > M$, consideremos la expresión

$$f(X) = B_{q+1}(Xk)-k^q\sum_{j=0}^{k-1}B_{q+1}\left(X+\frac{j}{k}\right),$$

cuyo grado como polinomio es a lo más $q+1$. Esta expresión toma, sin embargo, el mismo valor para una infinidad de X (es decir, $f(M+1) = f(M+2) = f(M+3), \cdots$, con $\text{grad}(f) \leq q+1$). En consecuencia, $f(X)$ debe de ser un polinomio constante, de donde, diferenciando, tenemos que

$$f'(X) = kB'_{q+1}(Xk) - k^q \sum_{j=0}^{k-1} B'_{q+1}\left(X + \frac{j}{k}\right) = 0.$$

Si aplicamos la proposición 1.3.1 parte (i), observaremos que

$$(q+1)k\left\{B_q(Xk) - k^{q-1}\sum_{j=0}^{k-1} B_q\left(X + \frac{j}{k}\right)\right\} = 0,$$

expresión que dividimos entre $(q+1)k \neq 0$, obteniendo así el resultado pedido. □

Corolario 1.3.1. *Si $m \in \mathbb{N} \cup \{0\}$, entonces se tiene que*

$$B_{2m}\left(\frac{1}{2}\right) = \left(\frac{1}{2^{2m-1}} - 1\right) B_{2m}(0) = \left(\frac{1}{2^{2m-1}} - 1\right) B_{2m}.$$

Demostración: Aplicando el teorema 1.3.1, con $k = 2$ y $q = 2m$, observamos que

$$B_{2m}(2X) = 2^{2m-1}\left[B_{2m}(X) + B_{2m}\left(X + \frac{1}{2}\right)\right],$$

despejando, tenemos que

$$2^{2m-1}B_{2m}\left(X + \frac{1}{2}\right) = B_{2m}(2X) - 2^{2m-1}B_{2m}(X).$$

Evaluando en $X = 0$ y despejando,

$$B_{2m}\left(\frac{1}{2}\right) = \frac{1}{2^{2m-1}}\left[B_{2m}(0) - 2^{2m-1}B_{2m}(0)\right] = \left(\frac{1}{2^{2m-1}} - 1\right) B_{2m}(0).$$

La segunda parte del corolario se deduce inmediatamente de la proposición 1.3.1 parte (ii). □

Otra consecuencia interesante de la proposición 1.3.1, es el siguiente teorema, el cual es de gran importancia.

Teorema 1.3.2 (Fórmula de suma de Euler-MacLaurin). *Sea $f : \mathbb{R} \to \mathbb{R}$ una función derivable q veces. Dados $a, b \in \mathbb{Z}$, se tiene que*

$$\sum_{n=a+1}^{b} f(n) = \int_a^b f(x)dx + \sum_{r=1}^{q}(-1)^r \frac{B_r}{r!}\{f^{(r-1)}(b) - f^{(r-1)}(a)\} + R_q, \tag{1.3.4}$$

en donde el término residual R_q viene dado por

$$R_q = \frac{(-1)^{q-1}}{q!}\int_a^b B_q(x - [x])f^{(q)}(x)dx. \tag{1.3.5}$$

Aquí, $[x]$ denota el único entero positivo k tal que $k \leq x < k + 1$.

Demostración: Comencemos por considerar el número $\displaystyle\int_0^1 f(x)dx$. Notando que $B_1'(X) = 1$, realizamos integración por partes

$$\int_0^1 f(x)dx = \int_0^1 B_1'(x)f(x)dx = [B_1(x)f(x)]_0^1 - \int_0^1 B_1(x)f'(x)dx.$$

La proposición 1.3.1 parte (i) nos asegura que $B_m(X) = \dfrac{1}{m+1}B'_{m+1}(X)$. Así, observamos que

$$\int_0^1 B_1(x)f'(x)dx = \int_0^1 \frac{B_2'(x)}{2}f'(x)dx = \left[\frac{B_2(x)}{2}f'(x)\right]_0^1 - \int_0^1 \frac{B_2(x)}{2}f''(x)dx.$$

Similarmente,

$$\int_0^1 \frac{B_2(x)}{2}f''(x)dx = \int_0^1 \frac{B_3'(x)}{2\cdot 3}f''(x)dx = \left[\frac{B_3(x)}{3!}f''(x)\right]_0^1 - \int_0^1 \frac{B_3(x)}{3!}f'''(x)dx.$$

Continuando con el proceso, en general observamos que

$$\begin{aligned}\int_0^1 \frac{B_m(x)}{m!}f^{(m)}(x)dx &= \int_0^1 \frac{B'_{m+1}(x)}{m!(m+1)}f^{(m)}(x)dx \\ &= \left[\frac{B_{m+1}(x)}{(m+1)!}f^{(m)}(x)\right]_0^1 - \int_0^1 \frac{B_{m+1}(x)}{(m+1)!}f^{(m+1)}(x)dx,\end{aligned}$$

para cualquier $1 \leq m < q$. Repitiendo el proceso q veces, obtendremos que

$$\int_0^1 f(x)dx = \sum_{k=1}^{q}(-1)^{k-1}\left[\frac{B_k(x)}{k!}f^{(k-1)}(x)\right]_0^1 + (-1)^q\int_0^1 \frac{B_q(x)}{q!}f^{(q)}(x)dx.$$

Ahora bien, la proposición 1.3.1 parte (ii) nos indica que $B_k(0) = B_k(1) = B_k$ cuando $k \neq 1$, mientras que, dado que $B_1(X) = X - \frac{1}{2}$, entonces $B_1(1) = \frac{1}{2} = -B_1(0)$. En consecuencia,

$$\begin{aligned}\int_0^1 f(x)dx &= \frac{1}{2}\{f(1)+f(0)\} + \sum_{k=2}^{q}(-1)^{k-1}\frac{B_k}{k!}\{f^{(k-1)}(1) - f^{(k-1)}(0)\} + \\ &\quad +(-1)^q \int_0^1 \frac{B_q(x)}{q!} f^{(q)}(x)dx \\ &= f(1) + \sum_{k=1}^{q}(-1)^{k-1}\frac{B_k}{k!}\{f^{(k-1)}(1) - f^{(k-1)}(0)\} + \\ &\quad +(-1)^q \int_0^1 \frac{B_q(x)}{q!} f^{(q)}(x)dx.\end{aligned}$$

Así pues, se tiene que

$$\begin{aligned}f(1) &= \int_0^1 f(x)dx + \sum_{k=1}^{q}(-1)^{k}\frac{B_k}{k!}\{f^{(k-1)}(1) - f^{(k-1)}(0)\} + \\ &\quad +(-1)^{q-1} \int_0^1 \frac{B_q(x)}{q!} f^{(q)}(x)dx,\end{aligned}$$

de modo que, si realizamos cambiamos $f(x)$ por $f(n-1+x)$, tendremos que

$$\begin{aligned}f(n) &= \int_0^1 f(n-1+x)dx + \sum_{k=1}^{q}(-1)^{k}\frac{B_k}{k!}\{f^{(n-1)}(n) - f^{(n-1)}(n-1)\} + \\ &\quad +(-1)^{q-1} \int_0^1 \frac{B_q(x)}{q!} f^{(q)}(n-1+x)dx.\end{aligned}$$

Así, sumando la expresión anterior desde $n = a+1$ hasta b, tenemos que

$$\begin{aligned}\sum_{n=a+1}^{b} f(n) &= \sum_{n=a+1}^{b}\int_0^1 f(n-1+x)dx + \\ &\quad + \sum_{n=a+1}^{b}\left[\sum_{k=1}^{q}(-1)^{k}\frac{B_k}{k!}\{f^{(n-1)}(n) - f^{(n-1)}(n-1)\}\right] \\ &\quad + \sum_{n=a+1}^{b}(-1)^{q-1}\int_0^1 \frac{B_q(x)}{q!} f^{(q)}(n-1+x)dx. \qquad (1.3.6)\end{aligned}$$

Ahora bien, se tiene que

$$\sum_{n=a+1}^{b}\int_0^1 f(n-1+x)dx = \sum_{n=a+1}^{b}\int_{n-1}^{n} f(x)dx = \int_a^b f(x)dx. \tag{1.3.7}$$

Por otra parte,

$$\begin{aligned}
&\sum_{n=a+1}^{b}\left[\sum_{k=1}^{q}(-1)^k\frac{B_k}{k!}\{f^{(n-1)}(n)-f^{(n-1)}(n-1)\}\right] = \\
&= \sum_{k=1}^{q}(-1)^k\frac{B_k}{k!}f^{(k-1)}(a+1)-\sum_{k=1}^{q}(-1)^k\frac{B_k}{k!}f^{(k-1)}(a)+ \\
&\quad +\sum_{k=1}^{q}(-1)^k\frac{B_k}{k!}f^{(k-1)}(a+2)-\sum_{k=1}^{q}(-1)^k\frac{B_k}{k!}f^{(k-1)}(a+1)+ \\
&\quad +\cdots+\sum_{k=1}^{q}(-1)^k\frac{B_k}{k!}f^{(k-1)}(b)-\sum_{k=1}^{q}(-1)^k\frac{B_k}{k!}f^{(k-1)}(b-1) \\
&= \sum_{k=1}^{q}(-1)^k\frac{B_k}{k!}\{f^{(k-1)}(b)-f^{(k-1)}(a)\}.
\end{aligned} \tag{1.3.8}$$

Si denotamos por $R_q := \displaystyle\sum_{n=a+1}^{b}(-1)^{q-1}\int_0^1 \frac{B_q(x)}{q!}f^{(q)}(n-1+x)dx$, entonces tendremos que

$$\begin{aligned}
R_q &= (-1)^{q-1}\sum_{n=a+1}^{b}\int_{n-1}^{n}\frac{B_q(x-[x])}{q!}f^{(q)}(x)dx \\
&= (-1)^{q-1}\int_a^b \frac{B_q(x-[x])}{q!}f^{(q)}(x)dx.
\end{aligned} \tag{1.3.9}$$

De las ecuaciones (1.3.7), (1.3.8) y (1.3.9), tenemos que la ecuación (1.3.6) se transforma en el resultado pedido. □

De esta forma, las ecuaciones (1.3.4) y (1.3.5) del teorema 1.3.2 reciben el nombre de **fórmula de suma de Euler-MacLaurin**, en honor a Euler y a Colin MacLaurin (1698-1746). Esta fórmula resulta ser de gran utilidad para realizar cierto tipo de aproximaciones. Únicamente mencionaremos dos de ellas, sin desarrollarlas. La primera de ellas es la conocida **fórmula de Stirling** que muestra el comportamiento asintótico de la función factorial. En efecto, considerando el logaritmo

de la función factorial, tenemos que $\log(N!) = \sum_{n=1}^{N} \log n$, así que de inmediato se puede aplicar la fórmula de Euler-MacLaurin y observar el comportamiento cuando $N \to \infty$. La segunda aplicación que podemos mencionar, resulta de aplicar la fórmula de Euler-MacLaurin a la sumatoria $\sum_{n=1}^{N} \frac{1}{n}$, pues al hacerlo, obtenemos una expresión que involucra a la famosa **constante de Euler-Mascheroni**, normalmente denotada por γ (de la cual no se sabe aún si pertenece o no a $\mathbb{Q}$), y que está definida como $\gamma := \lim_{n\to\infty} \sum_{k=1}^{n} \frac{1}{k} - \log n$. Gracias a la fórmula de Euler-MacLaurin, así como a ciertas propiedades de los números de Bernoulli, es posible aproximar dicha constante de manera bastante precisa: $\gamma = 0.577215665\ldots$ ([13], capítulo 2, secciones 15-16 (pp. 26-29)).

1.4. Los números $\zeta(2m)$ y $\zeta(1-m)$

Definición 1.4.1. *Sea* $U = \{s \in \mathbb{C} \big| \mathfrak{Re}(s) > 1\} \subseteq \mathbb{C}$. *Se define la* ***función zeta de Riemann****, denotada por* ζ*, como la siguiente función de variable compleja:*

$$\begin{aligned} \zeta : U &\longrightarrow \mathbb{C} \\ s &\longmapsto \sum_{n=1}^{\infty} \frac{1}{n^s}. \end{aligned}$$

La serie de la definición 1.4.1 converge para todos los $s \in U$, además de tener una gran cantidad de propiedades importantes. Por ejemplo, para $s \in U$, se cumple la identidad conocida como **producto de Euler**:

$$\begin{aligned} \zeta(s) &= \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ es primo}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) \\ &= \prod_{p \text{ es primo}} \left(1 - \frac{1}{p^s}\right)^{-1}. \end{aligned} \tag{1.4.1}$$

En la expresión anterior, la igualdad del primer renglón es una consecuencia del teorema fundamental de la aritmética, pues al desarrollar formalmente el producto infinito se obtienen, elevados a la s-ésima potencia, los recíprocos de todos los

posibles productos positivos de potencias de números primos (que es lo mismo que los recíprocos de todos los números naturales) sumados entre sí. La igualdad del segundo renglón se deduce del producto infinito del primer renglón a partir de la fórmula para la serie geométrica. Una demostración formal de la ecuación (1.4.1) puede encontrarse en [19], capítulo 1, sección 1 (pp. 1-2).

El objetivo principal de esta sección es estudiar la relación entre los números de Bernoulli y ciertos valores de la función ζ. Más concretamente, estudiaremos los números $\zeta(2m)$ para $m \in \mathbb{N}$; posteriormente, hablaremos acerca de cómo se puede extender la función ζ a todo el plano complejo, y observaremos el valor de los números $\zeta(1-m)$ para $m \in \mathbb{N}\backslash\{1\}$.

Fue Euler quien encontró una expresión para los números $\zeta(2m)$, misma que constituye uno de sus más notables cálculos. La demostración de dicho resultado requiere de un lema, el cual mencionamos a continuación.

Lema 1.4.1. *Sean*

$$g(z) = \pi \cot(\pi z) = \pi i \cdot \frac{e^{\pi i z} + e^{-\pi i z}}{e^{\pi i z} - e^{-\pi i z}} \quad y$$

$$f(z) = \frac{1}{z} + \sum_{n=1}^{\infty} \frac{2z}{z^2 - n^2}.$$

Entonces, las funciones $g(z)$ y $f(z)$ son holomorfas en todo z no entero, teniendo un polo simple con residuo 1 en cada entero n, con el mismo periodo. Más aún, $g(z) = f(z)$, para cada z no entero, es decir,

$$\pi \cot(\pi z) = \frac{1}{z} + \sum_{n=1}^{\infty} \frac{2z}{z^2 - n^2} \ , \quad \forall \ z \in \mathbb{C}\backslash\mathbb{Z}.$$

Demostración: Ver [18], capítulo 14, sección 70 (pp. 319), ó [17], capítulo 15, ejercicio 4 (pp. 339-340). □

En particular, tenemos que para x número real distinto de $m\pi$, $m \in \mathbb{Z}$,

$$\begin{aligned} \cot(x) &= \left(\frac{1}{\pi}\right) \pi \cot\left(\pi \cdot \frac{x}{\pi}\right) = \left(\frac{1}{\pi}\right)\left(\frac{1}{\frac{x}{\pi}} + \sum_{n=1}^{\infty} \frac{2\frac{x}{\pi}}{(\frac{x}{\pi})^2 - n^2}\right) \\ &= \left(\frac{1}{\pi}\right)\left(\frac{\pi}{x} + \sum_{n=1}^{\infty} \frac{2\frac{x}{\pi}}{\frac{x^2 - n^2\pi^2}{\pi^2}}\right) = \left(\frac{1}{\pi}\right)\left(\frac{\pi}{x} + \sum_{n=1}^{\infty} \frac{2\pi x}{x^2 - n^2\pi^2}\right) \\ &= \frac{1}{x} - 2\sum_{n=1}^{\infty} \frac{x}{n^2\pi^2 - x^2}. \end{aligned} \tag{1.4.2}$$

Con este resultado, estamos en posición de reproducir el cálculo de Euler para los números $\zeta(2m)$.

Teorema 1.4.1. *Para $m \in \mathbb{N}$, se tiene que*

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

Demostración: Utilizamos la ecuación (1.4.2) y la multiplicamos por x para obtener

$$x\cot x = 1 - 2\sum_{n=1}^{\infty}\frac{x^2}{n^2\pi^2 - x^2}, \tag{1.4.3}$$

donde

$$\begin{aligned}\frac{x^2}{n^2\pi^2 - x^2} &= \frac{n^2\pi^2}{n^2\pi^2 - x^2} - 1 = \frac{1}{1-(x/n\pi)^2} - 1\\ &= \sum_{m=1}^{\infty}\left(\frac{x}{n\pi}\right)^{2m},\end{aligned}$$

si $0 < |x| < \pi$. De ahí que

$$\sum_{n=1}^{\infty}\frac{x^2}{n^2\pi^2 - x^2} = \sum_{n=1}^{\infty}\left(\sum_{m=1}^{\infty}\frac{x^{2m}}{n^{2m}\pi^{2m}}\right) = \sum_{m=1}^{\infty}\frac{x^{2m}}{\pi^{2m}}\left(\sum_{n=1}^{\infty}\frac{1}{n^{2m}}\right) = \sum_{m=1}^{\infty}\frac{x^{2m}}{\pi^{2m}}\zeta(2m).$$

Así, de la ecuación (1.4.3), se tiene que

$$x\cot x = 1 - 2\sum_{m=1}^{\infty}\frac{x^{2m}}{\pi^{2m}}\zeta(2m). \tag{1.4.4}$$

Por otra parte, utilizando los lemas 1.2.1 y 1.4.1, se tiene que:

$$\begin{aligned}x\cot x &= xi\cdot\frac{e^{ix}+e^{-ix}}{e^{ix}-e^{-ix}} = xi\cdot\frac{e^{2ix}+1}{e^{2ix}-1} = \frac{ixe^{2ix}+ix}{e^{2ix}-1}\\ &= ix + \frac{2ix}{e^{2ix}-1} = ix + \sum_{n=0}^{\infty}B_n\frac{(2ix)^n}{n!}\\ &= ix + B_0 + 2ixB_1 + \sum_{n=2}^{\infty}B_n\frac{(2ix)^n}{n!};\end{aligned}$$

y, dado que $B_0 = 1, B_1 = -\frac{1}{2}$, concluimos que

$$x \cot x = 1 + \sum_{n=2}^{\infty} B_n \frac{(2ix)^n}{n!}. \tag{1.4.5}$$

De las ecuaciones (1.4.4) y (1.4.5), tenemos que

$$1 - 2\sum_{m=1}^{\infty} \frac{x^{2m}}{\pi^{2m}} \zeta(2m) = 1 + \sum_{m=2}^{\infty} B_m \frac{(2ix)^m}{m!}.$$

Igualando en la expresión anterior los coeficientes correspondientes a x^{2m}, obtenemos que

$$-\frac{2}{\pi^{2m}} \zeta(2m) = (-1)^m \frac{2^{2m}}{(2m)!} B_{2m}, \quad \forall\ m \in \mathbb{N}.$$

□

Por ejemplo, podemos tomar $m = 1, 2, 3$. Como $B_2 = \frac{1}{6}$, $B_4 = -\frac{1}{30}$, $B_6 = \frac{1}{42}$, tenemos entonces que $\zeta(2) = \frac{\pi^2}{6}$, $\zeta(4) = \frac{\pi^4}{90}$, $\zeta(6) = \frac{\pi^6}{945}$.

Por otro lado, como consecuencia del teorema 1.4.1, y puesto que por definición $\zeta(2m)$ es un número real positivo para $m \in \mathbb{N}$, se tiene entonces que $(-1)^{m+1} B_{2m} > 0$ para $m \geq 1$. Es decir, los números de Bernoulli de índice par no son cero y alternan signos.

Asimismo, el teorema 1.4.1 nos permite estimar el crecimiento de B_{2m}. Dado que $\zeta(2m) > 1$, se tiene que

$$|B_{2m}| = \frac{2(2m)!}{(2\pi)^{2m}} \zeta(2m) > \frac{2(2m)!}{(2\pi)^{2m}},$$

de donde, aprovechando que $e^n > n^n/n!$ (lo cual se observa a partir de la expansión en serie de potencias de e^n), es decir, $n!/n^n > e^{-n}$, encontramos que

$$|B_{2m}| > \frac{2(2m)!}{(2\pi)^{2m}} = 2\left(\frac{m}{\pi}\right)^{2m} \frac{(2m)!}{(2m)^{2m}} > 2\left(\frac{m}{\pi}\right)^{2m} \frac{1}{e^{2m}};$$

es decir, que

$$|B_{2m}| > 2\left(\frac{m}{\pi e}\right)^{2m},$$

de donde podemos inferir que los números de Bernoulli de índice par crecen de una manera bastante rápida. En particular,

$$|B_{2m}/2m| > \frac{1}{m}\left(\frac{m}{\pi e}\right)^{2m} \to \infty \text{ cuando } m \to \infty.$$

Todas estas propiedades acerca de los números de Bernoulli, pueden resumirse en la siguiente proposición.

Proposición 1.4.1.

(*i*) $(-1)^{m+1}B_{2m} > 0 \ \ \forall\ m \in \mathbb{N}$.

(*ii*) $|B_{2m}/2m| \to \infty$ *conforme* $m \to \infty$. □

Ahora procederemos a estudiar de una manera más general a la función ζ. Pese a que fue Euler quien, entre otras cosas, calculó los números $\zeta(2m)$, y estableció la ecuación (1.4.1) (que lleva su nombre), fue Georg Friedrich Bernhard Riemann (1826-1866) el primero que consideró a $\zeta(s)$ como una función analítica de una variable compleja. Esto lo hizo por primera vez en el importante artículo [16], que apareció en 1859 en la revista mensual de la Academia de Ciencias de Berlín, con motivo de la elección de Riemann como miembro de dicha Academia. En dicho artículo, Riemann encontró diversas propiedades de la función ζ, dando lugar al nacimiento de toda una teoría acerca de esta función, y permitiendo utilizar la misma en la teoría de números.

Definición 1.4.2. *Sea f una función de variable compleja. Dado el punto $z \in \mathbb{C}$, se dice que f es* ***regular*** *en z si f es univaluada y tiene derivada finita en cada punto de alguna vecindad de z.*

Lo primero que hay que hacer es observar que, pese a que la serie $\sum_{n=1}^{\infty} n^{-s}$, que define a la función zeta de Riemann, no converge cuando $\mathfrak{Re}(s) \leq 1$, sí es posible construir su continuación analítica, que define en todo el plano complejo una función meromorfa con un único polo en el punto $s = 1$. Además, tal función satisface una ecuación importante, conocida como la **ecuación funcional de la función zeta de Riemann**.

Teorema 1.4.2. *La función $\zeta(s)$ es regular para todos los valores de $s \in \mathbb{C}$ excepto para $s = 1$, en donde tiene un polo simple con residuo 1. Además, se satisface la ecuación funcional:*

$$\zeta(s) = 2^s \pi^{s-1} \operatorname{sen}\left(\frac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s). \tag{1.4.6}$$

Demostración: Se puede consultar [19], capítulo 2, secciones 1-10 (pp. 13-27), para encontrar siete distintas maneras de demostrar este hecho. Por otra parte, en [5], capítulo 1, secciones 6 y 7 (pp. 12-16), se detallan dos demostraciones de la ecuación (1.4.6), las cuales son mucho más cercanas a las que originalmente presentó Riemann en [16]. □

La $\Gamma(1-s)$ que aparece en la ecuación (1.4.6), no es otra que la famosa **función Gama**. Se trata de una función de variable compleja con valores complejos, $\Gamma : \mathbb{C} \to \mathbb{C}$, que tiene propiedades interesantes. Sin embargo, para los propósitos que aquí nos ocupan, no necesitaremos conocer con detalle ni la definición de dicha función, ni muchas de sus propiedades: basta saber que, cuando $n \in \mathbb{N}$, resulta ser $\Gamma(n) = (n-1)!$.

El teorema 1.4.2 permite que, a partir de ahora, tenga sentido hablar de $\zeta(s)$ para cualquier valor de $s \in \mathbb{C}\backslash\{1\}$.

Definición 1.4.3. *A la función $\zeta : \mathbb{C}\backslash\{1\} \longrightarrow \mathbb{C}$ del teorema 1.4.2 se le conoce como **función zeta de Riemann generalizada**, o simplemente, de ahora en adelante, como **función zeta de Riemann**.*

En lo que sigue, mostraremos cómo se puede derivar una fórmula para $\zeta(1-m)$, con $m \in \mathbb{N}\backslash\{1\}$, en términos de los números de Bernoulli.

Proposición 1.4.2. *Sea $m \in \mathbb{N}\backslash\{1\}$.*

(i) Si m es impar, entonces $\zeta(1-m) = 0$.

(ii) Si m es par, entonces $\zeta(1-m) = -\dfrac{B_m}{m}$.

Demostración:

(i) Tomemos $k \in \mathbb{N}$ con $m = 2k+1$ y evaluemos $\zeta(1-m)$. A partir de la ecuación (1.4.6), tendremos que

$$\begin{aligned}\zeta(1-m) &= \zeta(1-(2k+1)) = \zeta(-2k)\\ &= 2^{-2k}\pi^{-2k-1}\operatorname{sen}\left(\frac{-2k\pi}{2}\right)\Gamma\left(1-(-2k)\right)\zeta\left(1-(-2k)\right)\\ &= -2^{-2k}\pi^{-2k-1}\operatorname{sen}(\pi k)\Gamma(2k+1)\zeta(2k+1) = 0,\end{aligned}$$

debido a que $\operatorname{sen}(\pi k) = 0,\ \forall\ k \in \mathbb{N}$.

(*ii*) Tomemos $k \in \mathbb{N}$ tal que $m = 2k$, de modo que, al evaluar $\zeta(1-m)$ con ayuda de la ecuación (1.4.6), así como utilizando el teorema 1.4.1, obtendremos lo siguiente:

$$\begin{aligned}
\zeta(1-m) &= \zeta(1-2k) \\
&= 2^{1-2k}\pi^{(1-2k)-1}\operatorname{sen}\left(\frac{\pi(1-2k)}{2}\right)\cdot \\
&\quad \Gamma\left(1-(1-2k)\right)\zeta\left(1-(1-2k)\right) \\
&= 2^{1-2k}\pi^{-2k}\operatorname{sen}\left[\pi\left(\frac{1}{2}-k\right)\right]\Gamma(2k)\zeta(2k) \\
&= -2^{1-2k}\pi^{-2k}\operatorname{sen}\left[\left(k-\frac{1}{2}\right)\pi\right](2k-1)!\frac{(-1)^{k+1}(2\pi)^{2k}}{2(2k)!}B_{2k} \\
&= -2^{1-2k}\pi^{-2k}(-1)^{k+1}(2k-1)!\frac{(-1)^{k+1}2^{2k}\pi^{2k}}{2(2k-1)!2k}B_{2k} \\
&= -2\frac{B_{2k}}{4k} = -\frac{B_{2k}}{2k} = -\frac{B_m}{m}.
\end{aligned}$$

□

A partir de la proposición 1.4.2, se han encontrado una infinidad de ceros para la función zeta de Riemann: a saber, todos los enteros negativos pares. Estos son los denominados **ceros triviales** de dicha función, debido a la relativa facilidad con la cual se obtienen. Además, es posible demostrar, a partir de la ecuación funcional, la ecuación (1.4.6), que estos son los únicos ceros que tiene la función zeta dentro de la región $\{s \in \mathbb{C} \big| \mathfrak{Re}(s) > 1 \text{ ó } \mathfrak{Re}(s) < 0\}$ ([19], capítulo 2, sección 12 (pp. 30); [5], capítulo 1, sección 9 (pp. 18)). De manera que los demás ceros de esta función, los denominados no triviales, deberán yacer en la franja $0 \leq \mathfrak{Re}(s) \leq 1$. Asimismo se puede demostrar que hay una infinidad de ceros no triviales ([19], capítulo 2, sección 12 (pp. 30)). Riemann postuló que de hecho todos los ceros no triviales satisfacen $\mathfrak{Re}(s) = \frac{1}{2}$; sin embargo, tal afirmación no ha podido ser, a la fecha, ni demostrada ni refutada. Este postulado recibe el nombre de **hipótesis de Riemann**.

Ahora bien, por la proposición 1.2.1 sabemos que $B_m = 0$ para todo $m \in \mathbb{N}$ impar con $m \geq 3$. Es por ello que de la proposición 1.4.2 (*i*), se deduce automáticamente que también para m impar, cuando $m > 1$, se cumple la relación $\zeta(1-m) = 0 = -B_m/m$. Esto, junto con la proposición 1.4.2 (*ii*), proporciona una fórmula general para los valores de $\zeta(1-m)$ cuando $m \in \mathbb{N}\backslash\{1\}$. Este importante resultado, con el cual se concluye el presente capítulo, será expresado como teorema debido a su importancia (proporciona información sobre los ceros triviales de la función zeta de Riemann)

y a su generalidad (permite conocer el valor que toma la función zeta en cualquier entero negativo).

Teorema 1.4.3. *Sea $m \in \mathbb{N}$, con $m > 1$. Entonces, se satisface la siguiente ecuación:*

$$\zeta(1-m) = -\frac{B_m}{m}. \tag{1.4.7}$$

□

Capítulo 2

Propiedades algebraicas de los números de Bernoulli

En el presente capítulo ahondamos en algunas de las interesantes propiedades de los números de Bernoulli y sus relaciones algebraicas. En la primera sección, observamos la relación de los números de Bernoulli con los p-enteros. En la segunda sección, desarrollamos algunas importantes e interesantes congruencias que involucran a los números de Bernoulli. Finalmente, en la tercera sección, introducimos el concepto de número primo regular (que se encuentra estrechamente relacionado con los números de Bernoulli) y averiguamos cuántos números primos irregulares existen, así como la proporción entre números primos regulares e irregulares.

2.1. La función orden y los p-enteros

Sea p un número primo. Cada número racional $r \in \mathbb{Q}$ distinto de cero se puede expresar de manera única en la forma

$$r = p^n \cdot \frac{a}{b},$$

con $n, a, b \in \mathbb{Z},\ b > 0,\ (a, b) = 1$ y $p \nmid a,\ p \nmid b$.

Definición 2.1.1. *Bajo la expresión anterior de r, definimos el* ***orden p-ádico*** *de r, denotado por* $\mathrm{ord}_p\,(r)$*, como:*

$$\mathrm{ord}_p\,(r) := n.$$

Además, definimos $\mathrm{ord}_p\,(0) := \infty$.

Así, el orden p-ádico define una función $\text{ord}_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$. Esta función tiene las siguientes propiedades:

- $\text{ord}_p\,(r) = \infty \iff r = 0, \quad \forall\, r \in \mathbb{Q}$;
- $\text{ord}_p\,(rs) = \text{ord}_p\,(r) + \text{ord}_p\,(s), \quad \forall\, r, s \in \mathbb{Q}$;
- $\text{ord}_p\,(r+s) \geq \text{mín}\{\text{ord}_p(r), \text{ord}_p\,(s)\}, \quad \forall\, r, s \in \mathbb{Q}$;
- $\text{ord}_p\,(-r) = \text{ord}_p\,(r), \quad \forall\, r \in \mathbb{Q}$;
- $\text{ord}_p\,(r^{-1}) = -\text{ord}_p\,(r), \quad \forall\, r \in \mathbb{Q},\ r \neq 0$.

Definición 2.1.2. *Sea p un número primo. Un número racional $r \in \mathbb{Q}$ se dice que es un p-**entero** si* $\text{ord}_p\,(r) \geq 0$.

En otras palabras, tenemos que r es un p-entero $\iff r = a/b$, con $a, b \in \mathbb{Z}$ y $p \nmid b$. También es posible decir, con un mínimo de ambigüedad, que r es p-entero si y sólo si p no divide al denominador de r.

Es importante observar que el conjunto de los números racionales que son p-enteros forma un subanillo de $\mathbb{Q}$, y éste es exactamente el anillo $\mathbb{Z}$ localizado en el ideal primo $p\mathbb{Z} = \langle p \rangle$. Este subanillo es denotado por $\mathbb{Z}_{\langle p \rangle}$. Por lo tanto, se tiene que $\mathbb{Z} \subseteq \mathbb{Z}_{\langle p \rangle} \subseteq \mathbb{Q}$, en donde $\mathbb{Q}$ es el campo de cocientes de $\mathbb{Z}_{\langle p \rangle}$, es decir, $\mathbb{Q} = \text{coc}\left(\mathbb{Z}_{\langle p \rangle}\right)$.

Definición 2.1.3. *Sobre $\mathbb{Z}_{\langle p \rangle}$ definimos la siguiente relación de equivalencia: Para cada $r, s \in \mathbb{Z}_{\langle p \rangle}$, decimos que $r \equiv s \mod p^n$ si y sólo si* $\text{ord}_p\,(r-s) \geq n$.

De manera equivalente a la definición 2.1.3, podemos decir que $r \equiv s \mod p^n$ si y sólo si $r - s = a/b$, donde $a, b \in \mathbb{Z}$ con $p \nmid b$ y $p^n \mid a$. Esto es, $r \equiv s \mod p^n \iff r - s \in p^n\mathbb{Z}_{\langle p \rangle}$.

Pasemos ahora a utilizar las definiciones anteriores. Primeramente, notemos que, de la definición de los coeficientes binomiales, para $m \geq k$ se tiene que

$$\binom{m+1}{k} = \frac{(m+1)!}{k!(m+1-k)!} = \frac{m+1}{m+1-k} \cdot \frac{m!}{k!(m-k)!} = \frac{m+1}{m+1-k}\binom{m}{k}\,.$$

Además, utilizando el hecho de que $\binom{m}{k} = \binom{m}{m-k}$, observaremos que la ecuación del teorema 1.2.1 se convierte en:

$$\begin{aligned} S_m(n) &= \sum_{k=0}^{m} \binom{m}{k} B_k \frac{n^{m+1-k}}{m+1-k} \\ &= \sum_{k=0}^{m} \binom{m}{k} B_{m-k} \frac{n^{k+1}}{k+1} \\ &= B_m n + \binom{m}{1} B_{m-1} \frac{n^2}{2} + \cdots + B_0 \frac{n^{m+1}}{m+1}. \end{aligned} \tag{2.1.1}$$

Usaremos la ecuación (2.1.1), junto con el siguiente lema, para probar que para cada p número primo y para cada $m \geq 1$, pB_m debe de ser un p-entero.

Lema 2.1.1. *Sea p número primo, y $k \in \mathbb{N}$. Entonces,*

(*i*) $p^k/(k+1)$ *es p-entero.*

(*ii*) $p^k/(k+1) \equiv 0 \bmod p$ *si* $k \geq 2$.

(*iii*) $p^{k-2}/(k+1)$ *es p-entero si* $k \geq 3$ *y* $p \geq 5$.

Demostración:

(*i*) Veamos que $k+1 \leq p^k, \quad \forall\ k \in \mathbb{N}$ y $\forall\ p$ número primo. Probaremos esto por inducción sobre k. Si $k = 1$, el resultado es evidente. Suponiendo que $k+1 \leq p^k$, se tiene entonces que $k+2 \leq p^k + 1 < 2p^k \leq p^{k+1}$, de donde el enunciado se sigue, como queríamos, para todo número natural k y para todo número primo p.

Así, si escribimos $k+1 = p^a q$, con $(q,p) = 1$, tenemos entonces que $p^k/(k+1) = p^{k-a}/q$, y como $p^k/(k+1) \geq 1$, ello significa que necesariamente $p^{k-a} \geq q \geq 1 \Rightarrow k - a \geq 0$, que es lo que queríamos demostrar.

(*ii*) De la misma demostración que en (*i*), observemos que las desigualdades se pueden hacer estrictas si consideramos $k \geq 2$. De modo que, en este caso, la demostración procede exactamente de la misma forma, simplemente sustituyendo los signos de "mayor o igual" o "menor o igual" por los de "estrictamente mayor" o "estrictamente menor", respectivamente. De esta forma, en este caso concluiremos que $\mathrm{ord}_p\,(p^k/(k+1)) = k - a > 0$, o lo que es lo mismo, que $\mathrm{ord}_p\,(p^k/(k+1)) \geq 1$, que es lo que se quería demostrar.

(*iii*) Para probar este último inciso, al igual que en (*i*), veremos que $k+1 \leq p^{k-2}$, lo cual se hará también por inducción, pero suponiendo en este caso que $k \geq 3$ y $p \geq 5$. Entonces, nuestro caso inicial no es ya $k = 1$, sino $k = 3$, y en este caso, $k + 1 = 4 < 5 \leq p = p^{3-2} = p^{k-2}$. Ahora bien, si suponemos que $k + 1 < p^{k-2}$, para algún $k \geq 3$, entonces se tiene que $k + 2 < p^{k-2} + 1 < 2p^{k-2} < p^{k-1}$, con lo cual el enunciado quedó probado para todo $k \geq 3$, $p \geq 5$. Es decir, que $p^{k-2}/(k + 1) > 1$, de modo que si $k + 1 = p^a q$, con $(p, q) = 1$, entonces $p^{k-2}/(k + 1) = p^{k-2-a}/q$, y necesariamente se tendrá que $p^{k-2-a} > q \geq 1$, con lo cual $\text{ord}_p\ (p^{k-2}/(k + 1)) = k - 2 - a > 0$. Esto es, que $p^{k-2}/(k + 1)$ es un p-entero, y no sólo eso, sino que además $p^{k-2}/(k + 1) \equiv 0 \mod p$.

□

Proposición 2.1.1. *Sea p un número primo y $m \in \mathbb{N}$. Entonces, pB_m es p-entero. Si $m \geq 2$ es par, entonces se tiene además que $pB_m \equiv S_m(p) \mod p$.*

Demostración: La primera afirmación se demostrará por inducción. Obsérvese que $pB_1 = -p/2$, el cual es p-entero, $\forall\ p$. Suponemos que $m > 1$, y que la afirmación se cumple para todo número natural menor que m. De la ecuación (2.1.1), con $n = p$, obtenemos que

$$S_m(p) = \sum_{k=0}^{m} \binom{m}{k} B_{m-k} \frac{p^{k+1}}{k+1}.$$

Como $S_m(p) \in \mathbb{Z} \subseteq \mathbb{Z}_{\langle p \rangle}$, y el primer término de la suma de la derecha es exactamente pB_m, bastará entonces demostrar que el resto de los términos de la sumatoria son también p-enteros. Es decir, basta probar que

$$\binom{m}{k} B_{m-k} \frac{p^{k+1}}{k+1} = \binom{m}{k} pB_{m-k} \frac{p^k}{k+1}$$

es p-entero, para $1 \leq k \leq m$. Por hipótesis de inducción, pB_{m-k} es p-entero, para $1 \leq k \leq m$. Asimismo, por el lema 2.1.1, parte (*i*), $p^k/(k + 1)$ es p-entero. Siendo además $\binom{m}{k} \in \mathbb{Z} \subseteq \mathbb{Z}_{\langle p \rangle}$, se sigue que el producto de estas tres cantidades es también p-entero. De aquí se concluye que $pB_m \in \mathbb{Z}_{\langle p \rangle}$, $\forall\ m \in \mathbb{N}$ y $\forall\ p$ número primo.

Para demostrar la congruencia, en virtud de la expresión para $S_m(p)$, bastará con mostrar que

$$\text{ord}_p\ (S_m(p) - pB_m) = \text{ord}_p\ \left(\sum_{k=1}^{m} \binom{m}{k} B_{m-k} \frac{p^{k+1}}{k+1} \right) \geq 1.$$

Para ello, es suficiente ver que

$$\operatorname{ord}_p\left(\binom{m}{k} pB_{m-k}\frac{p^k}{k+1}\right) \geq 1, \quad \forall\ 1 \leq k \leq m.$$

Sin embargo, por el lema 2.1.1, parte (ii), se tiene que, para $k \geq 2$,

$$\operatorname{ord}_p\left(\binom{m}{k} pB_{m-k}\frac{p^k}{k+1}\right) = \operatorname{ord}_p\left(\binom{m}{k} pB_{m-k}\right) + \operatorname{ord}_p\left(\frac{p^k}{k+1}\right) \geq 0 + 1 = 1,$$

de donde se sigue lo pedido cuando $k \geq 2$. Ahora bien, cuando $k = 1$, necesitamos mostrar que

$$\operatorname{ord}_p\left(\frac{m}{2}\left(pB_{m-1}\right)p\right) \geq 1,$$

lo cual es cierto, ya que, como m es par, esto significa que si $m \geq 4$, entonces $B_{m-1} = 0$, con $\operatorname{ord}_p(0) = \infty \geq 1$; mientras que, si $m = 2$, entonces se tendrá

$$\operatorname{ord}_p\left(\frac{m}{2}\left(pB_{m-1}\right)p\right) = \operatorname{ord}_p\left(p^2B_1\right) = \operatorname{ord}_p\left(-\frac{p^2}{2}\right) \geq 1,$$

de donde en cualquier caso se cumple lo pedido. □

En lo que sigue, nos encaminaremos a demostrar el célebre teorema de Clausen-von Staudt, para lo cual utilizaremos tanto la proposición 2.1.1, como los siguientes dos resultados preliminares.

Teorema 2.1.1. *Sea p un número primo. Entonces, el grupo multiplicativo de enteros no cero módulo p, $(\mathbb{Z}/p\mathbb{Z})^*$, es un grupo cíclico.*

Demostración: Ver [9], capítulo 4, sección 1, teorema 1 (pp. 40). □

Definición 2.1.4. *Sean $a, n \in \mathbb{Z}$. Se dice que a es una **raíz primitiva módulo** n si la clase residual de a módulo n, $a + n\mathbb{Z}$, genera al grupo $(\mathbb{Z}/n\mathbb{Z})^*$, el grupo multiplicativo de números enteros primos relativos con n módulo n.*

De manera equivalente, podemos decir que a es raíz primitiva módulo n si $(a, n) = 1$ y $\phi(n)$ es el menor entero positivo tal que $a^{\phi(n)} \equiv 1 \bmod n$. Lo que hace el teorema 2.1.1, es garantizar que para un número primo p, existen raíces primitivas módulo p. Fue Johann Carl Friedrich Gauss (1777-1855) el primero en demostrar dicho teorema, mismo que juega un papel importante en la demostración del siguiente lema.

Lema 2.1.2. *Sea p un número primo, y $m \in \mathbb{Z}$.*

(*i*) *Si $(p-1) \nmid m$, entonces $S_m(p) \equiv 0 \bmod p$.*

(*ii*) *Si $(p-1) \mid m$, entonces $S_m(p) \equiv -1 \bmod p$.*

Demostración:

(*i*) Tomemos a $g \in \mathbb{Z}$ de modo que sea una raíz primitiva módulo p, es decir, que $g + p\mathbb{Z}$ sea un generador del grupo cíclico multiplicativo $(\mathbb{Z}/p\mathbb{Z})^*$. Así, el conjunto $\{1, g, g^2, \ldots, g^{p-2}\}$ es un conjunto completo de representantes módulo p de dicho grupo, al igual que el conjunto $\{1, 2, 3, \ldots, p-1\}$; además, se cumple que $g^{p-1} \equiv 1 \bmod p$, y más aún, si $k \in \mathbb{Z}$, entonces $g^k \equiv 1 \bmod p \Rightarrow (p-1) \mid k$. Por consiguiente,

$$\begin{aligned} S_m(p) &= 1^m + 2^m + \cdots + (p-1)^m \\ &\equiv 1 + g^m + g^{2m} + \cdots + g^{(p-2)m} \bmod p, \end{aligned}$$

de modo que $(g^m - 1)S_m(p) \equiv g^{m(p-1)} - 1 \equiv 1^m - 1 \equiv 0 \bmod p$. Como $(p-1) \nmid m$, entonces $g^m \not\equiv 1 \bmod p$, es decir, $g^m - 1 \not\equiv 0 \bmod p$, y por tanto se debe de tener que $S_m(p) \equiv 0 \bmod p$.

(*ii*) Si $(p-1) \mid m$, entonces se tiene que $k^m \equiv 1 \bmod p$, $\forall\ k \in \mathbb{Z}$ tal que $p \nmid k$, en virtud de que el grupo $(\mathbb{Z}/p\mathbb{Z})^*$ es de orden $p-1$. Así, se tiene que

$$\begin{aligned} S_m(p) = 1^m + 2^m + \cdots + (p-1)^m &\equiv 1 + 1 + \cdots + 1 \bmod p \\ &= p - 1 \equiv -1 \bmod p. \end{aligned}$$

□

El siguiente teorema, con el cual se concluye la presente sección, resulta ser de suma importancia, ya que muestra la forma que tienen los denominadores de los números de Bernoulli no cero. Básicamente, lo que se establece es que el denominador de B_{2m} es un número libre de cuadrado cuyos divisores primos son exactamente los números primos p tales que $(p-1) \mid 2m$. Fue demostrado de manera independiente y casi simultánea tanto por Thomas Clausen (1801-1885) como por Karl Georg Christian von Staudt (1798-1867).

Teorema 2.1.2 (Teorema de Clausen-von Staudt). *Para cualquier $m \in \mathbb{N}$, existe un $A_m \in \mathbb{Z}$ tal que $B_{2m} = A_m - \sum_{(p-1)|2m} 1/p$, en donde la suma corre sobre todos los números primos p tales que $(p-1) \mid 2m$.*

Demostración: Por la proposición 2.1.1 sabemos que, si p es un número primo cualquiera, entonces pB_{2m} es p-entero y que $pB_{2m} \equiv S_{2m}(p) \bmod p$. De esto y el lema 2.1.2, se sigue que, por un lado, si $(p-1) \nmid 2m$, entonces $pB_{2m} \equiv 0 \bmod p$, es decir, que $\operatorname{ord}_p\ (pB_{2m}) \geq 1$, con lo cual $\operatorname{ord}_p\ (B_{2m}) \geq 0$ y por lo tanto B_{2m} es un p-entero. Por otro lado, si $(p-1) \mid 2m$, entonces $pB_{2m} \equiv -1 \bmod p$, es decir, que $\operatorname{ord}_p\ (pB_{2m}+1) \geq 1$, lo cual implica que $\operatorname{ord}_p\ \left(B_{2m} + \frac{1}{p}\right) \geq 0$. Definimos

$$A_m := B_{2m} + \sum_{(p-1)|2m} \frac{1}{p}.$$

Escribiendo $C_m = \sum_{(p-1)|2m} \frac{1}{p}$ tenemos que $A_m = B_{2m} + C_m$. Además, C_m será un q-entero para cualquier número primo q que no aparezca en la sumatoria. Así, siendo q un número primo arbitrario, entonces hay dos casos: en primer lugar, si $(q-1) \nmid 2m$ entonces tanto B_{2m} como C_m son q-enteros y, en consecuencia, A_m también lo es; en segundo lugar, si $(q-1) \mid 2m$, entonces tanto $B_{2m} + \frac{1}{q}$ como $\sum_{\substack{(p-1)|2m \\ p \neq q}} \frac{1}{p}$ son q-enteros y, por lo tanto, también lo será su suma, la cual es A_m. De este modo, tenemos que A_m es q-entero para todos los números primos q, de donde se sigue que $A_m \in \mathbb{Z}$ y con esto se completa la demostración. □

Corolario 2.1.1. *Sea p un número primo. Entonces, B_{2m} es un p-entero $\iff$ $(p-1) \nmid 2m$. Si $(p-1) \mid 2m$, entonces $pB_{2m}+1$ es un p-entero; más aún, en este último caso, se tiene que*

$$1 + \operatorname{ord}_p\ \left(B_{2m} + \frac{1}{p}\right) = \operatorname{ord}_p\ \left(p\left(B_{2m} + \frac{1}{p}\right)\right) = \operatorname{ord}_p\ (pB_{2m}+1) \geq 1.$$

Finalmente, se tiene que 6 siempre divide al denominador de B_{2m}, $\forall\ m \in \mathbb{N}$.

Demostración: Escribamos $B_{2m} = U_{2m}/V_{2m}$, con $U_{2m}, V_{2m} \in \mathbb{Z},\ (U_{2m}, V_{2m}) = 1$. La primera afirmación se sigue de que, por el teorema 2.1.2, se tiene que

$$B_{2m} = \frac{A_m \left(\prod_{(p-1)|2m} p \right) - \sum_{(p-1)|2m} \left(\prod_{\substack{(q-1)|2m \\ q \neq p}} q \right)}{\prod_{(p-1)|2m} p}.$$

Dado que claramente, en la expresión de la derecha, el numerador y el denominador son primos relativos, se concluye que $V_{2m} = \prod_{(p-1)|2m} p$, de donde $\operatorname{ord}_p(B_{2m}) \geq 0 \iff (p-1) \nmid 2m$. Asimismo, de la expresión encontrada para V_{2m}, basta observar que tanto $2-1$ como $3-1$ dividen a $2m$, de modo que $2 \mid V_{2m}$ y $3 \mid V_{2m}$, por lo tanto, $6 \mid V_{2m}$. Las restantes afirmaciones ya han sido probadas. □

2.2. Congruencias importantes en $\mathbb{Z}$ y en $\mathbb{Z}_{\langle p \rangle}$

Aún falta mostrar diversas consecuencias de la ecuación (2.1.1). De aquí en adelante escribiremos, así como lo hicimos en la demostración del corolario 2.1.1, al m-ésimo número de Bernoulli como $B_m = U_m/V_m$, con $U_m, V_m \in \mathbb{Z}$, $(U_m, V_m) = 1$, además de suponer de antemano, a menos que se especifique lo contrario, que m es par.

Proposición 2.2.1. *Si m es par, $m \geq 2$, entonces $\forall\ n \in \mathbb{N}$ se tiene que:*

$$V_m S_m(n) \equiv U_m\ n \bmod n^2.$$

Demostración: Sea m par, $m \geq 2$, y $n \in \mathbb{N}$. Definamos, para $1 \leq k \leq m$, los números A_k^m de la siguiente manera:

$$A_k^m = \binom{m}{k} \left(B_{m-k} \frac{n^{k-1}}{k+1} \right).$$

Entonces, de acuerdo con la ecuación (2.1.1), se tiene que

$$S_m(n) = B_m n + \sum_{k=1}^{m} \left(\binom{m}{k} B_{m-k} \frac{n^{k-1}}{k+1} \right) n^2 = B_m n + \sum_{k=1}^{m} A_k^m n^2. \tag{2.2.1}$$

Lo primero que hay que hacer es demostrar que para $1 \leq k \leq m$, si p es un número primo tal que $p \mid n$, con $p \neq 2, 3$, entonces se tiene que $\operatorname{ord}_p(A_k^m) \geq 0$. Si $k = 1$ esto es claro, debido a que $B_1 = -1/2$ y $B_t = 0$ cuando $t > 1$ e

impar. Así, si $m = 2$, entonces $A_1^2 = \binom{2}{1} B_1 \frac{1}{2} = B_1 = -1/2$, de manera que, como $p \neq 2 \Rightarrow \text{ord}_p\ (A_1^2) = \text{ord}_p\ (-1/2) \geq 0$. Por otra parte, si $m \geq 4$, siendo m par, se tiene que $B_{m-1} = 0$, y por tanto $A_1^m = \binom{m}{1} B_{m-1} \frac{1}{2} = 0$, de donde $\text{ord}_p\ (A_1^m) = \text{ord}_p\ (0) = \infty$. El caso $k = 2$ también es fácil de probar, ya que $A_2^m = \binom{m}{2} B_{m-2} \frac{n}{3}$, donde $\binom{m}{2} \in \mathbb{Z}$, $\text{ord}_p\ (3) = 0$ (dado que $p \neq 3$), y además se tiene que $\text{ord}_p\ (nB_{m-2}) = \text{ord}_p\ (n/p) + \text{ord}_p\ (pB_{m-2}) \geq 0 + 0 = 0$, debido a que $p \mid n$ y a la proposición 2.1.1. De ahí que $\text{ord}_p\ (A_2^m) = \text{ord}_p\ \left(\binom{m}{2}\right) + \text{ord}_p\ \left(\frac{1}{3}\right) + \text{ord}_p\ (nB_{m-2}) \geq 0 + 0 + 0 = 0$. Por otra parte, si $k \geq 3$, entonces recordemos que la proposición 2.1.1 implica que $\text{ord}_p\ (B_{m-k}) \geq -1,\ \ \forall\, m-k \geq 0$ y $\forall\, p$ número primo. Además, como $p \mid n \Rightarrow \text{ord}_p\ (n) \geq 1$. Finalmente, del lema 2.1.1 parte (iii), se tiene que $0 \leq \text{ord}_p\ \left(\frac{p^{k-2}}{k+1}\right) = (k-2)\text{ord}_p\ (p) - \text{ord}_p\ (k+1) = k - 2 - \text{ord}_p\ (k+1)$, de donde se sigue que

$$\begin{aligned}
\text{ord}_p\ \left(B_{m-k}\frac{n^{k-1}}{k+1}\right) &= \text{ord}_p\ (B_{m-k}) + \text{ord}_p\ (n^{k-1}) - \text{ord}_p\ (k+1) \\
&\geq -1 + (k-1)\text{ord}_p\ (n) - \text{ord}_p\ (k+1) \\
&\geq -1 + (k-1) - \text{ord}_p\ (k+1) \\
&= k - 2 - \text{ord}_p\ (k+1) \\
&\geq 0.
\end{aligned}$$

De modo que $\text{ord}_p\ (A_k^m) \geq 0,\ \ \forall\ 1 \leq k \leq m$ cuando p es un número primo tal que $p \mid m$ y $p \neq 2, 3$. Consideremos ahora lo que ocurre con $\text{ord}_2\ (A_k^m)$. Si $k = 1$, entonces tenemos dos casos. El primero de ellos es cuando $m > 2$, y en este caso se tiene que $B_{m-1} = 0$. En consecuencia, $\text{ord}_2\ (A_1^m) = \text{ord}_2\ (0) = \infty$. El segundo caso es cuando $m = 2$, en donde, como ya vimos, $A_k^m = B_1 = -\frac{1}{2}$, de modo y manera que $\text{ord}_2\ (A_1^2) = \text{ord}_2\ (-1/2) = -1$. Por otra parte, cuando $k > 1$, entonces, cuando k es impar y $k \neq m-1$, se tiene que $B_{m-k} = 0$, de donde $\text{ord}_2\ (A_k^m) = \text{ord}_2\ (0) = \infty$. Si por otro lado, k es par, entonces se tiene que $\text{ord}_2\ (k+1) = 0$, de donde $\text{ord}_2\ (A_k^m) = \text{ord}_2\ \left(\binom{m}{k}\right) + \text{ord}_2\ (n^{k-1}) + \text{ord}_2\ (B_{m-k}) - \text{ord}_2\ (k+1) = \text{ord}_2\ \left(\binom{m}{k}\right) + \text{ord}_2\ (n^{k-1}) + \text{ord}_2\ (B_{m-k}) \geq 0 + 0 - 1 \geq -1$. Mientras tanto, si $k = m-1$, se tiene que $A_{m-1}^m = \binom{m}{m-1} B_1 \frac{n^{m-2}}{m} = -\frac{n^{m-2}}{2}$, de donde

$\text{ord}_2\ (A^m_{m-1}) = \text{ord}_2\ \left(-\dfrac{n^{m-2}}{2}\right) = \text{ord}_2\ (n^{m-2}) - \text{ord}_2\ (2) \geq 0-1 = -1$. En cualquier caso, resulta cierto que $\text{ord}_2\ (A^m_k) \geq -1$.
Finalmente, observaremos el comportamiento de $\text{ord}_3\ (A^m_k)$, suponiendo que $3 \mid n$. Por lo ya visto en los casos anteriores, se tiene que $A^m_1 = \begin{cases} 0;\ m > 2 \\ -1/2;\ m = 2 \end{cases}$, de donde $\text{ord}_3\ (A^m_1) = \begin{cases} \infty;\ m > 2 \\ 0;\ m = 2 \end{cases}$, de modo que $\text{ord}_3\ (A^m_1) \geq 0$. Además, se tiene también que $\text{ord}_3\ (A^m_2) = \text{ord}_3\ \left(\binom{m}{2} B_{m-2}\dfrac{n}{3}\right) = \text{ord}_3\ \left(\binom{m}{2}\right) + \text{ord}_3\ (nB_{m-2}) - \text{ord}_3\ (3) \geq 0 + 0 - 1 \geq -1$, debido a que, por la hipótesis de que $3 \mid n$, junto con la proposición 2.1.1, se tiene que $\text{ord}_3\ (nB_{m-2}) = \text{ord}_3\ (n/p) + \text{ord}_3\ (pB_{m-2}) \geq 0 + 0 = 0$. Por esa misma razón se tiene que $\text{ord}_3\ (A^m_3) = \text{ord}_3\ \left(\binom{m}{3} B_{m-3}\dfrac{n^2}{4}\right) = \text{ord}_3\ \left(\binom{m}{3}\right) + \text{ord}_3\ (nB_{m-3}) + \text{ord}_3\ \left(\dfrac{n}{4}\right) \geq 0 + 0 + 1$. Pero para $k \geq 4$, por el lema 2.1.1 parte (ii), se observa que $\text{ord}_3\ (3^k/(k+1)) \geq 1$, de donde, sabiendo que $3 \mid n$, se tiene que $\text{ord}_3\ \left(\dfrac{n^{k-2}}{k+1}\right) = \text{ord}_3\ \left(\dfrac{n^{k-2}}{3^{k-2}}\right) + \text{ord}_3\ \left(\dfrac{3^{k-2}}{k+1}\right) \geq 0 + \text{ord}_3\ \left(\dfrac{3^k}{3^2(k+1)}\right) = \text{ord}_3\ (3^k/(k+1)) - 2\text{ord}_3\ (3) \geq 1-2 = -1$. Con esto, obtenemos lo siguiente:

$$\begin{aligned} \text{ord}_3\ (A^m_k) &= \text{ord}_3\ \left(\binom{m}{k} B_{m-k}\frac{n^{k-1}}{k+1}\right) \\ &= \text{ord}_3\ \left(\binom{m}{k}\right) + \text{ord}_3\ (nB_{m-k}) + \text{ord}_3\ \left(\frac{n^{k-2}}{k+1}\right) \\ &\geq 0 + 0 - 1 = -1. \end{aligned}$$

Así pues, hemos demostrado que, si p es un número primo tal que $p \mid n$, entonces se tiene que $\text{ord}_p\ (A^m_k) \geq \begin{cases} 0;\ p \neq 2, 3 \\ -1;\ p = 2, 3 \end{cases}$. De esto se sigue que, de entre los números primos que dividen a n, los únicos que podrían dividir al denominador de A^m_k son 2 y 3, y más aún, dicho denominador no es divisible por potencias de 2 y 3 mayores que 1. Todo esto implica que el máximo común divisor de n y el denominador de A^m_k es un divisor de 6 y por lo tanto, esto también ocurrirá con el máximo común divisor de n y la suma de los A^m_k. En otras palabras, se puede escribir $\displaystyle\sum_{k=1}^{m} A^m_k = A/(lB)$, con $A, B, l \in \mathbb{Z},\ (B, n) = 1$ y $l \mid 6$; de modo que la ecuación (2.2.1) se convierte en:

$$S_m(n) = B_m n + \frac{An^2}{lB}.$$

Multiplicando por BV_m a ambos miembros de la ecuación anterior, tenemos que

$$BV_m S_m(n) = U_m nB + \frac{V_m An^2}{l}.$$

Debido al corolario 2.1.1, sabemos que $l \mid 6 \mid V_m \Rightarrow l \mid V_m$, por ello se tiene que $\dfrac{V_m A}{l} \in \mathbb{Z}$. En consecuencia, $BV_m S_m(n) \equiv BU_m n \bmod n^2$. Además, dado que $(B, n) = 1$, resulta válido dividir ambos lados de la congruencia entre B, con lo cual obtenemos el resultado deseado. □

Corolario 2.2.1. *Sea $m \in \mathbb{N} \cup \{0\}$ par, y p un número primo tal que $(p-1) \nmid m$. Entonces,*

$$S_m(p) \equiv B_m p \bmod p^2.$$

Demostración: Por la proposición anterior, tenemos que $V_m S_m(p) \equiv U_m p \bmod p^2$. Además, dado que $(p-1) \nmid m$, el teorema 2.1.2 implica que $p \nmid V_m$. De modo que $(p^2, V_m) = 1$, y por tanto, podemos dividir, dentro del anillo $\mathbb{Z}_{\langle p\rangle}$, ambos lados de la congruencia anterior entre V_m, con lo cual se tiene el resultado deseado. □

Ahora tenemos herramienta suficiente para demostrar las útiles congruencias demostradas por Georgy Fedoseevich Voronoi (1868-1908). Se dice que Voronoi descubrió estas congruencias en 1889 mientras aún era estudiante.

Proposición 2.2.2 (Congruencias de Voronoi). *Sea $m > 2$ un número par, y tomamos U_m, V_m como en la proposición anterior. Supóngase que $a, n \in \mathbb{N}$, $(a, n) = 1$. Entonces,*

$$(a^m - 1)U_m \equiv m a^{m-1} V_m \sum_{j=1}^{n-1} j^{m-1} \left[\frac{ja}{n}\right] \bmod n, \tag{2.2.2}$$

en donde $[\alpha]$ denota al único entero k tal que $k \leq \alpha < k+1$.

Demostración: Para $1 \leq j < n$, escribimos $ja = q_j n + r_j$, $0 \leq r_j < n$. Entonces, $[ja/n] = q_j$ y, como $(a, n) = 1$, los conjuntos $\{1, 2, \ldots, n-1\}$ y $\{r_1, r_2, \ldots, r_{n-1}\}$ son idénticos. Por el teorema del binomio de Newton, se sigue inmediatamente que

$$\begin{aligned} j^m a^m &\equiv r_j^m + m q_j n r_j^{m-1} \bmod n^2 \\ &\equiv r_j^m + mn \left[\frac{ja}{n}\right] r_j^{m-1} \bmod n^2; \end{aligned}$$

como $r_j \equiv ja \bmod n$, entonces, dado que $m-1 \geq 2$, tendremos que $r_j^{m-1} \equiv (ja)^{m-1} \bmod n^2$, de donde se sigue que

$$j^m a^m \equiv r_j^m + m a^{m-1} n \left[\frac{ja}{n}\right] j^{m-1} \bmod n^2.$$

Si sumamos todas estas congruencias, con j desde 1 hasta $n-1$, obtenemos que

$$S_m(n) a^m \equiv S_m(n) + m a^{m-1} n \sum_{j=1}^{n-1} \left[\frac{ja}{n}\right] j^{m-1} \bmod n^2,$$

con lo cual

$$S_m(n)(a^m - 1) \equiv m a^{m-1} n \sum_{j=1}^{n-1} \left[\frac{ja}{n}\right] j^{m-1} \bmod n^2;$$

de donde, multiplicando a ambos lados por V_m, y por la proposición 2.2.1, se tiene que

$$U_m n(a^m - 1) \equiv V_m S_m(n)(a^m - 1) \equiv m a^{m-1} n V_m \sum_{j=1}^{n-1} \left[\frac{ja}{n}\right] j^{m-1} \bmod n^2$$

y así, dividiendo toda la congruencia entre n, obtenemos el resultado deseado. □

La congruencia de Voronoi permite deducir numerosas propiedades de los números de Bernoulli. La siguiente proposición, que es un ejemplo de ello, comúnmente se atribuye a John Couch Adams (1819-1892), y proporciona cierta información acerca del numerador de B_m.

Proposición 2.2.3. *Sea $m > 2$ par, y sea p un número primo tal que $(p-1) \nmid m$. Entonces, B_m/m es p-entero.*

Demostración: Por el corolario 2.1.1, sabemos que, dado que $(p-1) \nmid m$, entonces B_m es un p-entero. Escribimos $m = p^t m_0$, donde $m_0 \in \mathbb{N}$, $p \nmid m_0$ y $t \in \mathbb{N} \cup \{0\}$. En la congruencia de Voronoi, proposición 2.2.2, congruencia (2.2.2), tomamos $n = p^t$ y escogemos $a \in \mathbb{Z}$ tal que $p \nmid a$, para obtener que

$$\begin{aligned}(a^m-1)U_m &\equiv ma^{m-1}V_m\sum_{j=1}^{p^t-1} j^{m-1}\left[\frac{ja}{p^t}\right] \bmod p^t\\ &\equiv p^t\left(m_0a^{m-1}V_m\sum_{j=1}^{p^t-1} j^{m-1}\left[\frac{ja}{p^t}\right]\right) \bmod p^t\\ &\equiv 0 \bmod p^t.\end{aligned}$$

Por el teorema 2.1.1, podemos elegir a de modo que sea una raíz primitiva módulo p. Entonces, como $(p-1)\nmid m$, se tendrá que $a^m\not\equiv 1 \bmod p$, es decir, que $p\nmid(a^m-1)$. De ahí que $(a^m-1,p^t)=1$. Es por esto que de la congruencia anterior se sigue que

$$U_m\equiv 0 \bmod p^t,$$

es decir, existe un $k\in\mathbb{Z}$ tal que $U_m=p^tk$. Luego, $B_m/m=U_m/(mV_m)=kp^t/(p^tm_0V_m)=k/(m_0V_m)$. Sabemos que $\operatorname{ord}_p(m_0)=0=\operatorname{ord}_p(V_m)$, por tanto,

$$\operatorname{ord}_p\left(\frac{B_m}{m}\right)=\operatorname{ord}_p(k)-\operatorname{ord}_p(m_0)-\operatorname{ord}_p(V_m)=\operatorname{ord}_p(k)\geq 0$$

y por tanto, B_m/m es un p-entero. □

Así, los números primos p tales que $(p-1)\nmid m$ no dividen al denominador de B_m/m, y tampoco al de B_m. Y, recíprocamente, los números primos p tales que $(p-1)\mid m$, dividen al denominador de B_m, y por tanto también al de B_m/m. Así, los denominadores de B_m y de B_m/m son divisibles por exactamente los mismos números primos. Por otra parte, si p es un número primo tal que $p\mid m$, y además $(p-1)\nmid m$, entonces si $p^s\mid m$, también p^s debe de dividir al numerador de B_m. Como ejemplo, tomemos $m=22$ y $p=11$. Entonces, $B_{22}=\dfrac{11\cdot 131\cdot 593}{2\cdot 3\cdot 23}$, de modo que $\dfrac{B_{22}}{22}=\dfrac{131\cdot 593}{2^2\cdot 3\cdot 23}$ es un 11-entero, y de hecho es una unidad en $\mathbb{Z}_{\langle 11\rangle}$. Como otro ejemplo, podemos tomar $m=50$ y $p=5$, en cuyo caso

$$B_{50}=\frac{5^2\cdot 417202699\cdot 47464429777438199}{2\cdot 3\cdot 11},$$

con lo cual, claramente se tiene que $\dfrac{B_{50}}{50}=\dfrac{417202699\cdot 47464429777438199}{2^2\cdot 3\cdot 11}\in\mathbb{Z}^*_{\langle 5\rangle}$.

El siguiente teorema, en el caso cuando $e=1$, es debido a Kummer. Esta es la razón de que esas congruencias sean conocidas hoy en día como congruencias de Kummer.

Teorema 2.2.1 (Congruencias de Kummer). *Supóngase que $m > 2$ es par, y sea p un número primo tal que $(p-1) \nmid m$. Definimos, para cada $k \in \mathbb{N}$, $C_k := (1-p^{k-1})B_k/k$. Entonces, si $n, e \in \mathbb{N}$, con $n \equiv m \bmod \phi(p^e)$, se tiene que $C_n \equiv C_m \bmod p^e$.*

Demostración: Escribimos, nuevamente, $B_m = U_m/V_m$, y sea $t = \operatorname{ord}_p(m)$. Por la proposición 2.2.3, $p^t \mid U_m$ y $p \nmid V_m$. En la congruencia (2.2.2), escogemos a tal que $p \nmid a$, y ponemos $n = p^{e+t}$, para obtener que

$$(a^m-1)U_m \equiv ma^{m-1}V_m \sum_{j=1}^{p^{e+t}-1} j^{m-1}\left[\frac{ja}{p^{e+t}}\right] \bmod p^{e+t};$$

como p^t divide tanto a m como a U_m, podemos entonces dividir toda la congruencia entre p^t, con lo cual resulta que

$$(a^m-1)\frac{U_m}{p^t} \equiv \frac{m}{p^t}a^{m-1}V_m \sum_{j=1}^{p^{e+t}-1} j^{m-1}\left[\frac{ja}{p^{e+t}}\right] \bmod p^e.$$

Puesto que $p \nmid V_m$ y $p \nmid (m/p^t)$, se tiene entonces que $(p, V_m m/p^t) = 1$. De ahí que podamos, dentro del anillo $\mathbb{Z}_{\langle p\rangle}$, dividir ambos lados de la congruencia entre $V_m m/p^t$, y como resultado tenemos que

$$\begin{aligned}\frac{(a^m-1)B_m}{m} = \frac{(a^m-1)U_m}{\frac{m}{p^t}V_m p^t} &\equiv \frac{m}{\frac{m}{p^t}V_m p^t}a^{m-1}V_m \sum_{j=1}^{p^{e+t}-1} j^{m-1}\left[\frac{ja}{p^{e+t}}\right] \bmod p^e \\ &\equiv a^{m-1}\sum_{j=1}^{p^{e+t}-1} j^{m-1}\left[\frac{ja}{p^{e+t}}\right] \bmod p^e. \qquad (2.2.3)\end{aligned}$$

Esta última expresión es la congruencia crucial, que nos llevará a la demostración completa del teorema. Demostremos primero que lo pedido se cumple cuando $e = 1$, pues este caso nos mostrará la idea principal que se utilizará en la demostración del caso general (idea que no es excesivamente complicada, pero que podría no ser del todo clara si se omite el paso previo para $e = 1$).
Así, si en la congruencia (2.2.3) suponemos que $e = 1$, obtenemos que

$$\frac{(a^m-1)B_m}{m} \equiv a^{m-1}\sum_{j=1}^{p^{t+1}-1} j^{m-1}\left[\frac{ja}{p^{t+1}}\right] \bmod p.$$

En el lado derecho de esta última congruencia, podemos omitir todos aquellos términos donde la j involucrada es divisible por p. Por otra parte, si $p \nmid j$, entonces

$j^{p-1} \equiv 1 \bmod p$, además de que, como $p \nmid a$, $a^{p-1} \equiv 1 \bmod p$. Así pues, módulo p, el lado derecho permanece sin cambio cuando sustituimos m por n, siempre que $n \equiv m \bmod (p-1)$. De ahí que

$$\frac{(a^m-1)B_m}{m} \equiv a^{n-1} \sum_{j=1}^{p^{t+1}-1} j^{n-1} \left[\frac{ja}{p^{t+1}}\right] \equiv \frac{(a^n-1)B_n}{n} \bmod p.$$

Si, debido al teorema 2.1.1, elegimos a como una raíz primitiva módulo p (con lo cual, como $n \equiv m \bmod (p-1)$, se tendrá que $a^n \equiv a^m \bmod p$) entonces, como $(p-1) \nmid m$, tendremos que $a^n - 1 \equiv a^m - 1 \not\equiv 0 \bmod p$; de modo que, de la congruencia de arriba, podemos concluir que $B_n/n \equiv B_m/m \bmod p$, que es el resultado deseado en el caso en el que $e = 1$ (pues en este caso, la congruencia que se desea demostrar, que originalmente sería $(1-p^{m-1})B_m/m \equiv (1-p^{n-1})B_n/n \bmod p$, se transforma simplemente en $B_n/n \equiv B_m/m \bmod p$, en virtud de que $p^{m-1} \equiv p^{n-1} \equiv 0 \bmod p$). Cuando $e > 1$, este procedimiento requiere una ligera modificación, pues no es tan fácil excluir los términos donde la j involucrada sea dividida por p. Sin embargo, se puede realizar una separación de la siguiente manera:

$$\begin{aligned}\sum_{j=1}^{p^{e+t}-1} j^{m-1}\left[\frac{ja}{p^{e+t}}\right] &= \sum_{\substack{j=1\\(p,j)=1}}^{p^{e+t}-1} j^{m-1}\left[\frac{ja}{p^{e+t}}\right] + \sum_{i=1}^{p^{e+t-1}-1} (ip)^{m-1}\left[\frac{(ip)a}{p^{e+t}}\right] \\ &= \sum_{\substack{j=1\\(p,j)=1}}^{p^{e+t}-1} j^{m-1}\left[\frac{ja}{p^{e+t}}\right] + p^{m-1}\sum_{i=1}^{p^{e+t-1}-1} i^{m-1}\left[\frac{ia}{p^{e+t-1}}\right].\end{aligned}$$

Si en la congruencia (2.2.3) cambiamos e por $e-1$, obtenemos

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

Como $m - 1 \geq 1$, podemos entonces multiplicar toda la congruencia por p^{m-1}, de modo que

$$\frac{p^{m-1}(a^m-1)B_m}{m} \equiv p^{m-1}a^{m-1} \sum_{i=1}^{p^{e+t-1}-1} i^{m-1}\left[\frac{ia}{p^{e+t-1}}\right] \bmod p^e.$$

Combinando esta congruencia con la separación en dos partes de la sumatoria, observaremos que

$$\begin{aligned}
\frac{(a^m-1)B_m}{m} &\equiv a^{m-1}\sum_{j=1}^{p^{e+t}-1} j^{m-1}\left[\frac{ja}{p^{e+t}}\right] \mod p^e \\
&\equiv a^{m-1}\sum_{\substack{j=1\\(p,j)=1}}^{p^{e+t}-1} j^{m-1}\left[\frac{ja}{p^{e+t}}\right] \\
&\quad +p^{m-1}a^{m-1}\sum_{i=1}^{p^{e+t-1}-1} i^{m-1}\left[\frac{ia}{p^{e+t-1}}\right] \mod p^e \\
&\equiv a^{m-1}\sum_{\substack{j=1\\(p,j)=1}}^{p^{e+t}-1} j^{m-1}\left[\frac{ja}{p^{e+t}}\right] + \frac{p^{m-1}(a^m-1)B_m}{m} \mod p^e.
\end{aligned}$$

En conclusión, hemos probado que

$$\frac{(1-p^{m-1})(a^m-1)B_m}{m} \equiv a^{m-1}\sum_{\substack{j=1\\(p,j)=1}}^{p^{e+t}-1} j^{m-1}\left[\frac{ja}{p^{e+t}}\right] \mod p^e.$$

Nuevamente, por el teorema 2.1.1, elegimos a de modo que sea una raíz primitiva módulo p. De esta forma, tenemos que $(a,p^e)=1$, de modo que $a^{\phi(p^e)} \equiv 1 \mod p^e$. Además, si $p \nmid j$, entonces también $(j,p^e)=1$ y por tanto $j^{\phi(p^e)} \equiv 1 \mod p^e$. De esta forma, si $n \in \mathbb{N}$ es tal que $n \equiv m \mod \phi(p^e)$, entonces $j^{n-1} \equiv j^{m-1} \mod p^e$ y $a^{n-1} \equiv a^{m-1} \mod p^e$. Así, podemos intercambiar n con m en el lado derecho de la congruencia anterior, para obtener que

$$\begin{aligned}
\frac{(1-p^{m-1})(a^m-1)B_m}{m} &\equiv a^{n-1}\sum_{\substack{j=1\\(p,j)=1}}^{p^{e+t}-1} j^{n-1}\left[\frac{ja}{p^{e+t}}\right] \\
&\equiv \frac{(1-p^{n-1})(a^n-1)B_n}{n} \mod p^e.
\end{aligned}$$

Como $(p-1) \nmid m$, se tiene entonces que $a^m \not\equiv 1 \mod p$, de modo que $(p, a^m-1)=1$. De este modo, $(p^e, a^m-1)=1$. Además, dado que $n \equiv m \mod \phi(p^e)$, podemos ver que $a^m-1 \equiv a^n-1 \mod p^e$. Es por esto que podemos dividir cada uno de los extremos de la congruencia de arriba entre estas últimas respectivas cantidades, obteniendo así el resultado deseado. □

Estas congruencias de Kummer pueden ser interpretadas de la siguiente manera: sea p un número primo fijo, y definimos la siguiente función de variable compleja:

$$\begin{aligned} \zeta^* : \mathbb{C} &\longrightarrow \mathbb{C} \\ s &\longmapsto (1-p^{-s})\zeta(s). \end{aligned}$$

Esta función recibe el nombre de **función zeta p-ádica**. Entonces, por el teorema 1.4.3, tendremos que, para $m \in \mathbb{N}\backslash\{1\}$, $\zeta^*(1-m) = (1-p^{-(1-m)})\zeta(1-m) = -(1-p^{m-1})B_m/m \in \mathbb{Q}$. De esta forma, el teorema 2.2.1 nos dice exactamente que, si $m, n \in \mathbb{N}\backslash\{1,2\}$, con $n \equiv m \bmod \phi(p^e)$ y $(p-1) \nmid m$, entonces se tendrá que $\zeta^*(1-m) \equiv \zeta^*(1-n) \bmod p^e$.

Ahora bien, se tiene que la función $d : \mathbb{Q} \times \mathbb{Q} \to \mathbb{R}^+ \cup \{0\}$ dada por $d(n,m) := p^{-\mathrm{ord}_p\,(n-m)}$ define una métrica en $\mathbb{Q}$, denominada **métrica p-ádica**. En esta métrica, dos números racionales están cerca si su diferencia es divisible por una potencia elevada de p. Lo discutido anteriormente puede interpretarse, de manera informal, como sigue: si $n, m \in \mathbb{N}\backslash\{1,2\}$, con $n \equiv m \bmod (p-1)$, $(p-1) \nmid m$, y n y m están cerca p-ádicamente, entonces $\zeta^*(1-m)$ y $\zeta^*(1-n)$ están cerca p-ádicamente. Más precisamente, tomemos un $\varepsilon > 0$ arbitrario. Entonces, es posible escoger un $e \in \mathbb{N}$ tal que $\varepsilon > p^{-e}$, y tomamos $\delta = p^{2-e} > 0$. Supóngase que $n, m \in \mathbb{N}\backslash\{1\}$, con $n \equiv m \bmod (p-1)$ y $d(n,m) < \delta$. Esto significa que $p^{-\mathrm{ord}_p\,(n-m)} < p^{2-e} \Rightarrow -\mathrm{ord}_p\,(n-m) < 2-e \Rightarrow \mathrm{ord}_p\,(n-m) > e-2 \Rightarrow \mathrm{ord}_p\,(n-m) \geq e-1 \Rightarrow p^{e-1} \mid (n-m)$. Como además supusimos que $n \equiv m \bmod (p-1)$, entonces $(p-1) \mid (n-m)$, y, dado que obviamente $(p^{e-1}, p-1) = 1$, se tiene entonces que $\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1) \mid (n-m)$. En otras palabras, se tiene que $n \equiv m \bmod \phi(p^e)$. Por lo discutido anteriormente, sabemos que esto último implica que $\zeta^*(1-n) \equiv \zeta^*(1-m) \bmod p^e$, es decir, que $\mathrm{ord}_p\,(\zeta^*(1-n)-\zeta^*(1-m)) \geq e \Rightarrow -\mathrm{ord}_p\,(\zeta^*(1-n)-\zeta^*(1-m)) \leq -e$, de donde podemos ver que $d(\zeta^*(1-n), \zeta^*(1-m)) = p^{-\mathrm{ord}_p\,(\zeta^*(1-n)-\zeta^*(1-m))} \leq p^{-e} < \varepsilon$.

Con base en estas ideas, se han realizado extensiones de la función ζ^* al anillo de los enteros p-ádicos $\mathbb{Z}_p$, que es la completación del espacio métrico $(\mathbb{Z}, d|_{\mathbb{Z}\times\mathbb{Z}})$, y se han investigado las propiedades de estas funciones zeta p-ádicas. Posteriormente, Kenkichi Iwasawa (1917-1998) observó que las propiedades de estas funciones zeta p-ádicas se relacionan estrechamente con la estructura de los grupos de clases de campos ciclotómicos. De esta forma, las congruencias de Kummer resultan ser de gran importancia, y tienen interesantes consecuencias.

2.3. Números primos regulares e irregulares

Definición 2.3.1. *Un número primo impar $p \in \mathbb{Z}$, $p > 3$, se dice que es **regular** si p no divide a ninguno de los numeradores $U_2, U_4, \ldots, U_{p-3}$ de los correspondientes*

números de Bernoulli. Si p no es regular, se dice que es ***irregular****. El número primo* 3 *es regular por definición.*

La noción de número primo regular fue introducida por Kummer, como resultado de su empeño por demostrar el último teorema de Fermat. Notemos que, de acuerdo con el corolario 2.1.1, podemos ver que, dado un número primo p, se tiene que $(p-1) \nmid 2, 4, \ldots, (p-3)$, y en consecuencia $B_2, B_4, \ldots, B_{p-3}$ son p-enteros. Así, cuando $1 \leq i \leq (p-3)/2$, se cumple que $\text{ord}_p\ B_{2i} \geq 0$, con lo cual la regularidad de p equivale a que $\text{ord}_p\ B_{2i} = 0,\ \forall\ 1 \leq i \leq (p-3)/2$. Asimismo, como es fácil ver, las unidades en $\mathbb{Z}_{\langle p \rangle}$ son exactamente aquellos elementos $x \in \mathbb{Z}_{\langle p \rangle}$ tales que $\text{ord}_p\ (x) = 0$; en consecuencia, tenemos que p es regular $\iff B_2, B_4, \ldots, B_{p-3} \in \mathbb{Z}^*_{\langle p \rangle}$. O bien, de manera equivalente, p es irregular $\iff$ para algún $1 \leq i \leq (p-3)/2$, se tiene que $B_{2i} \in \mathbb{Z}_{\langle p \rangle} \backslash \mathbb{Z}^*_{\langle p \rangle}$. Los dos primeros números primos irregulares son 37 y 59, pues $\text{ord}_{37}\ (B_{32}) = 1$ y $\text{ord}_{59}\ (B_{44}) = 1$. Después de ellos, son también números primos irregulares $67, 101, 103, 131, 149$ y 157. En 1915, Johan Ludwig William Valdemar Jensen (1859-1925) demostró que existe una infinidad de números primos irregulares de la forma $4n + 3$.

Enseguida demostraremos que existe una infinidad de números primos irregulares. La demostración se debe a Leonard Carlitz (1907-1999). No ha sido aún demostrado resultado alguno acerca de la infinitud o finitud del conjunto de números primos regulares.

Teorema 2.3.1. *El conjunto de números primos irregulares es infinito.*

Demostración: Sea $P = \{p_1, \ldots, p_s\}$ un conjunto finito de números primos irregulares. Demostraremos que siempre podemos encontrar un número primo irregular $p \notin P$. Tomemos un número par $k \geq 2$, y sea $n := k(p_1 - 1) \cdots (p_s - 1)$. En caso de que $P = \emptyset$, se toma simplemente $n := k$. Por la proposición 1.4.1, parte (ii), podemos elegir una k suficientemente grande para que $|B_n/n| > 1$. Debido a esta desigualdad, es posible elegir un número primo p que satisfaga que $\text{ord}_p\ (B_n/n) > 0$. En consecuencia, y dado que $n \in \mathbb{Z}$, se tiene que $\text{ord}_p\ (B_n) - \text{ord}_p\ (n) > 0 \Rightarrow \text{ord}_p\ (B_n) > \text{ord}_p\ (n) \geq 0$, con lo cual B_n es un p-entero. Por el teorema de Clausen-von Staudt, teorema 2.1.2, esto implica que $(p-1) \nmid n$, de modo que $p \neq p_i$, para cualquier $1 \leq i \leq s$. Es decir, $p \notin P$. Además, es claro que $p \neq 2$. A continuación, demostraremos que p es irregular.
Como $(p-1) \nmid n$, entonces podemos escoger m tal que $n \equiv m \mod (p-1)$ con $0 \leq m < p-1$, de modo que m es par y $m \neq 0$, de donde se sigue que $2 \leq m \leq p-3$. Por la congruencia de Kummer (teorema 2.2.1), tenemos que $(1 - p^{n-1})B_n/n \equiv (1 - p^{m-1})B_m/m \mod p$. Siendo $n \equiv m \mod (p-1)$, se tiene que

$p^{n-1} \equiv p^{m-1} \bmod p$, por lo cual $(1-p^{n-1})B_n/n \equiv (1-p^{n-1})B_m/m \bmod p$. Además, es claro que $p \nmid (1-p^{n-1})$, así que podemos dividir la congruencia entre $1-p^{n-1}$ y obtener $B_n/n \equiv B_m/m \bmod p$. Esto significa que $\operatorname{ord}_p\,(B_n/n - B_m/m) > 0$. Por otra parte, dado que también $\operatorname{ord}_p\,(B_n/n) > 0$, podemos ver entonces que

$$\begin{aligned} \operatorname{ord}_p\left(\frac{B_m}{m}\right) &= \operatorname{ord}_p\left(\frac{B_n}{n} - \left(\frac{B_n}{n} - \frac{B_m}{m}\right)\right) \\ &\geq \min\left\{\operatorname{ord}_p\left(\frac{B_n}{n}\right), \operatorname{ord}_p\left(\frac{B_n}{n} - \frac{B_m}{m}\right)\right\} > 0. \end{aligned}$$

Es decir, que $\operatorname{ord}_p\,(B_m) \geq \operatorname{ord}_p\,(B_m/m) > 0$. Siendo m igual a alguno de los números $2, 4, \ldots, p-3$, se sigue de ahí que p es un número primo irregular. □

A continuación, intentaremos averiguar cuál es la proporción de números primos regulares dentro del conjunto de números primos. Para tal fin, introduciremos algunas nociones de probabilidad, en particular la noción de distribución binomial y de distribución Poisson. Con la ayuda de estos conceptos, será posible observar que, dado un número primo aleatorio, la probabilidad de que sea regular se aproxima más y más a $1/\sqrt{e} \approx 0.61 \geq 1/2$, entre más grande sea el número primo en cuestión. En otras palabras, uno esperaría que la cantidad de números primos regulares sea mayor que la de números primos irregulares. Sin embargo, tal cálculo probabilístico no es del todo riguroso (pues introduce una suposición que, aunque plausible, no parece ser demostrable), y es por ello por lo que, en lugar de teorema, se le da el nombre de "argumento heurístico".

Denotaremos por $\mathcal{P}(E)$ a la probabilidad de que ocurra un evento E cualquiera. A continuación, introducimos uno de los conceptos primordiales en probabilidad, el de variable aleatoria. Una **variable aleatoria**, de una manera informal, refiere a una función que, de alguna manera, depende "del azar". Así por ejemplo, al lanzar un par de dados, el número resultante puede expresarse por medio de una variable aleatoria X que tome valores entre 2 y 12, es decir, $2 \leq X \leq 12$. En general, se utilizan variables aleatorias que toman valores reales, es decir que $X \in \mathbb{R}$, y para un número $x \in \mathbb{R}$, se denota la probabilidad de que la variable aleatoria X tome el valor x por $\mathcal{P}(X = x)$. Asimismo, toda función $f : \mathbb{R} \to [0, 1]$ tal que para cada $x \in \mathbb{R}$, se tenga que $f(x) = \mathcal{P}(X = x)$ para alguna variable aleatoria fija X, se llama **función de distribución**. Obsérvese que, en el caso en el que la variable aleatoria X sólo pueda tomar los valores $x_1, \ldots, x_n$ (en cuyo caso X es llamada **variable aleatoria finita**), entonces se debe de tener que $\displaystyle\sum_{k=1}^{n} f(x_k) = \sum_{k=1}^{n} \mathcal{P}(X = x_k) = 1$.

Definición 2.3.2. *Sea X una variable aleatoria. Decimos que X tiene* ***distribución Bernoulli*** *si X toma únicamente dos valores.*

Si X es una variable aleatoria que tiene distribución Bernoulli, y los valores que puede tomar son a y b, entonces la variable aleatoria $X' := \dfrac{X-a}{b-a}$ también tiene distribución Bernoulli, y los únicos valores que toma son 0 y 1. De esta forma, para cualquier variable aleatoria con distribución Bernoulli es posible suponer que toma los valores 0 y 1. Además, si X es una variable aleatoria con distribución Bernoulli, y se conoce $\mathcal{P}(X = 1) =: \alpha$, entonces necesariamente se tendrá que $\mathcal{P}(X = 0) = 1 - \mathcal{P}(X = 1) = 1 - \alpha$. Al número α se le conoce como el **parámetro** de la distribución Bernoulli en cuestión, y por lo anterior, resulta que conociendo este número se puede conocer completamente la función de distribución f correspondiente a esta variable aleatoria, la cual viene dada por:

$$f(x) = \begin{cases} \alpha; & x = 1 \\ 1-\alpha; & x = 0 \\ 0; & \text{cualquier otro caso.} \end{cases}$$

Teorema 2.3.2. *Sean n variables aleatorias $X_1, \ldots, X_n$, independientes todas ellas entre sí (en el sentido de que el valor que tome cualquiera de ellas no afecta al valor de cualquiera de las otras) con distribución Bernoulli y parámetro α igual para todas ellas. Entonces, se tiene que la variable $X = X_1 + \cdots + X_n$ puede tomar los valores $0, 1, \ldots, n$, y más aún, para cada $k \in \mathbb{Z},\ 0 \leq k \leq n$, se tiene que*

$$\mathcal{P}(X = k) = \binom{n}{k} \alpha^k (1-\alpha)^{n-k}.$$

Demostración: La primera afirmación es obvia, enseguida probaremos la segunda. Primero que nada, obsérvese que, de ser cierta dicha afirmación, tendríamos que

$$\sum_{k=0}^{n} \mathcal{P}(X = k) = \sum_{k=0}^{n} \binom{n}{k} \alpha^k (1-\alpha)^{n-k} = \big(\alpha + (1-\alpha)\big)^n = 1$$

que es tal y como debe de ocurrir si las probabilidades están bien calculadas. Observemos ahora que, para que se tenga que $X = k$, se debe de tener que exactamente k de las variables $X_1, \ldots, X_n$ tomen el valor 1, tomando las restantes $n - k$ el valor 0. Hay exactamente $\binom{n}{k}$ posibles combinaciones de valores en las n variables, que satisfacen esta condición. Ahora bien, la probabilidad de que ocurra cada una de estas combinaciones es el producto de las probabilidades de que cada una de las

variables X_k tomen el valor correspondiente, es decir, el resultado de multiplicar k veces el número $\mathcal{P}(X_k = 1) = \alpha$, y $n - k$ veces el número $\mathcal{P}(X_k = 0) = 1 - \alpha$. De manera que la probabilidad $\mathcal{P}(X = k)$ resulta ser el resultado de sumar $\binom{n}{k}$ veces el número $\alpha^k(1-\alpha)^{n-k}$. □

La función de distribución f_n correspondiente a la variable X del teorema 2.3.2, vendrá entonces dada por:

$$f_n(x) = \begin{cases} \binom{n}{x}\alpha^x(1-\alpha)^{n-x}; & x \in \{0, 1, \ldots, n\} \\ 0; & \text{otro caso.} \end{cases}$$

Esta función de distribución recibe el nombre de **distribución binomial**, con parámetro α.

Observemos qué ocurre con este tipo de distribuciones binomiales cuando se hace tender n a infinito, si el parámetro α depende de n. Cuando $x \notin \mathbb{N} \cup \{0\}$, entonces se tendrá que $f_n(x) = 0, \ \forall\, n \in \mathbb{N}$; mientras que, en el caso contrario, si $x \in \mathbb{N} \cup \{0\}$, entonces a partir de cierto momento se tendrá que $x \leq n$. De ahí en adelante, se tendrá que:

$$\begin{aligned} f_n(x) &= \binom{n}{x}\alpha_n^x(1-\alpha_n)^{n-x} = \binom{n}{x}\left(\frac{z_n}{n}\right)^x\left(1-\frac{z_n}{n}\right)^{n-x} \\ &= \left(\frac{n!}{x!(n-x)!}\right)\left(\frac{z_n^x}{n^x}\right)\left(1-\frac{z_n}{n}\right)^n\left(1-\frac{z_n}{n}\right)^{-x} \\ &= \left(\frac{z_n^x}{x!}\right)\left(\frac{(n-1)!}{(n-x)!n^{x-1}}\right)\left(1-\frac{z_n}{n}\right)^n\left(1-\frac{z_n}{n}\right)^{-x}, \end{aligned} \tag{2.3.1}$$

en donde $z_n := n\alpha_n$. Ahora bien, por otra parte, se tiene que

$$\begin{aligned} \frac{(n-1)!}{(n-x)!n^{x-1}} &= \frac{(n-1)(n-2)\cdots(n-x+1)}{n^{x-1}} \\ &= \left(\frac{n-1}{n}\right)\left(\frac{n-2}{n}\right)\cdots\left(\frac{n-(x-1)}{n}\right) \\ &= \prod_{k=1}^{x-1}\left(\frac{n-k}{n}\right) = \prod_{k=1}^{x-1}\left(1-\frac{k}{n}\right). \end{aligned}$$

Esto, junto con la ecuación (2.3.1), da como resultado lo siguiente:

$$f_n(x) = \left(\frac{z_n^x}{x!}\right)\left(1-\frac{z_n}{n}\right)^n\left(1-\frac{z_n}{n}\right)^{-x}\prod_{k=1}^{x-1}\left(1-\frac{k}{n}\right). \tag{2.3.2}$$

Si suponemos que $\lim\limits_{n\to\infty} z_n = z$, entonces se tendrá que, mientras que $n \to \infty$, $\dfrac{z_n^x}{x!} \longrightarrow \dfrac{z^x}{x!}$. Por otra parte, $\left(1-\dfrac{z_n}{n}\right)^{-x} \longrightarrow \left(1-\dfrac{z}{n}\right)^{-x} \longrightarrow (1)^{-x} = 1$, además de que $\displaystyle\prod_{k=1}^{x-1}\left(1-\frac{k}{n}\right) \longrightarrow \prod_{k=1}^{x-1}(1) = 1$. Por si todo lo anterior no fuera poco, se tiene además que $\left(1-\dfrac{z_n}{n}\right)^n \longrightarrow \left(1-\dfrac{z}{n}\right)^n \longrightarrow e^{-z}$. De estos cuatro límites, junto con la ecuación (2.3.2), podemos concluir que

$$f(x) := \lim_{n\to\infty} f_n(x) = \begin{cases} \dfrac{z^x}{x!}e^{-z}; & x \in \mathbb{N}\cup\{0\} \\ 0; & \text{otro caso.} \end{cases} \tag{2.3.3}$$

Esta nueva función f, resulta ser también una función de distribución para una variable aleatoria X que puede tomar valores en $\mathbb{N}\cup\{0\}$, ya que

$$\sum_{k=0}^{\infty} f(k) = \sum_{k=0}^{\infty}\frac{z^k}{k!}e^{-z} = e^{-z}\sum_{k=0}^{\infty}\frac{z^k}{k!} = e^{-z}\cdot e^z = 1.$$

Esta distribución recibe el nombre de **distribución Poisson**, con parámetro $z = \lim\limits_{n\to\infty} z_n = \lim\limits_{n\to\infty} n\alpha_n$.

Con todo lo anterior, tenemos ya, en materia de probabilidad, las herramientas necesarias para llevar a cabo nuestra investigación acerca de los números primos regulares, misma que desarrollamos a continuación.

Definición 2.3.3. *Si p es un número primo, entonces se define el* ***índice de irregularidad de*** *p, denotado por $i(p)$, como*

$$i(p) := \#\{U_k \big| k \in \{2,4,\ldots,p-3\},\ p \mid U_k\}.$$

Bajo esta definición, se tiene que, si p es un número primo, entonces p es regular $\iff$ $i(p) = 0$. Ahora bien, si dado un número primo p suponemos (lo cual no se encuentra rigurosamente demostrado, si bien es plausible) que los números U_k se encuentran aleatoriamente distribuidos módulo p, es decir, que para cada $0 \le j < p$, se tiene que $\mathcal{P}(U_k \equiv j \bmod p) = 1/p$, entonces podemos llegar a estimar de manera bastante precisa la probabilidad de que p sea un número primo regular. En efecto,

de la suposición asumida, se tiene que en particular $\mathcal{P}(p \mid U_k) = 1/p$. Sea X_k la variable aleatoria que toma el valor 1 cuando $p \mid U_k$, y el valor 0 en caso contrario. Entonces, es fácil ver que $i(p) = X_2 + X_4 + \cdots + X_{p-3}$.

Teorema 2.3.3. *Supóngase que los numeradores de los números de Bernoulli se encuentran aleatoriamente distribuidos módulo cualquier número primo p. Entonces, se tiene que*

$$\lim_{p\to\infty} \mathcal{P}(p \text{ es regular}) = \frac{1}{\sqrt{e}} \approx 0.61.$$

Demostración: Sea p un número primo, y sean las $(p-3)/2$ variables aleatorias X_k, con $k \in \{2, 4, \ldots, p-3\}$, como en la discusión de arriba. Por la suposición, tenemos que, para cada $k \in \{2, 4, \ldots, p-3\}$, $\mathcal{P}(X_k = 1) = 1/p$. Debido al teorema 2.3.2, se observa que, para cada $k \in \{2, 4, \ldots, p-3\}$,

$$\mathcal{P}(i(p) = k) = \binom{\frac{p-3}{2}}{k} \left(\frac{1}{p}\right)^k \left(1 - \frac{1}{p}\right)^{\frac{1}{2}(p-3)-k},$$

que es la distribución binomial con parámetro $\alpha_n = 1/p$ para $n = (p-3)/2$ variables aleatorias independientes con distribución Bernoulli. Entonces, $z_n = n\alpha_n = \left(\frac{p-3}{2}\right)\left(\frac{1}{p}\right) = 1/2 - 3/(2p) \longrightarrow 1/2 = z$ cuando $n \longrightarrow \infty$, que es lo mismo que decir cuando $p \longrightarrow \infty$. Esto indica que es posible considerar el límite $\lim_{p\to\infty} \mathcal{P}(i(p) = k)$, el cual vendrá dado por la distribución Poisson que aparece en la ecuación (2.3.3), con parámetro $z = 1/2$:

$$\lim_{p\to\infty} \mathcal{P}(i(p) = k) = \frac{(1/2)^k}{k!} e^{-1/2}, \quad \forall\ k \in \mathbb{N} \cup \{0\}.$$

En particular, se tiene que

$$\lim_{p\to\infty} \mathcal{P}(i(p) = 0) = e^{-\frac{1}{2}},$$

que es exactamente lo que se tenía que probar. □

El resultado anterior se debe a Carl Ludwig Siegel (1896-1981). La idea principal de dicho resultado radica en que aproximadamente el 61 % de los números primos deberían ser regulares. Pese a que no se ha podido probar resultado alguno acerca de la finitud o infinitud de los números primos regulares, este último resultado junto con el teorema 2.3.1 nos hace sospechar que la cantidad de números primos regulares es infinita, si bien el argumento anterior dista mucho de ser una prueba rigurosa.

Capítulo 3

El último teorema de Fermat

Otro importante problema cuya solución, al menos parcialmente, se encuentra estrechamente relacionada con los números de Bernoulli, es el famoso último teorema de Fermat. El resultado principal del presente capítulo es un caso particular de este teorema. Pese a que actualmente el último teorema de Fermat está demostrado, el caso particular que aquí se desarrolla tiene una gran importancia histórica, pues durante mucho tiempo constituyó el mayor avance disponible en la demostración de este teorema. Las dos primeras secciones construyen la teoría y los lemas necesarios para demostrar el caso particular en cuestión. La tercera sección prepara el camino para mostrar, en la cuarta sección, la relación existente entre el resultado principal de este capítulo y los números de Bernoulli. Finalmente, en la quinta y última sección, se establece el resultado principal.

3.1. El campo $\mathbb{Q}(\zeta_n)$ y el anillo $\mathbb{Z}[\zeta_n]$

En esta sección haremos un recordatorio de los conceptos y resultados fundamentales de los campos ciclotómicos, así como de los anillos de enteros ciclotómicos.

Sea $n \in \mathbb{N}$. Una **raíz n-ésima de la unidad en** $\mathbb{C}$ es un número complejo ζ tal que $\zeta^n = 1$. El conjunto de las raíces n-ésimas de la unidad es un subgrupo finito con n elementos del grupo multiplicativo $\mathbb{C}^*$, y además es grupo cíclico; cualquier generador de este grupo cíclico se denomina **raíz n-ésima primitiva de la unidad**, y cualquiera de estas es denotada por ζ_n, o simplemente por ζ si no existe riesgo de confusión con respecto a n. Por ejemplo, $e^{2\pi i/n}$ es una raíz n-ésima primitiva de la unidad.

La cantidad de generadores del grupo multiplicativo de las raíces n-ésimas de la unidad es $\phi(n)$, donde ϕ es la función de Euler, y, si tenemos una de ellas, ζ_n, entonces

las raíces n-ésimas primitivas de la unidad serán los números ζ_n^i, con $1 \leq i \leq n$ y $(i,n) = 1$.

Definición 3.1.1. *Si $n \in \mathbb{N}$, se define el n-**ésimo campo ciclotómico sobre** $\mathbb{Q}$ como el mínimo subcampo de $\mathbb{C}$ que contiene a ζ_n, es decir, $\mathbb{Q}(\zeta_n)$.*

Se tiene que la extensión de campos $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ es una extensión de Galois de grado $|\mathrm{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = \phi(n)$ cuyo grupo de Galois es isomorfo al grupo multiplicativo de las unidades módulo n, es decir, a $(\mathbb{Z}/n\mathbb{Z})^*$. De manera más precisa, el grupo de Galois de la extensión $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ está determinado por todos los automorfismos σ de $\mathbb{Q}(\zeta_n)$ tales que $\sigma(\zeta_n) = \zeta_n^i$, con $1 \leq i \leq n$ y $(i,n) = 1$. De este modo, los $\sigma \in \mathrm{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ están en correspondencia biunívoca con los i tales que $1 \leq i \leq n$, $(i,n) = 1$; además, tal correspondencia preserva la operación de grupo, por consiguiente, $\mathrm{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$. Por otra parte, el conjunto $\left\{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{\phi(n)-1}\right\}$ resulta ser una base de la extensión $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Por lo tanto, el polinomio irreducible de ζ_n sobre $\mathbb{Q}$ es un polinomio mónico irreducible sobre $\mathbb{Q}[X]$ de grado $\phi(n)$; este polinomio es llamado el **n-ésimo polinomio ciclotómico sobre** $\mathbb{Q}$ y es denotado por $\Phi_n(X)$, o simplemente por Φ_n. En consecuencia, tenemos que

$$\mathbb{Q}(\zeta_n) \cong \frac{\mathbb{Q}[X]}{\langle \Phi_n(X) \rangle} \ .$$

En particular, si p es un número primo, tenemos que el grado de la extensión $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ es $\phi(p) = p - 1$. Por consiguiente, $\left\{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}\right\}$ es base de $\mathbb{Q}(\zeta_p)$ sobre $\mathbb{Q}$, y $\mathrm{Gal}\,(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{F}_p^*$, en donde $\mathbb{F}_p$ es el campo finito de p elementos. Además, el p-ésimo polinomio ciclotómico sobre $\mathbb{Q}$ viene dado por $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$. Notemos que si $p = 2$, entonces $\zeta_2 = -1$, $\Phi_2(X) = X + 1$ y $\mathbb{Q}(\zeta_2) = \mathbb{Q}$. Es por ello por lo que, de ahora en adelante, supondremos que p es un número primo impar.

Proposición 3.1.1. *Sean $n, m \in \mathbb{N}$ tales que $(m,n) = 1$. Entonces, $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{mn})$ y $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.*

Demostración: Para probar la primera afirmación, notemos que ζ_{mn}^n es una raíz m-ésima primitiva de la unidad, por lo cual $\zeta_m \in \mathbb{Q}(\zeta_{mn})$. Similarmente, tenemos que $\zeta_n \in \mathbb{Q}(\zeta_{mn})$. Por tanto, se tiene que $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_{mn})$ y que $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_{mn})$, lo cual implica que $\mathbb{Q}(\zeta_m, \zeta_n) \subseteq \mathbb{Q}(\zeta_{mn})$. Pero, por otra parte, dado que $(n,m) = 1$, se tiene que $\zeta_m\zeta_n$ es una raíz mn-ésima primitiva de la unidad, por lo cual $\zeta_{mn} \in \mathbb{Q}(\zeta_m, \zeta_n)$. Por ello, $\mathbb{Q}(\zeta_{mn}) \subseteq \mathbb{Q}(\zeta_m, \zeta_n)$, de donde se concluye que $\mathbb{Q}(\zeta_{mn}) = \mathbb{Q}(\zeta_m, \zeta_n)$.

Pasemos ahora a la segunda afirmación. Comencemos por observar que, dado que $(n, m) = 1$, se tiene que $[\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}] = \phi(mn) = \phi(m)\phi(n)$, lo cual implica que $[\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}(\zeta_n)] = \dfrac{[\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_n) : \mathbb{Q}]} = \dfrac{\phi(m)\phi(n)}{\phi(n)} = \phi(m)$. Además, se tiene que $\mathrm{Gal}\left(\mathbb{Q}(\zeta_m)/(\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n))\right) \cong \mathrm{Gal}\left(\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_n)\right)$, de modo que, por la Teoría de Galois, necesariamente se tiene que $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$. □

Corolario 3.1.1. *Sea p un número primo impar. Entonces, las únicas raíces de la unidad no triviales contenidas en $\mathbb{Q}(\zeta_p)$ son $\pm\zeta_p^t$, con $1 \leq t < p$.*

Demostración: Sea $\lambda \in \mathbb{Q}(\zeta_p)$ una raíz de la unidad no trivial, y m su orden multiplicativo, es decir, λ es una raíz m-ésima primitiva de la unidad. En consecuencia, escribimos $\zeta_m = \lambda$. Entonces, tenemos que $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_p)$, con lo cual $\phi(m) \mid \phi(p) = p - 1$. Si $p \nmid m$ entonces, por la proposición 3.1.1, tendremos que $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$, de modo que $\zeta_m \notin \mathbb{Q}(\zeta_p)$, lo cual es absurdo. Luego, se tiene que necesariamente $p \mid m$, con $\phi(m) \mid \phi(p) = p - 1$. Expresando $m = p^l k$ con $l, k \in \mathbb{N}$, $(k, p) = 1$, tenemos que $\phi(m) = \phi(p^l)\phi(k) = p^{l-1}(p-1)\phi(k)$. Dado que $\phi(m) \mid (p-1)$, entonces necesariamente se tiene que $l = 1$ y que $\phi(k) = 1$. Sin embargo, $\phi(k) = 1 \iff k = 1$ o $k = 2$. Si $k = 1$ entonces tenemos que $m = p$ y, por lo tanto, $\zeta_m = \zeta_p^t$ para algún $1 \leq t < p$. Mientras que si $k = 2$, entonces $m = 2p$ y, por consiguiente, $\zeta_m = -\zeta_p^t$ para algún $1 \leq t < p$. □

Definición 3.1.2. *Si $n \in \mathbb{N}$, se define el n-**ésimo anillo de enteros ciclotómico sobre** $\mathbb{Z}$ como el mínimo subanillo de $\mathbb{C}$ que contiene a ζ_n, es decir, $\mathbb{Z}[\zeta_n]$.*

Es posible demostrar que el n-ésimo polinomio ciclotómico Φ_n es un polinomio con coeficientes en $\mathbb{Z}$ el cual es irreducible sobre $\mathbb{Z}[X]$, por lo tanto, se tiene que

$$\frac{\mathbb{Z}[X]}{\langle \Phi_n(X) \rangle} \cong \mathbb{Z}[\zeta_n].$$

Además, notemos que $\mathbb{Z}[\zeta_n]$ resulta ser un $\mathbb{Z}$-módulo, teniendo como una $\mathbb{Z}$-base al conjunto $\left\{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{\phi(n)-1}\right\}$. Por lo tanto, cualquier subconjunto no vacío de $\left\{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{\phi(n)-1}\right\}$ debe de ser un conjunto $\mathbb{Z}$-linealmente independiente de $\mathbb{Z}[\zeta_n]$. Por otra parte, es claro que

$$\mathbb{Q} \cap \mathbb{Z}[\zeta_n] = \mathbb{Z}.$$

Definición 3.1.3. *Sea $\alpha \in \mathbb{Q}(\zeta_n)$. Entonces, un **conjugado** de α es cualquier elemento del conjunto $\{\sigma(\alpha) \big| \sigma \in \mathrm{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{Q})\}$. En otras palabras, un conjugado de α es cualquier raíz del polinomio irreducible de α sobre $\mathbb{Q}$.*

Proposición 3.1.2. *Sean $n \in \mathbb{N}$ y $G = \mathrm{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Entonces, se cumple lo siguiente:*

(*i*) *Si $\sigma \in G$, entonces σ restringido al anillo $\mathbb{Z}[\zeta_n]$ determina un automorfismo de $\mathbb{Z}[\zeta_n]$.*

(*ii*) *Si $\alpha \in \mathbb{Z}[\zeta_n]$ y $f(X) = \mathrm{irr}\,(\alpha, \mathbb{Q})$, entonces $f(X) \in \mathbb{Z}[X]$.*

Demostración:

(*i*) Notemos que cada elemento α en el anillo $\mathbb{Z}[\zeta_n]$ es de la forma $h(\zeta_n)$, con $h(X) \in \mathbb{Z}[X]$ y, por otro lado, cada elemento $\sigma \in G$ está completamente determinado por su acción sobre ζ_n. Por lo tanto, si $\sigma(\zeta_n) = \zeta_n^i$, con $1 \leq i < n$ y $(i, n) = 1$, entonces $\sigma(\alpha) = h(\sigma(\zeta_n)) = h(\zeta_n^i) \in \mathbb{Z}[\zeta_n]$. Es decir, se tiene que $\sigma(\mathbb{Z}[\zeta_n]) \subseteq \mathbb{Z}[\zeta_n]$. De esta forma, la función $\sigma|_{\mathbb{Z}[\zeta_n]} : \mathbb{Z}[\zeta_n] \to \mathbb{Z}[\zeta_n]$ es un endomorfismo que además es monomorfismo.

Sea $\beta = g(\zeta_n) \in \mathbb{Z}[\zeta_n]$, con $g(X) \in \mathbb{Z}[X]$. Dado que $(i, n) = 1$, entonces es posible escoger un j tal que $ij \equiv 1 \bmod n$, de modo que $\zeta_n^{ij} = \zeta_n$. Tomemos $\gamma := g(\zeta_n^j) \in \mathbb{Z}[\zeta_n]$. Entonces, $\sigma(\gamma) = g(\sigma(\zeta_n^j)) = g(\zeta_n^{ji}) = g(\zeta_n) = \beta$. En consecuencia, $\sigma_{\mathbb{Z}[\zeta_n]} : \mathbb{Z}[\zeta_n] \to \mathbb{Z}[\zeta_n]$ es un epimorfismo. Es por ello que σ restringido al anillo $\mathbb{Z}[\zeta_n]$ es un automorfismo de $\mathbb{Z}[\zeta_n]$.

(*ii*) Sean $\alpha_1, \ldots, \alpha_m \in \mathbb{Q}(\zeta_n)$ exactamente todos los conjugados de α, con $\alpha_1 = \alpha$. Puesto que para cada $1 \leq j \leq m$ existe $\sigma \in G$ tal que $\sigma(\alpha) = \alpha_j$, y dado que $\alpha \in \mathbb{Z}[\zeta_n]$, entonces, por la parte (i) de la presente proposición, se tiene que $\alpha_j \in \mathbb{Z}[\zeta_n], \quad \forall\ 1 \leq j \leq m$. Por lo tanto, $f(X) = (X - \alpha_1) \cdots (X - \alpha_m) \in \mathbb{Q}[X] \cap \mathbb{Z}[\zeta_n][X] = (\mathbb{Q} \cap \mathbb{Z}[\zeta_n])[X] = \mathbb{Z}[X]$.

□

Definición 3.1.4. *Sea E/F una extensión finita de Galois, con $G := \mathrm{Gal}\,(E/F)$.*

(*i*) *Se define la **norma de E sobre F** como la función $N_{E/F} : E \to F$ dada por*

$$N_{E/F}(\alpha) := \prod_{\sigma \in G} \sigma(\alpha),$$

para cada $\alpha \in E$.

(*ii*) *Se define la* ***traza de*** E ***sobre*** F *como la función* $T_{E/F} : E \to F$ *dada por*

$$T_{E/F}(\alpha) := \sum_{\sigma \in G} \sigma(\alpha),$$

para cada $\alpha \in E$.

Si no existe riesgo de confusión sobre la extensión E/F *con la que se está trabajando, escribiremos* N *y* T *en lugar de* $N_{E/F}$, $T_{E/F}$.

Observemos que realmente las funciones norma y traza sobre la extensión E/F son funciones que van de E en F. En efecto, para cada $\alpha \in E$, se tiene que $N(\alpha), T(\alpha) \in E^G$, en donde E^G es el campo fijo de E por G, el cual viene dado por $E^G = \{x \in E \big| \sigma(x) = x \ \ \forall\ \sigma \in G\}$. Ahora bien, por la teoría de Galois, se sabe que, siendo E/F una extensión Galois, se tiene que $E^G = F$.

Se tienen las siguientes propiedades de la función norma.

Proposición 3.1.3. *Sea* E/F *una extensión de Galois finita, con* $G := \mathrm{Gal}\,(E/F)$. *Entonces, la función norma,* $N : E \to F$ *satisface las siguientes propiedades:*

(*i*) $N(\alpha) = 0 \iff \alpha = 0, \quad \forall\ \alpha \in E$.

(*ii*) *Si* $\alpha \in F$, *entonces* $N(\alpha) = \alpha^{[E:F]}$. *En particular,* $N(1) = 1$.

(*iii*) *La función norma es multiplicativa, es decir,* $N(\alpha\beta) = N(\alpha)N(\beta), \quad \forall\ \alpha, \beta \in E$.

Demostración: Se sigue inmediatamente de la definición de N. □

De manera totalmente análoga, establecemos las propiedades de la traza.

Proposición 3.1.4. *Sea* E/F *una extensión de Galois finita, con* $G := \mathrm{Gal}\,(E/F)$. *Entonces, la función traza,* $T : E \to F$ *satisface las siguientes propiedades:*

(*i*) *Si* $\alpha \in F$, *entonces* $T(\alpha) = [E : F]\alpha$. *En particular,* $T(1) = [E : F]$.

(*ii*) *Si* $\alpha \in F$, $\beta \in E$, *entonces* $T(\alpha\beta) = \alpha T(\beta)$.

(*iii*) *La función traza es aditiva, es decir,* $T(\alpha + \beta) = T(\alpha) + T(\beta), \quad \forall\ \alpha, \beta \in E$.

Demostración: Se sigue inmediatamente de la definición de T. □

Proposición 3.1.5. *Sea $F \subseteq K \subseteq E$ una torre de campos tal que E/F es finita y de Galois, con K/F de Galois. Entonces, para cada $\alpha \in E$ se tiene que*

$$N_{E/F}(\alpha) = N_{K/F}(N_{E/K}(\alpha)), \quad y$$

$$T_{E/F}(\alpha) = T_{K/F}(T_{E/K}(\alpha)).$$

En particular, si $\alpha \in K$, entonces $N_{E/F}(\alpha) = N_{K/F}\left(\alpha^{[E:K]}\right) = N_{K/F}(\alpha)^{[E:K]}$, y $T_{E/F}(\alpha) = T_{K/F}([E:K]\alpha) = [E:K]T_{K/F}(\alpha)$.

Demostración: Sean $G := \mathrm{Gal}\,(E/F)$, $N := \mathrm{Gal}\,(E/K) = \{\theta_1, \ldots, \theta_r\}$ y $H = \mathrm{Gal}\,(K/F) = \{\gamma_1, \ldots, \gamma_s\}$. Para cada $1 \leq i \leq s$, extendemos cada F-automorfismo γ_i de K a un F-automorfismo $\overline{\gamma_i}$ de E. Entonces, tenemos que $G = \{\overline{\gamma_i}\theta_j \mid 1 \leq i \leq s,\ 1 \leq j \leq r\}$, y por tanto

$$\begin{aligned} N_{E/F}(\alpha) &= \prod_{i=1}^{s}\prod_{j=1}^{r}\overline{\gamma_i}\theta_j(\alpha) = \prod_{i=1}^{s}\overline{\gamma_i}\left(\prod_{j=1}^{r}\theta_j(\alpha)\right) \\ &= \prod_{i=1}^{s}\overline{\gamma_i}\left(N_{E/K}(\alpha)\right) = \prod_{i=1}^{s}\gamma_i\left(N_{E/K}(\alpha)\right) \\ &= N_{K/F}\left(N_{E/K}(\alpha)\right). \end{aligned}$$

Por otra parte,

$$\begin{aligned} T_{E/F}(\alpha) &= \sum_{i=1}^{s}\sum_{j=1}^{r}\overline{\gamma_i}\theta_j(\alpha) = \sum_{i=1}^{s}\overline{\gamma_i}\left(\sum_{j=1}^{r}\theta_j(\alpha)\right) \\ &= \sum_{i=1}^{s}\overline{\gamma_i}\left(T_{E/K}(\alpha)\right) = \sum_{i=1}^{s}\gamma_i\left(T_{E/K}(\alpha)\right) \\ &= T_{K/F}\left(T_{E/K}(\alpha)\right). \end{aligned}$$

La penúltima afirmación se sigue, de manera inmediata, de la proposición 3.1.3 partes (*ii*) y (*iii*); mientras que la última es igualmente inmediata, y se deduce de la proposición 3.1.4, partes (*i*) y (*iii*). □

En particular, tenemos el siguiente resultado.

Proposición 3.1.6. *Sean $n \in \mathbb{N}$, $\alpha \in \mathbb{Q}(\zeta_n)$ y N, T las funciones norma y traza, respectivamente, de $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$. Sea $f(X) = \mathrm{irr}\,(\alpha, \mathbb{Q}) = a_0 + a_1X + \cdots + a_{m-1}X^{m-1} + X^m$. Entonces, se tiene lo siguiente:*

(*i*) $N(\alpha) = ((-1)^m a_0)^{[\mathbb{Q}(\zeta_n):\mathbb{Q}(\alpha)]}$.

(*ii*) $T(\alpha) = -[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\alpha)]a_{m-1}$.

(*iii*) *La función N restringida a $\mathbb{Z}[\zeta_n]$ es una función multiplicativa de $\mathbb{Z}[\zeta_n]$ en $\mathbb{Z}$.*

(*iv*) *La función T restringida a $\mathbb{Z}[\zeta_n]$ es una función aditiva de $\mathbb{Z}[\zeta_n]$ en $\mathbb{Z}$.*

(*v*) *Si $\alpha \in \mathbb{Z}[\zeta_n]$, entonces se tiene que $\alpha \in \mathbb{Z}[\zeta_n]^* \iff N(\alpha) = \pm 1$.*

(*vi*) *Si $\alpha \in \mathbb{Z}[\zeta_n]$ es tal que $N(\alpha)$ es un número primo, entonces α es un elemento irreducible de $\mathbb{Z}[\zeta_n]$.*

Demostración:

(*i*) De acuerdo con las notaciones de la proposición, tenemos que $m = \text{grad}(f) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$, pero también m es el número de conjugados de α. Sean $\alpha_1, \ldots, \alpha_m$ los conjugados de α, con $\alpha_1 = \alpha$. Entonces, $f(X) = (X - \alpha_1) \cdots (X - \alpha_m)$ y, de esta forma, $a_0 = (-1)^m \alpha_1 \cdots \alpha_m$. Observemos que la extensión $\mathbb{Q}(\alpha)/\mathbb{Q}$ es de Galois, y si $H := \text{Gal}\,(\mathbb{Q}(\alpha)/\mathbb{Q})$, entonces se tiene que

$$N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = \prod_{\gamma \in H} \gamma(\alpha) = \alpha_1 \cdots \alpha_m = (-1)^m a_0.$$

Por lo tanto, por la proposición 3.1.5, tenemos que

$$N(\alpha) = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)^{[\mathbb{Q}(\zeta_n):\mathbb{Q}(\alpha)]} = ((-1)^m a_0)^{[\mathbb{Q}(\zeta_n):\mathbb{Q}(\alpha)]}.$$

(*ii*) De manera totalmente análoga a la del inciso (*i*), escogemos los conjugados $\alpha_1, \ldots, \alpha_m$ de α, con $\alpha_1 = \alpha$, y recordamos que $f(X) = (X - \alpha_1) \cdots (X - \alpha_m)$. Esto implica que $a_{m-1} = -(\alpha_1 + \cdots + \alpha_m)$. Dado que la extensión $\mathbb{Q}(\alpha)/\mathbb{Q}$ es de Galois, siendo H como en el inciso (*i*), entonces se tiene que

$$T_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = \sum_{\gamma \in H} \gamma(\alpha) = \alpha_1 + \cdots + \alpha_m = -a_{m-1}.$$

Por lo tanto, por la proposición 3.1.5, tenemos que

$$T(\alpha) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\alpha)] T_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = -[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\alpha)]a_{m-1}.$$

(*iii*) De acuerdo con la proposición 3.1.2 parte (*ii*) y las notaciones correspondientes, tenemos que, si $\alpha \in \mathbb{Z}[\zeta_n]$, entonces $f(X) \in \mathbb{Z}[X] \Rightarrow a_0 \in \mathbb{Z}$; por lo tanto $N(\alpha) = ((-1)^m a_0)^{[\mathbb{Q}(\zeta_n):\mathbb{Q}(\alpha)]} \in \mathbb{Z}$, luego se tiene la afirmación.

(*iv*) De manera total y completamente análoga a como se hace en el inciso (*iii*), observamos que $\alpha \in \mathbb{Z}[\zeta_n] \Rightarrow f(X) \in \mathbb{Z}[X] \Rightarrow a_{m-1} \in \mathbb{Z}$; por lo tanto, $T(\alpha) = -[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\alpha)]a_{m-1} \in \mathbb{Z}$, que es lo que se quería demostrar.

(*v*) Si $\alpha \in \mathbb{Z}[\zeta_n]^*$, entonces existe $\beta \in \mathbb{Z}[\zeta_n]$ tal que $\alpha\beta = 1$, de lo cual se sigue que $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$, en donde $N(\alpha), N(\beta) \in \mathbb{Z}$. Es decir, se tiene que $N(\alpha) \in \mathbb{Z}^*$. Por lo tanto, $N(\alpha) = \pm 1$.

Recíprocamente, supóngase que $\alpha \in \mathbb{Z}[\zeta_n]$, con $N(\alpha) = \pm 1$. Hay dos maneras de demostrar que $\alpha \in \mathbb{Z}[\zeta_n]^*$. La primera de ellas hace notar que, por el inciso (*i*) y por la proposición 3.1.2 parte (*ii*), tenemos que $a_0 \in \mathbb{Z}$, con $\pm 1 = N(\alpha) = ((-1)^m a_0)^{[\mathbb{Q}(\zeta_n):\mathbb{Q}(\alpha)]}$, de modo que $a_0 \in \mathbb{Z}^* \Rightarrow a_0 = \pm 1$. Así, $f(X) = \pm 1 + a_1 X + \cdots + a_{m-1}X^{m-1} + X^m \in \mathbb{Z}[X]$, con $f(\alpha) = 0$. Luego entonces, $a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} + \alpha^m = \mp 1$, o equivalentemente, tendremos que

$$\beta := \frac{1}{\alpha} = \mp \left(a_1 + \cdots + a_{m-1}\alpha^{m-2} + \alpha^{m-1}\right) \in \mathbb{Z}[\zeta_n],$$

en donde $\alpha\beta = 1$. La segunda opción consiste en considerar el hecho de que, si $\alpha_1, \cdots, \alpha_m$ son los conjugados de α, con $\alpha = \alpha_1$, entonces se tiene que

$$\pm 1 = N(\alpha) = \prod_{i=1}^{m} \alpha_i = \alpha \prod_{i=2}^{m} \alpha_i.$$

En donde, por la proposición 3.1.2 parte (*i*), se tiene que $\alpha_i \in \mathbb{Z}[\zeta_n], \quad \forall\ 1 \leq i \leq m$. De manera que

$$\beta := \pm \prod_{i=2}^{m} \alpha_i \in \mathbb{Z}[\zeta_n],$$

con $\alpha\beta = 1$. En cualquiera de los dos razonamientos anteriores, se encuentra un $\beta \in \mathbb{Z}[\zeta_n]$ tal que $\alpha\beta = 1$. Por lo tanto, $\alpha \in \mathbb{Z}[\zeta_n]^*$.

(*vi*) Supóngase que $\alpha \in \mathbb{Z}[\zeta_n]$ y que $N(\alpha) \in \mathbb{Z}$ es un número primo. Entonces, $N(\alpha) \neq \pm 1$, y por (*v*) esto significa que $\alpha \notin \mathbb{Z}[\zeta_n]^*$. Sean $\beta, \gamma \in \mathbb{Z}[\zeta_n]$ tales que $\alpha = \beta\gamma$. Entonces, $N(\alpha) = N(\beta)N(\gamma)$ donde los elementos involucrados son números enteros y $N(\alpha)$ es número primo. Luego, necesariamente $N(\beta) = \pm 1$ o $N(\gamma) = \pm 1$, es decir, β o γ debe de ser una unidad de $\mathbb{Z}[\zeta_n]$. Por lo tanto, α es elemento irreducible de $\mathbb{Z}[\zeta_n]$.

□

Corolario 3.1.2. *Sean p número primo impar, y $t \in \mathbb{Z}$ tal que $p \nmid t$. Entonces, el ideal $\langle 1-\zeta_p^t \rangle$ es un ideal maximal de $\mathbb{Z}[\zeta_p]$.*

Demostración: Sea $G = \mathrm{Gal}\,(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Tenemos que $\{\sigma(1-\zeta_p^t)\big|\sigma \in G\}$ es el conjunto de conjugados de $1-\zeta_p^t$. Pero se tiene que $\sigma(1-\zeta_p^t) = 1-\sigma(\zeta_p^t)$, para cada $\sigma \in G$, y el conjunto de conjugados de ζ_p^t es precisamente $\left\{\zeta_p, \ldots, \zeta_p^{p-1}\right\}$. En consecuencia, el conjunto de conjugados de $1-\zeta_p^t$ es $\left\{1-\zeta_p, \ldots, 1-\zeta_p^{p-1}\right\}$. Por lo tanto, si denotamos por N a la norma de $\mathbb{Q}(\zeta_p)$ sobre $\mathbb{Q}$, tendremos que $N(1-\zeta_p^t) = (1-\zeta_p)\cdots(1-\zeta_p^{p-1}) = \Phi_p(1) = p$, dado que $\Phi_p(X) = (X-\zeta_p)\cdots(X-\zeta_p^{p-1}) = 1+X+\cdots+X^{p-1}$. Así, por la proposición 3.1.6 parte (vi), se tiene que $1-\zeta_p^t$ es un elemento irreducible de $\mathbb{Z}[\zeta_p]$ y, por consiguiente, el ideal $\langle 1-\zeta_p^t \rangle$ es maximal. □

Lema 3.1.1. *Sea p un número primo, y supóngase que $r, s \in \mathbb{Z}$, con $(p, rs) = 1$. Entonces, $\dfrac{\zeta_p^r - 1}{\zeta_p^s - 1} \in \mathbb{Z}[\zeta_p]^*$.*

Demostración: Puesto que $(p, s) = 1$, existen $u, v \in \mathbb{Z}$ tales que $su + pv = 1$; esto implica que $r = s(ur) + p(vr)$. Sea $t = ur$. Se tiene, entonces, que

$$\frac{\zeta_p^r - 1}{\zeta_p^s - 1} = \frac{\zeta_p^{st} - 1}{\zeta_p^s - 1} = 1 + \zeta_p^s + \cdots + \zeta_p^{s(t-1)} \in \mathbb{Z}[\zeta_p].$$

Análogamente, se tiene que $\dfrac{\zeta_p^s - 1}{\zeta_p^r - 1} \in \mathbb{Z}[\zeta_p]$. Por lo tanto, se tiene lo deseado. □

Definición 3.1.5. *Las unidades del lema 3.1.1 son llamadas* ***unidades ciclotómicas****.*

Proposición 3.1.7. *En el anillo $\mathbb{Z}[\zeta_p]$, se tiene que $\langle 1-\zeta_p \rangle^{p-1} = \langle p \rangle$.*

Demostración: De acuerdo con el lema 3.1.1, tenemos que, para cada $1 \leq i, j \leq p-1$, los elementos $1-\zeta_p^i$ y $1-\zeta_p^j$ son asociados* y, por lo tanto, generan el mismo ideal $\langle 1-\zeta_p \rangle$. Pero, puesto que $(1-\zeta_p)(1-\zeta_p^2)\cdots(1-\zeta_p^{p-1}) = p$, entonces, a nivel de ideales, se tiene que

$$\langle 1-\zeta_p \rangle^{p-1} = \langle 1-\zeta_p \rangle \langle 1-\zeta_p^2 \rangle \cdots \langle 1-\zeta_p^{p-1} \rangle = \langle p \rangle.$$

□

*Recordemos que, dado un dominio entero A, se dice que dos elementos $a, b \in A$ son **asociados** si existe una unidad $u \in A^*$ tal que $a = ub$. Cuando esto ocurre, se tiene que $\langle a \rangle = \langle b \rangle$.

Para llevar a cabo la demostración del teorema principal del presente capítulo (que, como ya se mencionó, es un caso particular del último teorema de Fermat), es necesario garantizar que los ideales del anillo $\mathbb{Z}[\zeta_p]$, donde p es un número primo, se factoricen de manera única como producto de ideales primos. De hecho, la demostración sería ligeramente más sencilla si pudiéramos asegurar que $\mathbb{Z}[\zeta_p]$ es un dominio de factorización única. Sin embargo, tal condición en general no se cumple. Afortunadamente, la condición levemente más débil que involucra sólo la factorización de ideales, es suficiente para nuestros propósitos, y esta última es mucho más fácil de satisfacer. En lo que sigue nos encaminaremos a analizar y explicar los casos en los que se cumple dicha condición.

Definición 3.1.6. *Sea $\alpha \in \mathbb{Q}(\zeta_p)$. Decimos que α es **entero** sobre $\mathbb{Z}$ si α es raíz de un polinomio mónico con coeficientes en $\mathbb{Z}$.*

Cuando $\alpha \in \mathbb{Q}(\zeta_p)$ es entero sobre $\mathbb{Z}$, entonces tenemos que $\operatorname{irr}(\alpha, \mathbb{Q})$ es un polinomio con coeficientes en $\mathbb{Z}$. Por lo tanto, si T y N representan, respectivamente, la traza y la norma de $\mathbb{Q}(\zeta_p)$ sobre $\mathbb{Q}$, entonces se tiene que $T(\alpha), N(\alpha) \in \mathbb{Z}$.

La **cerradura entera** de $\mathbb{Z}$ en $\mathbb{Q}(\zeta_p)$ es el conjunto de los elementos de $\mathbb{Q}(\zeta_p)$ los cuales son enteros sobre $\mathbb{Z}$. Si a este conjunto lo denotamos por $\mathcal{O}$, entonces tenemos que $\mathcal{O}$ es un subanillo de $\mathbb{Q}(\zeta_p)$, extensión de $\mathbb{Z}$. En particular, tenemos que $\zeta_p^i \in \mathcal{O}$ para cada $i \in \mathbb{Z}$ tal que $p \nmid i$.

Las definiciones anteriores son aplicables a cualquier extensión de anillos conmutativos con identidad. Así, dada una extensión de anillos conmutativos con identidad B/A, se dice que un elementeo $\alpha \in B$ es **entero** sobre A si α es raíz de un polinomio mónico con coeficientes en A. En este sentido tenemos, por ejemplo, que para cualquier $\alpha \in B$, se tiene que α es entero sobre A si y sólo si el A-módulo $A[\alpha]$ es finitamente generado ([8], capítulo VIII, sección 5, teorema 5.3 (pp. 395-396)). Un resultado que también es útil es el que establece que, si C/B y B/A son extensiones de anillos conmutativos con identidad tales que C es extensión entera de B y B es una extensión entera de A, entonces C es una extensión entera de A; en particular, se tiene que si $\alpha \in C$ es entero sobre sobre B y B es extensión entera de A, entonces α es entero sobre A ([8], capítulo VIII, sección 5, teorema 5.6 (pp. 397)). La **cerradura entera** de B sobre A es el conjunto que consta de los elementos de B que son enteros sobre A. Que un dominio entero A sea **enteramente cerrado** significa que todos los elementos del campo de cocientes de A, $\operatorname{coc}(A)$, que son enteros sobre A, pertenecen a A. Por ejemplo, la cerradura entera de $\mathbb{Z}$ en $\mathbb{Q}$, es decir, el conjunto de los elementos de $\mathbb{Q}$ que son enteros sobre $\mathbb{Z}$, es exactamente $\mathbb{Z}$, así, se tiene que $\mathbb{Z}$ es enteramente cerrado.

Teorema 3.1.1. *Sea p un número primo. Entonces, el anillo $\mathbb{Z}[\zeta_p]$ es la cerradura entera de $\mathbb{Z}$ en $\mathbb{Q}(\zeta_p)$.*

Demostración: Sea $\mathcal{O}$ la cerradura entera de $\mathbb{Z}$ en $\mathbb{Q}(\zeta_p)$. Dada la proposición 3.1.2 parte (ii), resulta claro que $\mathbb{Z}[\zeta_p] \subseteq \mathcal{O}$. Ahora bien, tomemos $\alpha \in \mathcal{O}$. Entonces, existen $a_0, \ldots, a_{p-2} \in \mathbb{Q}$ tales que $\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$. Sea T la función traza de $\mathbb{Q}(\zeta_p)$ sobre $\mathbb{Q}$. Recordando que, para cada $i \in \mathbb{Z}$ tal que $p \nmid i$, $\operatorname{irr}\left(\zeta_p^i, \mathbb{Q}\right) = \Phi(X) = 1 + X + \cdots + X^{p-2} + X^{p-1}$, la proposición 3.1.6 parte (ii) nos asegura que $T(\zeta_p^i) = -[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\zeta_p^i)]1 = -1$. En consecuencia, para cada $i = 0, \ldots, p-2$, recordando que $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$, obtenemos que

$$\begin{aligned} T(\alpha\zeta_p^{-i}) &= T\left(a_0\zeta_p^{-i} + a_1\zeta_p^{1-i} + \cdots + a_{i-1}\zeta_p^{p-1} + a_i + a_{i+1}\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2-i}\right) \\ &= -a_0 - a_1 - \cdots - a_{i-1} + (p-1)a_i - a_{i+1} - \cdots - a_{p-2}. \end{aligned}$$

Similarmente,

$$T(\alpha\zeta_p) = T\left(a_0\zeta_p + a_1\zeta_p^2 + \cdots + a_{p-2}\zeta_p^{p-1}\right) = -a_0 - a_1 - \cdots - a_{p-2}.$$

En consecuencia, se tiene que $T(\alpha\zeta_p^{-i} - \alpha\zeta_p) = T(\alpha\zeta_p^{-i}) - T(\alpha\zeta_p) = pa_i$. Cabe destacar que, dado que $\mathcal{O}$ es un anillo con $\alpha, \zeta_p \in \mathcal{O}$, entonces $\alpha\zeta_p^{-i} - \alpha\zeta_p \in \mathcal{O}$. Esto significa que $pa_i = T(\alpha\zeta_p^{-i} - \alpha\zeta_p) \in \mathbb{Z}$, para cada $i = 0, \ldots, p-2$. Así pues, $p\alpha \in \mathbb{Z}[\zeta_p]$ y, por consiguiente (dado que el conjunto $\{1, 1-\zeta_p, \cdots, (1-\zeta_p)^{p-2}\}$ es $\mathbb{Z}$-base del $\mathbb{Z}$-módulo $\mathbb{Z}[\zeta_p]$) existen $b_0, \ldots, b_{p-2} \in \mathbb{Z}$ tales que

$$p\alpha = b_0 + b_1(1-\zeta_p) + \cdots + b_{p-2}(1-\zeta_p)^{p-2}. \tag{3.1.1}$$

De acuerdo con la proposición 3.1.7, $\langle 1-\zeta_p\rangle^{p-1} = \langle p\rangle$, de modo que p y $(1-\zeta_p)^{p-1}$ son asociados, por consiguiente existe $u \in \mathbb{Z}[\zeta]^*$ tal que $p = u(1-\zeta_p)^{p-1}$. De aquí que, al substituir a p por $u(1-\zeta_p)^{p-1}$ en la ecuación (3.1.1), tenemos que $(1-\zeta_p)|b_0$ dentro del anillo $\mathbb{Z}[\zeta_p]$. Tomando normas, obtenemos que $p \mid b_0^{p-1} \Rightarrow p \mid b_0$. Sea, pues, $c_0 \in \mathbb{Z}$ tal que $b_0 = pc_0$. Entonces la ecuación (3.1.1) se transforma en

$$p(\alpha - c_0) = b_1(1-\zeta_p) + \cdots + b_{p-2}(1-\zeta_p)^{p-2}. \tag{3.1.2}$$

De nuevo, al substituir p por $u(1-\zeta_p)^{p-1}$ en la ecuación (3.1.2) y dividir entre $1-\zeta_p$, obtenemos que $(1-\zeta_p)|b_1$ y, al sacar normas, obtenemos que $p|b_1$. Siguiendo con el proceso, llegamos a que $p|b_i$ para cada uno de los $i = 0, \ldots, p-2$. Por lo tanto, existen enteros $c_0, \ldots, c_{p-2} \in \mathbb{Z}$ tales que $\alpha = c_0 + c_1\zeta_p + \cdots + c_{p-2}\zeta_p^{p-2} \in \mathbb{Z}[\zeta_p]$. De modo que $\mathcal{O} \subseteq \mathbb{Z}[\zeta_p]$. Por consiguiente, $\mathbb{Z}[\zeta_p] = \mathcal{O}$. □

3.2. Dominios Dedekind y campos numéricos

Definición 3.2.1. *Sea D un dominio entero. Se dice que D es un* ***dominio Dedekind****, o simplemente que D es* ***Dedekind****, si D es enteramente cerrado, noetheriano, y cada ideal primo de D es un ideal maximal.*

Comentaremos algunos propiedades que tienen los dominios Dedekind, las cuales pueden ser consultadas en libros como [8], capítulo VIII, sección 6 (pp. 400-409); [11], capítulo 3, sección 3 (pp. 376-388); o [10], capítulo I, secciones 3-7 (pp. 8-34). Sea D un dominio entero y $K = \operatorname{coc}(D)$. Entonces, tenemos que K es un D-módulo. Un **ideal fraccional** de D es un D-submódulo $I \subseteq K$, no cero, tal que $\alpha I \subseteq D$, para algún $\alpha \in D$. Por ejemplo, los ideales de D son ideales fraccionales, llamados **ideales enteros**. Entonces, el conjunto de ideales fraccionales constituye un monoide conmutativo con identidad, denotado por $\mathfrak{I}(D)$, cuya multiplicación está dada por

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i \middle| a_i \in I,\ b_i \in J;\ n \in \mathbb{N} \right\}.$$

Un ideal fraccional $I \in \mathfrak{I}(D)$ se dice que es **invertible** si existe un ideal fraccional J de D tal que $IJ = D$. El inverso de I, si existe, es único y es denotado por I^{-1}. Además, se tiene que $I^{-1} = \{\alpha \in K \big| \alpha I \subseteq D\}$, y si I es un ideal entero, entonces $D \subseteq I^{-1}$.

Antes de enunciar el resultado que caracteriza a los dominios Dedekind, mencionaremos una definición.

Definición 3.2.2. *Sea D un anillo. Se dice que D es un* ***anillo de valuación discreta*** *si D es un dominio de ideales principales el cual es local.*

En otras palabras, un anillo de valuación discreta es un anillo el cual es un dominio de ideales principales y tiene un único ideal maximal no cero.

Así pues, se tiene el siguiente resultado:

Teorema 3.2.1. *Sea D un dominio entero. Entonces, las siguientes condiciones son equivalentes:*

(*i*) *D es un dominio Dedekind.*

(*ii*) *Cada ideal propio de D se expresa de manera única como producto de un número finito de ideales primos de D.*

(*iii*) *Cada ideal fraccional de D es invertible.*

(*iv*) *D es noetheriano y para cada ideal primo P de D, la localización D_P de D en P es un anillo de valuación discreta.*

Demostración: [8], capítulo VIII, sección 6, teorema 6.10 (pp. 405-407). También se puede consultar [11], capítulo 3, sección 3, teoremas 3.5 (pp. 380-381), 3.6 (pp. 381-382), y 3.18 inciso (*i*) (pp. 387-388). □

De acuerdo con el teorema 3.2.1, tenemos que si D es un dominio Dedekind, entonces el monoide $\mathfrak{I}(D)$ de los ideales fraccionales de D es un grupo abeliano libre cuyos generadores libres son los ideales primos no cero de D. Así, cada ideal fraccional I de D se ha de expresar, de manera única, en la forma

$$I = P_1^{n_1} \cdots P_t^{n_t}, \tag{3.2.1}$$

para algún $t \in \mathbb{N}$, para algunos $P_1, \ldots, P_t$ ideales primos no cero de D y para algunos $n_1, \ldots, n_t \in \mathbb{Z}$. En particular, si D es un dominio Dedekind, $K = \operatorname{coc}(D)$, y $\alpha \in K \backslash \{0\}$, entonces el **ideal fraccional principal** generado por α, $\langle \alpha \rangle := \alpha D$, se ha de expresar como en la ecuación (3.2.1). Sea $\mathfrak{P}(D)$ el conjunto de los ideales fraccionales principales. Se tiene que $\mathfrak{P}(D)$ es un subgrupo de $\mathfrak{I}(D)$, y al grupo cociente $\mathfrak{C}(D) = \mathfrak{I}(D)/\mathfrak{P}(D)$ se le conoce con el nombre de **grupo de clases** de D. En el caso de que el grupo de clases de D sea finito, se denota por $h(D) := |\mathfrak{C}(D)|$ al orden de dicho grupo, y dicho número es llamado el **número de clases** de D.

En muchas ocasiones, las notaciones anteriores son expresadas en términos del campo de cocientes de D, es decir, se escribe $\mathfrak{I}(K)$, $\mathfrak{P}(K)$, $\mathfrak{C}(K) = \mathfrak{I}(K)/\mathfrak{P}(K)$, $h(K)$, etc., con $K = \operatorname{coc}(D)$.

No es difícil probar el siguiente hecho (ver [11], capítulo 3, sección 3, proposición 3.1 (pp. 377)).

Proposición 3.2.1. *Sea D un dominio Dedekind. Entonces, las siguientes condiciones son equivalentes:*

(*i*) *D es un dominio de ideales principales.*

(*ii*) *D es un dominio de factorización única.*

(*iii*) *$h(D) = 1$.* □

En particular, tenemos que el anillo de los números enteros $\mathbb{Z}$ es un dominio Dedekind, y $h(\mathbb{Z}) = 1$.

Proposición 3.2.2. *Sean D un dominio Dedekind, $K = \mathrm{coc}\,(D)$ y E/K una extensión finita de campos. Entonces, la cerradura entera de D en E es un dominio Dedekind.*

Demostración: Ver [10], capítulo I, sección 6, teorema 6.1 (pp. 23-26). □

Corolario 3.2.1. *El anillo $\mathbb{Z}[\zeta_p]$ es un dominio Dedekind.*

Demostración: Es inmediata del teorema 3.1.1 y de la proposición 3.2.2. □

Consideremos un dominio Dedekind D con $K = \mathrm{coc}\,(D)$, y sea E/K una extensión finita. Si B es la cerradura entera de D en E, entonces la proposición 3.2.2 nos garantiza que B es también un dominio Dedekind. Por consiguiente, para cada P ideal primo no cero de D, se tiene que el ideal generado por P en B se descompone de manera única en la forma:

$$PB = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}, \tag{3.2.2}$$

donde $g \in \mathbb{N}$, $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ son ideales primos no cero de B y $e_1, \ldots, e_g \in \mathbb{N}$. Para cada $1 \leq i \leq g$, el ideal primo $\mathfrak{P}_i$ se dice que está **encima** de P. Se tiene que el campo D/P está encajado en el campo $B/\mathfrak{P}_i$; dichos campos son llamados **campos residuales**. La extensión de campos $(B/\mathfrak{P}_i)/(D/P)$ es una extensión finita cuya grado $[B/\mathfrak{P}_i : D/P]$ es llamado el **grado residual** y es denotado por $f_i = f(\mathfrak{P}_i|P)$. El exponente e_i se denomina el **índice de ramificación**, y se denota por $e_i = e(\mathfrak{P}_i|P)$. El ideal primo P se dice que es **ramificado** si $e_i > 1$ para algún $1 \leq i \leq g$. Los ideales primos $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ de B son exactamente aquellos ideales primos de B que contienen al ideal primo P, y satisfacen que $\mathfrak{P}_i \cap D = P$, para cada $1 \leq i \leq g$.

Cuando la extensión finita de campos E/K es separable, se tiene que la cantidad de ideales primos de D ramificados en B es finita ([10], capítulo I, sección 7, teorema 7.3 (pp. 30-32)). Además, para cada ideal primo P de D factorizado como en la ecuación (3.2.2), se tiene que $[E : K] = \sum_{i=1}^{g} e_i f_i$ ([10], capítulo I, sección 6, corolario 6.7 (pp. 28)). En particular, se tiene el siguiente resultado.

Teorema 3.2.2. *Sean D un dominio Dedekind, $K = \mathrm{coc}\,(D)$, E/K una extensión finita de Galois con $G = \mathrm{Gal}\,(E/K)$, y B la cerradura entera de D en E. Para cada ideal primo P de D, desarrollamos la factorización del ideal PB*

$$PB = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g},$$

con ideales primos $\mathfrak{P}_i$ distintos de B. Entonces, todos los grados residuales son iguales, es decir, hay un f tal que $f(\mathfrak{P}_i|P) = f, \ \ \forall\ 1 \leq i \leq g$. También los índices de ramificación son todos ellos iguales entre sí, digamos que $e = e(\mathfrak{P}_i|P), \ \ \forall\ 1 \leq i \leq g$. Además, se tiene que $efg = [L : K]$. Más aún, la acción de G permuta transitivamente los ideales primos $\mathfrak{P}_i$ de B que están encima de P.

Demostración: [10], capítulo I, sección 6, teorema 6.8 (pp. 29). □

La acción del grupo G en el teorema 3.2.2 está dada como sigue: Para cada ideal primo $\mathfrak{P}$ de R y para cada $\sigma \in G$,

$$\sigma(\mathfrak{P}) = \{\sigma(a) \big| a \in \mathfrak{P}\}.$$

A continuación, hablaremos un poco de campos numéricos para mencionar algunos resultados que necesitaremos más adelante.

Definición 3.2.3.

(*i*) *Sea K un campo de característica cero. Entonces, si $[K : \mathbb{Q}] < \infty$, se dice que K es un* ***campo numérico****.*

(*ii*) *Si K es un campo numérico, entonces la cerradura entera de $\mathbb{Z}$ en K se conoce como el* ***anillo de enteros algebraicos****, o simplemente* ***anillo de enteros****, de K, y en general suele denotarse por $\mathcal{O}_K$ o simplemente $\mathcal{O}$, cuando no existe posibilidad de confusión respecto de K.*

Sean K un campo numérico, y $\mathcal{O}$ su anillo de enteros algebraicos. De acuerdo con la proposición 3.2.2, se tiene que $\mathcal{O}$ es un dominio Dedekind. Por lo tanto, podemos construir el grupo de clases de $\mathcal{O}$, denotado por $\mathfrak{C}(\mathcal{O})$. Como $K = \mathrm{coc}\,(\mathcal{O})$, hablaremos del grupo de clases de K, $\mathfrak{C}(K)$, en vez de referirnos al de $\mathcal{O}$. Bajo esta forma de expresión, el número de clases de K, denotado por $h(K)$, viene dado por $h(K) := |\mathfrak{C}(K)|$.

Teorema 3.2.3. *Sea K un campo numérico. Entonces, $h(K)$ es finito.*

Demostración: Ver [9], capítulo 12, sección 2, teorema 1 (pp. 178). □

Analicemos lo que esto significa para el caso del campo numérico $\mathbb{Q}(\zeta_p)$, con p número primo. En primer lugar, el teorema 3.1.1 establece que $\mathbb{Z}[\zeta_p]$ es el anillo de enteros algebraicos de $\mathbb{Q}(\zeta_p)$, es decir, $\mathbb{Z}[\zeta_p] = \mathcal{O}_{\mathbb{Q}(\zeta_p)}$, y la cardinalidad de su grupo de clases es el número de clases del campo $\mathbb{Q}(\zeta_p)$, denotado por $h(\mathbb{Q}(\zeta_p))$. Ahora bien, recordemos que el grupo de clases de un dominio Dedekind es el cociente de su grupo de ideales fraccionales módulo el subgrupo de los ideales fraccionales principales; en otras palabras, $\mathfrak{C}(\mathbb{Z}[\zeta_p]) = \mathfrak{I}(\mathbb{Z}[\zeta_p])/\mathfrak{P}(\mathbb{Z}[\zeta_p])$. Así, tenemos que $h(\mathbb{Q}(\zeta_p)) = 1 \iff \mathbb{Z}[\zeta_p]$ es un dominio de ideales principales. En el caso general, se observa que

$$h(\mathbb{Q}(\zeta_p)) = |\mathfrak{C}(\mathbb{Z}[\zeta_p])| = \frac{|\mathfrak{I}(\mathbb{Z}[\zeta_p])|}{|\mathfrak{P}(\mathbb{Z}[\zeta_p])|}.$$

Esto nos indica que el número $h(\mathbb{Q}(\zeta_p))$ en cierto modo mide lo lejos que se encuentra el dominio Dedekind $\mathbb{Z}[\zeta_p]$ de ser un dominio de ideales principales. Como ya se mencionó en algún momento, para poder demostrar el resultado principal de la presente sección, sería ideal considerar números primos p tales que $\mathbb{Z}[\zeta_p]$ fuera un dominio de ideales principales, o equivalentemente, tales que $h(\mathbb{Q}(\zeta_p)) = 1$. Sin embargo, tal condición en general no se cumple. Está demostrado que, si p es un número primo, entonces $h(\mathbb{Q}(\zeta_p)) = 1 \iff p \leq 19$. De manera que, para la mayor parte de los números primos, no es posible contar con la factorización única dentro del correspondiente anillo de enteros ciclotómicos. Como ya se dijo, es posible salir adelante con la suposición, más débil, de que el anillo de enteros ciclotómicos es simplemente un dominio Dedekind, ya que, como se ha visto, en este tipo de dominios la factorización de ideales es única. Sin embargo, hay que pagar cierto precio a cambio: el teorema en cuestión se podrá demostrar únicamente para los números primos p tales que $p \nmid h(\mathbb{Q}(\zeta_p))$.

En relación con esto, consideraremos un hecho importante que concierne al número de clases. Sea p un número primo, e $I \subseteq \mathbb{Z}[\zeta_p]$ un ideal no principal del p-ésimo anillo de enteros ciclotómicos. Esto significa que, dentro del grupo de clases $\mathfrak{C}(\mathbb{Q}(\zeta_p))$, el elemento $I\mathfrak{P}(\mathbb{Q}(\zeta_p))$ no es la identidad. Entonces, si $s \in \mathbb{Z}$ es tal que I^s es un ideal principal, ello significará que el elemento $(I\mathfrak{P}(\mathbb{Q}(\zeta_p)))^s = I^s\mathfrak{P}(\mathbb{Q}(\zeta_p))$ es la identidad. De ahí que, si o es el orden del elemento $I\mathfrak{P}(\mathbb{Q}(\zeta_p))$ dentro del grupo $\mathfrak{C}(\mathbb{Q}(\zeta_p))$, entonces $o \neq 1$, y además $o \mid s$ y, por la teoría de grupos, $o \mid |\mathfrak{C}(\mathbb{Q}(\zeta_p))| = h(\mathbb{Q}(\zeta_p))$. Esto significa que $(s, h(\mathbb{Q}(\zeta_p))) > 1$. Por consiguiente, si se da el caso de que $p \nmid h(\mathbb{Q}(\zeta_p))$, e I es un ideal de $\mathbb{Z}[\zeta_p]$ tal que I^p es un ideal principal, entonces ello significará que I es también un ideal principal. Este hecho será de fundamental importancia en la sección 3.5.

De momento, concluyamos la presente sección con un par de lemas que serán necesarios para llegar a la meta del presente capítulo.

Lema 3.2.1. *Sea K un campo numérico, con $n = [K : \mathbb{Q}]$, y sean $\sigma_1, \sigma_2, \ldots, \sigma_n$ los n encajes de K en $\mathbb{C}$. Si $\alpha \in \mathcal{O}_K$ es tal que $|\sigma_i(\alpha)| \leq 1, \quad \forall\ 1 \leq i \leq n$, entonces α es una raíz de la unidad.*

Demostración: Tenemos que α es una raíz del polinomio

$$f(X) = \prod_{i=1}^{n} (X - \sigma_i(\alpha)) \in \mathbb{Z}[X].$$

Por las hipótesis, si escribimos $f(X) = a_0 + a_1 X + \cdots + a_n X^n$, entonces para cada $0 \leq m \leq n$ se tiene que $|a_m| \leq \binom{n}{m}$, con $a_m \in \mathbb{Z}$. Este tipo de condiciones, las pueden cumplir sólo una cantidad finita de polinomios de grado n en $\mathbb{Z}[X]$. Ahora bien, si α satisface las condiciones solicitadas, entonces también lo hacen todos los α^t para cualquier $t \in \mathbb{Z}$, es decir que todos los α^t son raíces de algún polinomio que, al igual que $f(X)$, satisface ciertas condiciones en cuanto a la acotación de sus coeficientes. Sin embargo, dado que sólo una cantidad finita de polinomios satisfacen dicha condición, se sigue que entre todos ellos no pueden tener más que una cantidad finita de raíces. Esto implica que el conjunto $\{\alpha^t \big| t \in \mathbb{Z}\}$ debe de ser finito. En otras palabras, dos potencias distintas de α necesariamente se repiten, por lo tanto existe una $t \in \mathbb{N}$ para la cual $\alpha^t = 1$. $\quad \therefore \alpha$ es una raíz de la unidad. $\square$

Lema 3.2.2. *Sea p un número primo impar, y sea $u \in \mathbb{Z}[\zeta_p]^*$. Entonces, es posible elegir un $s \in \mathbb{Z}$ tal que $\zeta_p^s u \in \mathbb{R}$.*

Demostración: Sabemos que $\overline{\zeta_p} = \zeta_p^{p-1}$, lo cual implica que la conjugación compleja es un $\mathbb{Q}$-automorfismo de $\mathbb{Q}(\zeta_p)$, más aún, es un $\mathbb{Z}$-automorfismo de $\mathbb{Z}[\zeta_p]$. Esto significa que si $u \in \mathbb{Z}[\zeta_p]^*$, entonces también se tendrá que $\overline{u} \in \mathbb{Z}[\zeta_p]^*$. Así, se tiene que $\tau = u/\overline{u} \in \mathbb{Z}[\zeta_p]^* \subseteq \mathbb{Z}[\zeta_p] = \mathcal{O}_{\mathbb{Q}(\zeta_p)}$. Más aún, si $\rho \in \mathrm{Gal}\,(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, entonces se tiene que $\rho(\tau) = \dfrac{\rho(u)}{\rho(\overline{u})} = \dfrac{\rho(u)}{\overline{\rho(u)}}$, de donde se sigue que $|\rho(\tau)| = 1, \quad \forall\ \rho \in \mathrm{Gal}\,(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Esto último implica, debido al lema 3.2.1, que τ es una raíz de la unidad, y por el corolario 3.1.1 esto último significa que $\tau = \pm\zeta_p^t$, para algún $t \in \mathbb{Z},\ 0 \leq t < p$.
Sea $\lambda = 1 - \zeta_p$, de manera que, dentro del anillo $\mathbb{Z}[\zeta_p]$, se cumpla la congruencia $\zeta_p^j \equiv 1 \bmod \lambda, \quad \forall\ j \in \mathbb{Z}$. Así, si $u = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$, con $a_i \in \mathbb{Z}\ \ \forall\ 0 \leq i \leq p-2$, entonces, dado $\rho \in \mathrm{Gal}\,(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, se tendrá que $u \equiv a_0 + a_1 + \cdots + a_{p-2} \equiv \rho(u) \bmod \lambda$, debido a que $\rho(\zeta_p) = \zeta_p^k$, para algún $k \in \mathbb{Z}$. En particular, $u \equiv \overline{u} \bmod \lambda$. De esta manera, si tuviéramos que $\tau = -\zeta_p^t$, para algún t, entonces tendríamos que

$u = -\zeta_p^t \overline{u}$, de manera que $u \equiv -\overline{u} \bmod \lambda \Rightarrow u \equiv -u \bmod \lambda \Rightarrow 2u \equiv 0 \bmod \lambda \Rightarrow \lambda \mid 2u$ dentro del anillo $\mathbb{Z}[\zeta_p]$. Esto implicaría que $2u = \alpha\lambda$, para algún $\alpha \in \mathbb{Z}[\zeta_p]$. Tomando normas a ambos lados, tendremos que $2^{p-1} = N(2)N(u) = N(\alpha)N(\lambda) = N(\alpha)p$, de donde se sigue que $p \mid 2^{p-1}$ en $\mathbb{Z}$. Siendo p un número primo se debe de tener que $p \mid 2$, lo cual implica que $p = 2$. Pero habíamos supuesto que p era un número primo impar, razón por la cual esta última conclusión es una contradicción. Por consiguiente, se debe de tener, para algún $1 \leq t < p$, que $\tau = \zeta_p^t \Rightarrow u = \zeta_p^t \overline{u}$. Ahora bien, es posible elegir algún $s \in \mathbb{Z}$ tal que $-2s \equiv t \bmod p$ (por ejemplo, si t es par podemos escoger $s = \dfrac{2p-t}{2}$, y si t es impar podemos elegir $s = \dfrac{p-t}{2}$), de manera que $u = \zeta_p^{-2s}\overline{u}$. En consecuencia, se tiene que $\zeta_p^s u = \zeta_p^{-s}\overline{u} = \overline{\zeta_p^s u}$, lo cual implica que $\zeta_p^s u \in \mathbb{R}$. □

3.3. Caracteres de Dirichlet y L-series

Sea $m \in \mathbb{Z}$, y sea $\chi' : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ un homomorfismo de grupos. Se define la función $\chi : \mathbb{Z} \to \mathbb{C}$, de la manera siguiente: para cada $n \in \mathbb{Z}$,

$$\chi(n) := \begin{cases} 0; & (n,m) > 1 \\ \chi'(n + m\mathbb{Z}); & (n,m) = 1. \end{cases} .$$

Definición 3.3.1. *Las funciones $\chi : \mathbb{Z} \to \mathbb{C}$ definidas como en el párrafo anterior, son conocidas con el nombre de* ***caracteres de Dirichlet módulo*** *m.*

Proposición 3.3.1. *Una función $\chi : \mathbb{Z} \to \mathbb{C}$ es un caracter de Dirichlet módulo m si y sólo si:*

(a) $\chi(n+m) = \chi(n), \quad \forall\ n \in \mathbb{Z}$;

(b) $\chi(kn) = \chi(k)\chi(n), \quad \forall\ k, n \in \mathbb{Z}$; *y*

(c) $\chi(n) = 0 \iff (n,m) > 1$.

Demostración: Sea χ un caracter de Dirichlet "inducido" por el homomorfismo de grupos $\chi' : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$. Es obvio que χ satisface la condición (c). Ahora bien, para ver que χ satisface la condición (a), tomemos $n \in \mathbb{Z}$, y tendremos dos casos. Cuando $(n,m) = 1$, entonces se tendrá que $(n+m, m) = 1$ y por consiguiente $\chi(n+m) = \chi'((n+m) + m\mathbb{Z}) = \chi'(n + m\mathbb{Z}) = \chi(n)$. Si por el contrario, se tiene que

$(n,m) > 1$, entonces, dado que $(n,m) \mid n+m$, se tendrá que también $(n+m,m) > 1$. En consecuencia, $\chi(n+m) = 0 = \chi(n)$. En cualquiera de los dos casos, observamos que χ satisface la condición (a). Sólo resta demostrar que χ satisface la condición (b). Para tal fin, tomemos $k, n \in \mathbb{Z}$. Nuevamente, tenemos dos casos. Si $(k,m) = 1$ y $(n,m) = 1$, entonces se tendrá que $(kn,m) = 1$, y por consiguiente, $\chi(kn) = \chi'(kn + m\mathbb{Z}) = \chi'((k + m\mathbb{Z})(n + m\mathbb{Z})) = \chi'(k + m\mathbb{Z})\chi'(n + m\mathbb{Z}) = \chi(k)\chi(n)$. Mientras tanto, si alguno de los números (k,m) o (n,m) es estrictamente mayor que 1, entonces se tendrá que $(kn,m) > 1$. Sin pérdida de generalidad, supongamos que es $(n,m) > 1$. Entonces, $\chi(k)\chi(n) = \chi(k)0 = 0 = \chi(kn)$. En ambos casos, χ satisface la condición (b).
Recíprocamente, sea $\chi : \mathbb{Z} \to \mathbb{C}$ una función que satisface las condiciones (a), (b) y (c). Entonces, definimos la función $\chi' : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ como sigue: para cada $n \in \mathbb{Z}$, con $(n,m) = 1$,

$$\chi'(n + m\mathbb{Z}) := \chi(n).$$

La condición (a) nos garantiza que la definición de $\chi'(n + m\mathbb{Z})$ no depende del representante escogido para $n + m\mathbb{Z}$, mientras que la condición (c) garantiza que efectivamente el contradominio de χ' es $\mathbb{C}^*$. Así las cosas, se tiene que efectivamente $\chi' : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ es una función, y por la condición (b) se tiene que χ' es un homomorfismo de grupos. Finalmente, observando de nuevo la condición (c) vemos que efectivamente χ' "induce" a la función χ de modo que esta última sea un caracter de Dirichlet módulo m. □

Ahora que hemos caracterizado a los caracteres de Dirichlet, hagamos algunas observaciones adicionales. Sea χ un caracter de Dirichlet módulo m, "inducido" por el homomorfismo de grupos $\chi' : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$. Así, tomemos z un valor no nulo de χ, y $n \in \mathbb{Z}$ tal que $\chi(n) = z$. Al ser $z \neq 0$, se tendrá que $(n,m) = 1$. En consecuencia, observamos que $z^{\phi(m)} = \chi(n)^{\phi(m)} = \chi'(n + m\mathbb{Z})^{\phi(m)} = \chi'((n + m\mathbb{Z})^{\phi(m)}) = \chi'(1 + m\mathbb{Z}) = 1$. De manera que los valores no nulos de χ, son raíces $\phi(m)$-ésimas de la unidad.

Dado $m \in \mathbb{Z}$, y dados χ, ψ dos caracteres de Dirichlet módulo m, defimos el producto entre χ y ψ como la función $\chi\psi : \mathbb{Z} \to \mathbb{C}$ dada por $(\chi\psi)(n) := \chi(n)\psi(n)$, para cada $n \in \mathbb{N}$. Es fácil comprobar que $\chi\psi$ es también un caracter de Dirichlet módulo m. Denotemos por $\mathcal{C}_m$ al conjunto de caracteres de Dirichlet módulo m. Entonces, resulta que, con el producto que acabamos de definir, el conjunto $\mathcal{C}_m$ es un grupo. Consideremos el caracter de Dirichlet χ_0 dado como sigue: para cada $n \in \mathbb{Z}$,

$$\chi_0(n) := \begin{cases} 0; & (n,m) > 1 \\ 1; & (n,m) = 1 \end{cases}$$

Es entonces fácil ver que en efecto $\chi_0 \in \mathcal{C}_m$, y que $\chi_0\chi = \chi\chi_0 = \chi, \ \ \forall\ \chi \in \mathcal{C}_m$. Por otra parte, para cada $\chi \in \mathcal{C}_m$, definimos χ^{-1} de modo que, para cada $n \in \mathbb{Z}$,

$$\chi^{-1}(n) := \begin{cases} 0; & (n,m) > 1 \\ \chi(n)^{-1}; & (n,m) = 1. \end{cases}$$

Resulta claro que $\chi^{-1} \in \mathcal{C}_m$ y que $\chi\chi^{-1} = \chi^{-1}\chi = \chi_0$. En conclusión, $\mathcal{C}_m$ es un grupo. Ahora bien, recordando que cada $\chi \in \mathcal{C}_m$ toma valores no nulos que son raíces de la unidad, resulta entonces claro que, tal y como está definido, $\chi^{-1}(n) = \overline{\chi(n)}, \ \forall\, n \in \mathbb{Z}$. Es por ello que, dado $\chi \in \mathcal{C}_m$, en ocasiones denotaremos a su inverso por $\overline{\chi} = \chi^{-1}$.

Surge la pregunta, ¿Qué estructura tiene el grupo $\mathcal{C}_m$? Esta pregunta es fácil de responder cuando $(\mathbb{Z}/m\mathbb{Z})^*$ es un grupo cíclico. En particular, si p es un número primo, entonces por el teorema 2.1.1, se tendrá que $(\mathbb{Z}/p\mathbb{Z})^*$ es un grupo cíclico, y la estructura de $\mathcal{C}_p$ será sencilla. Estudiemos el caso general: supóngase que $(\mathbb{Z}/m\mathbb{Z})^*$ es un grupo cíclico, y tomemos $n \in \mathbb{Z}$ tal que $n + m\mathbb{Z}$ es un generador de este grupo. Esto significa que $(n,m) = 1$ y que $\phi(m)$ es el mínimo entero positivo que satisface la congruencia $n^{\phi(m)} \equiv 1 \bmod m$. Tomemos también $\zeta_{\phi(m)}$ una raíz $\phi(m)$-ésima primitiva de la unidad. Sabemos que, para cada $\chi \in \mathcal{C}_m$, dado que $(n,m) = 1$, se tendrá que $\chi(n)$ es no nulo y es una raíz $\phi(m)$-ésima de la unidad. En consecuencia, existe un $e \in \mathbb{N}$, que además es único si pedimos que $0 \leq e < \phi(m)$, tal que $\chi(n) = \zeta^e_{\phi(m)}$. De hecho, χ queda completamente determinado por este entero e. En efecto, para cada $k \in \mathbb{Z}$, se tiene que, si $(k,m) > 1 \Rightarrow \chi(k) = 0$; mientras que si $(k,m) = 1$, entonces se tendrá que $k \equiv n^s \bmod m$ para algún entero $0 \leq s < \phi(m)$, de donde, para algún $t \in \mathbb{Z}$, $\chi(k) = \chi(n^s + tm) = \chi(n^s) = \chi(n)^s = (\zeta^e_{\phi(m)})^s = \zeta^{es}_{\phi(m)}$. Recíprocamente, para cada número entero $0 \leq e < \phi(m)$, existe el caracter $\chi_e \in \mathcal{C}_m$ que satisface

$$\chi_e(k) = \begin{cases} 0; & (k,m) > 1 \\ \zeta^{es}_{\phi(m)}; & (k,m) = 1 \text{ con } k \equiv n^s \bmod m. \end{cases}$$

Todo esto nos indica que hay una biyección entre $\mathcal{C}_m$ y los enteros s tales que $0 \leq s < \phi(m)$, en otras palabras, hemos demostrado que $|\mathcal{C}_m| = \phi(m)$. Más aún, si tomamos los χ_e como los acabamos de definir (básicamente, χ_e está caracterizado por el hecho de que $\chi_e(n) = \zeta^e_{\phi(m)}$), entonces observamos que para cada e, se tiene que $\chi_e = \chi_1^e$. En consecuencia, $\mathcal{C}_m$ es un grupo cíclico (generado por χ_1), al igual que $(\mathbb{Z}/m\mathbb{Z})^*$, teniendo ambos grupos orden $\phi(m)$, por consiguiente, $\mathcal{C}_m \cong (\mathbb{Z}/m\mathbb{Z})^*$.

De hecho, en general se cumple que $\mathcal{C}_m \cong (\mathbb{Z}/m\mathbb{Z})^*$, no obstante que el grupo $(\mathbb{Z}/m\mathbb{Z})^*$ no sea cíclico. Aunque no probaremos este hecho, indicaremos que la prueba en cuestión se basa principalmente en el hecho de que todo grupo abeliano puede escribirse como el producto directo de grupos cíclicos (ver [1], capítulo 3,

sección 1, teorema 3.1.6 (pp. 81-82)). Así pues, para $m \in \mathbb{Z}$ arbitrario, se tiene que $\mathcal{C}_m \cong (\mathbb{Z}/m\mathbb{Z})^* \cong \mathrm{Gal}\,(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. De modo que, si χ es un caracter de Dirichlet módulo m, entonces es posible considerar al homomorfismo "inductor" χ' como un homomorfismo de $\mathrm{Gal}\,(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ en $\mathbb{C}^*$. Sea K el campo fijo del kernel de χ, es decir, $K = \mathbb{Q}(\zeta_m)^{\ker(\chi')}$. Entonces, $K \subseteq \mathbb{Q}(\zeta_m)$, y este campo recibe el nombre de **campo perteneciente a** χ. Más en general, si X es un grupo finito de caracteres de Dirichlet módulo m, entonces consideremos H como la intersección de los kernels de los elementos de X, es decir, $H = \bigcap_{\chi \in X} \ker(\chi) = \{\sigma \in \mathrm{Gal}\,(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \,\big|\, \chi(\sigma) = 1, \ \forall\, \chi \in X\}$; y sea K el campo fijo de H, es decir, $K = \mathbb{Q}(\zeta_m)^H$. El campo K es llamado el **campo perteneciente a** X, y tenemos que $[K : \mathbb{Q}] = |X|$. De hecho, se tiene que $X \cong \mathrm{Gal}\,(K/\mathbb{Q})$. Si X es cíclico generado por χ, entonces el campo K perteneciente a X es precisamente el mismo que el campo perteneciente a χ, tal y como lo definimos antes.

Ahora bien, si $n, m \in \mathbb{Z}$ son tales que $n \mid m$, entonces, hay un homomorfismo natural $\varphi : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^*$ (a saber, $\varphi(k + n\mathbb{Z}) = k + m\mathbb{Z}$). Así, si se tiene un homomorfismo de grupos $\chi' : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$, que induzca el caracter de Dirichlet χ módulo n, tendremos además otro homomorfismo de grupos $\psi' := \chi' \circ \varphi : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$, que induce un caracter de Dirichlet módulo m, ψ, tal que $\psi(k) = \chi(k)$ para cualquier k tal que $(k, m) = 1$. En otras palabras, si se tiene un caracter de Dirichlet módulo m, y $n \mid m$, entonces es posible encontrar otro caracter de Dirichlet módulo n que tiene "menos ceros" que el caracter original. Esto nos sugiere lo siguiente: para cada homomorfismo de grupos χ', elegimos el mínimo entero positivo f_χ tal χ' induzca el caracter de Dirichlet χ módulo f_χ. Tal número f_χ recibe el nombre de **conductor** de χ, y todo caracter de Dirichlet módulo su conductor recibe el nombre de **primitivo**. Por otra parte, resulta a veces conveniente clasificar los caracteres de Dirichlet de la manera siguiente: si $\chi(-1) = -1$, entonces χ se denominará **impar**, mientras que si $\chi(-1) = 1$, entonces χ será denominado **par**. En ocasiones se escribe $\delta_\chi = 0$ si χ es par, y $\delta_\chi = 1$ si χ es impar. Es claro que el producto de dos caracteres pares o dos impares resulta ser un caracter par, mientras que al multiplicar un caracter par y uno impar, el resultado es un caracter impar. Así, si χ, ψ son caracteres de Dirichlet módulo un mismo entero m, podemos decir que $\delta_{\chi\psi} \equiv \delta_\chi + \delta_\psi \bmod 2$.

Mencionaremos la definición del discriminante de una extensión, dado que será útil de ahora en adelante.

Definición 3.3.2. *Sean E/K una extensión de Galois, y T la traza de dicha extensión. Si $x_1, \ldots, x_n$ es una base de E/K, entonces se define el* ***discriminante de la base*** *$x_1, \ldots, x_n$, denotado por $\Delta(x_1, \ldots, x_n)$ como el determinante* $\det(T(x_i x_j))$.

Es posible demostrar que, dada la extensión de Galois E/K, el número $\Delta(x_1, \ldots, x_n)$ es independiente de la elección de base. En consecuencia, hablamos del **discriminante de la extensión** E/F sin hacer referencia a la base de la extensión. Cuando se tiene K un campo numérico, hablamos del **discriminante de** K para referirnos al discriminante de $K/\mathbb{Q}$, y lo denotamos por $d(K)$. Finalizamos la exposición de los caracteres de Dirichlet enunciando sin demostración el siguiente teorema que involucra al discriminante de un campo numérico.

Teorema 3.3.1 (Fórmula del Conductor-Discriminante). *Sean X un grupo de caracteres de Dirichlet, y K el campo numérico perteneciente a X. Entonces, el discriminante de K viene dado por*

$$d(K) = (-1)^{r_2} \prod_{\chi \in X} f_\chi,$$

en donde $2r_2$ es el número de encajes complejos de K en $\mathbb{C}$.

Demostración: Puede verse en [20], capítulo 4 (pp. 35-36). □

En adelante mencionaremos brevemente lo que son las L-series, así como algunas propiedades de dichas series que, en general, no serán demostradas por ir más allá de la meta del presente trabajo.

Definición 3.3.3. *Sea χ un caracter de Dirichlet módulo m. Definimos la **L-serie de Dirichlet asociada a** χ, como la función de variable compleja $L(s, \chi)$ tal que, para cada $s \in \mathbb{C}$, con $\mathfrak{Re}(s) > 1$,*

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

Sea χ un caracter de Dirichlet módulo m. Dado que $|\chi(n)| = 1$, entonces se tiene que $|\chi(n)/n^s| \leq |1/n^s|$, de donde $|L(s, \chi)| \leq |\zeta(s)| < \infty$ para todos los $s \in \mathbb{C}$ tales que $\mathfrak{Re}(s) < 1$. Además, dado que χ es una función multiplicativa, se tiene para la L-serie correspondiente una fórmula análoga al producto de Euler de la función zeta de Riemann:

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \text{ es primo}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}. \tag{3.3.1}$$

De hecho, la función zeta de Riemann guarda una estrecha relación con la L-serie de Dirichlet asociada al caracter identidad χ_0. En efecto, consideremos el caracter de

Dirichlet identidad, χ_0, módulo m. Entonces, como $\chi_0(p) = 0$ para cualquier número primo p tal que $p \mid m$, de la ecuación 3.3.1 podremos deducir que

$$\begin{aligned} L(s,\chi_0) &= \prod_{p\nmid m}\left(1-\frac{1}{p^s}\right)^{-1} \\ &= \prod_{p\mid m}\left(1-\frac{1}{p^s}\right)\prod_{p}\left(1-\frac{1}{p^s}\right)^{-1} \\ &= \prod_{p\mid m}\left(1-\frac{1}{p^s}\right)\zeta(s). \end{aligned}$$

A continuación, enunciamos el resultado que muestra cómo los valores de las L-series vienen dados en términos de los así llamados números de Bernoulli generalizados.

Definición 3.3.4. *Sea χ un caracter de Dirichlet no trivial módulo su conductor m. Para cada $n \in \mathbb{N}\cup\{0\}$, se define el n-ésimo* ***número de Bernoulli generalizado****, denotado por $B_{n,\chi}$, mediante la siguiente fórmula:*

$$\sum_{a=1}^{m}\chi(a)\frac{te^{at}}{e^{mt}-1} = \sum_{n=0}^{\infty}\frac{B_{n,\chi}}{n!}t^n.$$

De la definición anterior, se sigue que los números $B_{k,\chi}$ se encuentran en el subcampo de $\mathbb{C}$ generado por los valores de χ. En particular, los $B_{k,\chi}$ son números algebraicos. Dado que definimos los números $B_{k,\chi}$ para caracteres de Dirichlet χ módulo su conductor, observamos que el caracter identidad χ_0 debe considerarse módulo 1. Así, dado el lema 1.2.1, los números B_{n,χ_0} vendrán dados por

$$\sum_{n=0}^{\infty}\frac{B_{n,\chi_0}}{n!}t^n = \frac{te^t}{e^t-1} = t+\frac{t}{e^t-1} = 1+\frac{1}{2}t+\sum_{n=2}^{\infty}\frac{B_n}{n!}t^n.$$

De modo que $-B_{1,\chi_0} = B_1$ y $B_{n,\chi_0} = B_n$, para $n \neq 2$. Es en este sentido, los números de Bernoulli generalizados, generalizan a los números de Bernoulli. Por otra parte, observemos lo que ocurre cuando, en la fórmula definitoria de los números de Bernoulli generalizados, intercambiamos t por $-t$:

$$\begin{aligned} \sum_{a=1}^{m}\chi(a)\frac{(-t)e^{-at}}{e^{-mt}-1}\cdot\frac{e^{mt}}{e^{mt}} &= \sum_{a=1}^{m}\chi(a)\frac{-te^{(m-a)t}}{1-e^{mt}} \\ &= \sum_{a=1}^{m}\chi(a)\frac{te^{(m-a)t}}{e^{mt}-1}. \end{aligned}$$

Haciendo el cambio de variable $a \mapsto m-a$, y tomando en cuenta que $\chi(0) = \chi(m) = 0$, la expresión anterior se convierte en

$$\sum_{a=0}^{m-1} \chi(m-a)\frac{te^{at}}{e^{mt}-1} = \sum_{a=0}^{m-1} \chi(-a)\frac{te^{at}}{e^{mt}-1} = \sum_{a=1}^{m} \chi(-1)\chi(a)\frac{te^{at}}{e^{mt}-1}.$$

De ahí que la función que define a los números de Bernoulli generalizados, será par o impar dependiendo de si el correspondiente caracter de Dirichlet χ es par o impar. De manera que, salvo en el caso cuando $\chi = \chi_0$, en general se tiene que $B_{2k+1,\chi} = 0$ cuando χ es par, y $B_{2k,\chi} = 0$ cuando χ es impar, para cualquier $k \in \mathbb{N}$. Esto se puede resumir diciendo que $B_{k,\chi} = 0$, cuando $k \not\equiv \delta_\chi \bmod 2$.

Proposición 3.3.2. *Sean χ un caracter de Dirichlet módulo su conductor m, y F cualquier múltiplo de m. Entonces,*

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

Demostración: Escribamos, de manera formal, la identidad $e^{Xt} = \sum_{n=0}^{\infty} X^n\frac{t^n}{n!}$. Entonces, de manera formal, el lema 1.2.1 nos dirá que

$$\begin{aligned}\frac{te^{Xt}}{e^t-1} &= \left(\sum_{n=0}^{\infty} B_n\frac{t^n}{n!}\right)\left(\sum_{n=0}^{\infty}\frac{X^nt^n}{n!}\right)\\ &= \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\frac{n!}{k!(n-k)!}B_kX^{n-k}\right)\frac{t^n}{n!}\\ &= \sum_{n=0}^{\infty} B_n(X)\frac{t^n}{n!}.\end{aligned}$$

Así pues, consideremos la siguiente suma infinita:

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

Hacemos un par de cambios de variable: tomamos $g = F/m$, y $a = b+cm$. Entonces, la expresión anterior se convierte en

$$\sum_{b=1}^{m} \sum_{c=0}^{g-1} \chi(b+cm) \frac{te^{(b+cm)t}}{e^{mgt}-1} = \sum_{b=1}^{m} \chi(b) \sum_{c=0}^{g-1} \frac{te^{(b+cm)t}}{e^{mgt}-1}.$$

Ahora bien,

$$\begin{aligned}\sum_{c=0}^{g-1} \frac{te^{(b+cm)t}}{e^{mgt}-1} &= \frac{te^{bt}(e^{mt}+e^{2mt}+\cdots+e^{(g-1)mt})}{e^{mgt}-1} \\ &= \frac{e^{gmt}-1}{e^{mt}-1} \cdot \frac{te^{bt}}{e^{gmt}-1}.\end{aligned}$$

Así, concluimos que

$$\sum_{n=0}^{\infty} \left(F^{n-1} \sum_{a=1}^{F} \chi(a) B_n\left(\frac{a}{F}\right) \right) \frac{t^n}{n!} = \sum_{b=1}^{m} \chi(b) \frac{te^{bt}}{e^{mt}-1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}$$

y la proposición se tiene. □

Teorema 3.3.2. *Sea χ un caracter de Dirichlet primitivo y sea $k \in \mathbb{N}$. Entonces, se tiene que*

$$L(1-k,\chi) = -\frac{B_{k,\chi}}{k}.$$

Demostración: Ver [9], capítulo 16, sección 6, proposición 16.6.12 (pp. 264-265), o bien [20], capítulo 4, teorema 4.2 (pp. 32-33). □

En ocasiones resulta útil cierta función, denotada por τ, que se conoce con el nombre de **suma de Gauss**. Dado un caracter de Dirichlet módulo m, se define

$$\tau(\chi) := \sum_{a=1}^{f_\chi} \chi(a) e^{2\pi i a/f_\chi}.$$

A continuación enunciamos una curiosa propiedad de las sumas de Gauss, que será utilizada más adelante. Para ello, recordemos que un campo numérico K se llama **totalmente real** si todos sus encajes en $\mathbb{C}$ yacen en $\mathbb{R}$, y **complejo** en caso contrario.

Proposición 3.3.3. *Sea K el campo perteneciente al grupo X de caracteres de Dirichlet. Entonces,*

$$\prod_{\chi\in X} \tau(\chi) = \begin{cases} \sqrt{|d(K)|}; & K \text{ es totalmente real} \\ i^{[K:\mathbb{Q}]/2}\sqrt{|d(K)|}; & K \text{ es complejo.} \end{cases}$$

Demostración: [20], capítulo 4, corolario 4.6 (pp. 36). □

La suma de Gauss está también involucrada en el cálculo de los valores de $L(1,\chi)$. En efecto, resulta que las L-series satisfacen la siguiente ecuación funcional, análoga a la de la función ζ ([20], capítulo 4, pp. 30)

$$\Gamma(s)\cos\left(\frac{\pi(s-\delta_\chi)}{2}\right) L(s,\chi) = \frac{\tau(\chi)}{2i^{\delta_\chi}}\left(\frac{2\pi}{f_\chi}\right)^s L(1-s,\overline{\chi}). \tag{3.3.2}$$

Como consecuencia de la ecuación (3.3.2), tenemos el siguiente teorema.

Teorema 3.3.3. *Sea χ un caracter de Dirichlet impar. Entonces, se tiene que*

$$L(1,\chi) = \pi i \frac{\tau(\chi)}{f_\chi} B_{1,\overline{\chi}}.$$

Demostración: Dado que χ es impar, se tiene que $\delta_\chi = 1$. Así, debido a la ecuación (3.3.2), con $s = 1$, observamos que, aplicando el teorema 3.3.2, se tiene que

$$\Gamma(1)\cos\left(\frac{\pi(1-1)}{2}\right) L(1,\chi) = \frac{\tau(\chi)}{2i}\left(\frac{2\pi}{f_\chi}\right) L(1-1,\overline{\chi}) = (-i)\tau(\chi)\frac{\pi}{f_\chi}(-B_{1,\overline{\chi}}).$$

Tomando en cuenta que $\Gamma(1) = \cos(0) = 1$, el resultado se sigue.

□

3.4. Fórmula para el número de clases

Definición 3.4.1. *Sea D un dominio Dedekind, e I un ideal de D. Entonces, se define la* ***norma del ideal*** *I como $N(I) := |D/I|$, la cantidad de elementos del anillo cociente.*

Teorema 3.4.1. *Sea K un campo numérico, y $\mathcal{O}_K$ su anillo de enteros. Entonces, para cualquier ideal I de $\mathcal{O}_K$, se tiene que $N(I) < \infty$.*

Demostración: Ver [9], capítulo 12, sección 2, proposición 12.2.3 (pp. 176). □

Definición 3.4.2. *Sean K un campo numérico, y $\mathcal{O}_K$ su anillo de enteros. Entonces, se define la* ***función zeta de Dedekind del campo*** *K, o simplemente* ***función zeta del campo*** *K como la función de la variable compleja s, con $\mathfrak{Re}(s) > 1$, dada por*

$$\zeta_K(s) := \sum_{\substack{\mathfrak{U} \text{ ideal de } \mathcal{O}_K \\ \mathfrak{U} \neq \langle 0 \rangle}} \frac{1}{N(\mathfrak{U})^s}.$$

Obsérvese que $\zeta_{\mathbb{Q}}$ no es otra cosa que la ya clásica función zeta de Riemann. De manera que el concepto de función zeta de un campo numérico, al igual que el concepto de L-serie, proporciona una generalización de la función zeta de Riemann. Dado un campo numérico K, su función zeta de Dedekind satisface una identidad análoga al producto de Euler:

$$\zeta_K(s) = \sum_{\substack{\mathfrak{U} \text{ ideal de } \mathcal{O}_K \\ \mathfrak{U} \neq \langle 0 \rangle}} \frac{1}{N(\mathfrak{U})^s} = \prod_{\mathfrak{P} \text{ ideal primo de } \mathcal{O}_K} \left(1 - \frac{1}{N(\mathfrak{P})^s}\right)^{-1}.$$

Definición 3.4.3. *Sean K un campo numérico, y r_1, $2r_2$ los números de encajes reales y complejos, respectivamente, de K en $\mathbb{C}$, de modo que $\sigma_1, \ldots, \sigma_{r_1}$ son los encajes reales y $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+1}}, \ldots, \overline{\sigma_{r_1+r_2}}$ sean los encajes complejos. Sea también $r = r_1 + r_2 - 1$, y tomemos un conjunto de generadores $\{u_1, \ldots, u_r\}$ en $\mathcal{O}_K^*$ del grupo cociente $\mathcal{O}_K^*/W$ (en donde W es el grupo de raíces de la unidad contenidas en K), además de denotar por $N_i = 1$ cuando σ_i es un encaje real y $N_i = 2$ cuando σ_i es un encaje complejo. Entonces, se define el* ***regulador de*** *K, denotado por* $\mathrm{Reg}\,(K)$*, como el número*

$$\mathrm{Reg}\,(K) := |\det(N_i \log|\sigma_i(u_j)|)_{1 \leq i,j \leq r}|.$$

Resulta que efectivamente el grupo $\mathcal{O}_K^*/W$ de la definición anterior, tiene orden r. Por otra parte, el número $\mathrm{Reg}\,(K)$ resulta ser independiente de la elección del conjunto de generadores.

Teorema 3.4.2 (Fórmula para el número de clases). *Sea K un campo numérico, y considérese su función zeta ζ_K. Entonces, ésta se puede extender a una función meromorfa en todo el plano complejo salvo el punto $s = 1$, en donde se encuentra un polo simple. Más aún, se tiene que*

$$\mathrm{Res}_{s=1}\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h(K) \mathrm{Reg}\,(K)}{w\sqrt{|d(K)|}}. \tag{3.4.1}$$

En donde r_1 es el número de encajes reales del campo K en $\mathbb{C}$, $2r_2$ es el número de encajes complejos, y w corresponde al número de raíces de la unidad contenidas en K.

Demostración: Ver [12], capítulo VIII, sección 2, pp. 160-161, en particular el teorema 5. □

Teorema 3.4.3. *Sean X un grupo de caracteres de Dirichlet, y K el campo perteneciente a X. Entonces, para cada $s \in \mathbb{C}\backslash\{1\}$, se tiene que*

$$\zeta_K(s) = \prod_{\chi \in X} L(s, \chi).$$

Demostración: Ver [20], capítulo 4, teorema 4.3 (pp. 34). □

Combinando el teorema 3.4.3 con la ecuación (3.4.1), tenemos que

$$\frac{2^{r_1}(2\pi)^{r_2} h(K)\mathrm{Reg}\,(K)}{w\sqrt{|d(K)|}} = \prod_{\substack{\chi \in X \\ \chi \neq \chi_0}} L(1, \chi) \tag{3.4.2}$$

para un campo numérico K perteneciente a un grupo de caracteres X. De este modo, tenemos (en teoría) un método para calcular el número de clases $h(K)$ del campo numérico K, siempre y cuando conozcamos el regulador $\mathrm{Reg}\,(K)$. Esto último en general es sumamente difícil, pues los cálculos involucrados son demasiado largos para ser prácticos. Sin embargo, existe una ingeniosa táctica, muy útil para obtener información acerca del número de clases, que consiste básicamente en factorizar dicho número en dos factores, uno de los cuales es "relativamente" fácil de trabajar. Lo primero que hay que hacer es darse cuenta de que, dado que cada campo $K \subseteq \mathbb{C}$ contiene a $\mathbb{Q}$, siempre es posible hablar de su subcampo real maximal, usualmente denotado por K^+ y dado por $K \cap \mathbb{R}$. Entonces, resulta que, si K pertenece al grupo de caracteres X, su subcampo real maximal K^+ será exactamente el campo perteneciente al grupo de caracteres $X^+ = \{\chi \in X \big| \delta_\chi = 0\}$, es decir, a los caracteres pares de X. Una consecuencia de esto es que, dado el campo K perteneciente al grupo de caracteres X, entonces $K \not\subseteq \mathbb{R} \Rightarrow \exists\, \chi \in X$ tal que $\delta_\chi = 1$. En otras palabras, todo campo numérico no real debe pertenecer a un grupo de caracteres tal que al menos un caracter sea impar. Más aún, en este caso, el grupo de caracteres en cuestión tendrá la mitad de caracteres pares y la mitad impares.

Un **CM-campo** es una extensión cuadrática totalmente imaginaria de un campo numérico totalmente real. Tales campos son obtenidos de campos numéricos totalmente reales al adjuntar una raíz cuadrada de un número cuyos conjugados son todos negativos. Todos los campos $\mathbb{Q}(\zeta_n)$ son CM-campos; sus subcampos reales maximales son $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, y son obtenidos de $\mathbb{Q}(\zeta_n)$ al adjuntar la raíz cuadrada de $\zeta_n^2 + \zeta_n^{-2} - 2$ (el discriminante del polinomio $X^2 - (\zeta_n + \zeta_n^{-1})X + 1$).

Teorema 3.4.4. *Sean K un CM-campo, y K^+ su subcampo real maximal. Entonces, $h(K^+) \mid h(K)$.*

Demostración: Ver [20], capítulo 4, teorema 4.10 (pp. 39). □

Dado un campo K, con K^+ su subcampo real maximal, es común denotar al número $h(K^+)$ como $h^+(K)$. Ahora bien, dado el teorema 3.4.4, entonces se tiene que el cociente $h(K)/h^+(K) \in \mathbb{Z}$. A dicho cociente se le denota como $h^-(K)$ y recibe el nombre de **número de clases relativo del campo** K.

A continuación introduciremos otra cantidad importante para el estudio de los campos numéricos. Dado un campo numérico K, se considera el grupo E de unidades del anillo de enteros $\mathcal{O}_K$, y el grupo análogo E^+ correspondiente a las unidades de $\mathcal{O}_{K^+}$. Por último, se considera el grupo W de las raíces de la unidad contenidas en K. Entonces, se define el número $Q(K)$ como $Q(K) := [E : WE^+]$. Es posible demostrar que $Q(K) = 1$ o 2 para cualquier CM-campo K; sin embargo, nosotros nos limitaremos a demostrar, más adelante, que $Q(\mathbb{Q}(\zeta_p)) = 1$, cuando p es un número primo. De momento, nos limitamos a enunciar una proposición que concierne a dicho número.

Proposición 3.4.1. *Sean K un CM-campo y K^+ su campo real maximal. Entonces, si $r = \frac{1}{2}[K : \mathbb{Q}] - 1$, se tiene que*

$$\frac{\mathrm{Reg}\,(K)}{\mathrm{Reg}\,(K+)} = \frac{1}{Q(K)} 2^r.$$

Demostración: [20], capítulo 4, proposición 4.16 (pp. 42). □

Teorema 3.4.5. *Sea K el campo perteneciente al grupo de caracteres de Dirichlet X. Entonces, se tiene que*

$$h^-(K) = Q(K) w \prod_{\substack{\chi \in X \\ \delta_\chi = 1}} \left(-\frac{1}{2} B_{1,\chi} \right),$$

en donde w es el número de raíces de la unidad presentes en el campo K.

Demostración: Sea $n = [K : \mathbb{Q}]$. Estamos suponiendo que K no es real, de modo que tiene n encajes complejos y ninguno real, mientras que K^+ tiene $n/2$ encajes reales. Por otra parte, es claro que el número de raíces de la unidad en K^+ es 2. En consecuencia, dada la ecuación (3.4.2), se tiene que

$$\prod_{\substack{\chi \in X \\ \chi \neq 1}} L(1, \chi) = \frac{(2\pi)^{n/2} h(K) \mathrm{Reg}\,(K)}{w \sqrt{|d(K)|}}, y$$

$$\prod_{\substack{\chi\in X\\ \delta_\chi=0\\ \chi\neq 1}} L(1,\chi)=\frac{2^{n/2}h^+(K)\mathrm{Reg}\,(K^+)}{2\sqrt{|d(K^+)|}}.$$

Dividiendo estas dos expresiones, y tomando en cuenta la proposición 3.4.1, tenemos que

$$\prod_{\substack{\chi\in X\\ \delta_\chi=1}} L(1,\chi)=\frac{\pi^{n/2}h^-(K)\frac{1}{Q(K)}2^{n/2-1}}{w/2\sqrt{|d(K)/d(K^+)|}}.$$

Dado que este último producto involucra únicamente caracteres impares, podemos aplicar el teorema 3.3.3, para obtener que

$$\frac{(2\pi)^{n/2}h^-(K)}{Q(K)w\sqrt{|d(K)/d(K^+)|}}=\prod_{\substack{\chi\in X\\ \delta_\chi=1}}\pi i\frac{\tau(\chi)}{f_\chi}B_{1,\overline{\chi}}.$$

Debido al teorema 3.3.1, tenemos que

$$|d(K)/d(K^+)|=\frac{\displaystyle\prod_{\chi\in X} f_\chi}{\displaystyle\prod_{\substack{\chi\in X\\ \delta_\chi=0}} f_\chi}=\prod_{\substack{\chi\in X\\ \delta_\chi=1}} f_\chi.$$

Tomando además en cuenta que el número de caracteres impares en X es $n/2$, tenemos que

$$\begin{aligned}\frac{(2\pi)^{n/2}h^-(K)}{Q(K)w\sqrt{|d(K)/d(K^+)|}} &= (\pi i)^{n/2}\frac{\displaystyle\prod_{\substack{\chi\in X\\ \delta_\chi=1}}\tau(\chi)}{\displaystyle\prod_{\substack{\chi\in X\\ \delta_\chi=1}} f_\chi}\prod_{\substack{\chi\in X\\ \delta_\chi=1}} B_{1,\overline{\chi}}\\ &= (\pi i)^{n/2}\frac{\displaystyle\prod_{\substack{\chi\in X\\ \delta_\chi=1}}\tau(\chi)}{|d(K)/d(K^+)|}\prod_{\substack{\chi\in X\\ \delta_\chi=1}} B_{1,\overline{\chi}}.\end{aligned}$$

Es decir, que

$$h^-(K)=Q(K)w\frac{(\pi i)^{n/2}}{(2\pi)^{n/2}}\frac{\displaystyle\prod_{\substack{\chi\in X\\ \delta_\chi=1}}\tau(\chi)}{\sqrt{|d(K)/d(K^+)|}}\prod_{\substack{\chi\in X\\ \delta_\chi=1}} B_{1,\overline{\chi}}.$$

Por otra parte, la proposición 3.3.3 implica que

$$\begin{aligned}\sqrt{\left|\frac{d(K)}{d(K^+)}\right|} &= \frac{\sqrt{|d(K)|}}{\sqrt{|d(K^+)|}} \\ &= \frac{i^{-n/2}\prod_{\chi\in X}\tau(\chi)}{\prod_{\substack{\chi\in X\\ \delta_\chi=0}}\tau(\chi)} \\ &= i^{-n/2}\prod_{\substack{\chi\in X\\ \delta_\chi=1}}\tau(\chi),\end{aligned}$$

de modo que tenemos

$$h^-(K) = Q(K)w\frac{i^n}{2^{n/2}}\prod_{\substack{\chi\in X\\ \delta_\chi=1}}B_{1,\overline{\chi}}.$$

Basta notar que $i^n/2^{n/2} = (-1/2)^{n/2}$ y repartir cada uno de los $-1/2$ en cada uno de los factores del producto, para obtener el resultado deseado. □

La importancia del teorema anterior radica en que proporciona una fórmula para el número de clases relativo que no involucra ni reguladores, ni otro tipo de cantidades difíciles de calcular. Por esto, la fórmula que proporciona dicho teorema es adecuada a nuestros propósitos. De ahora en adelante, comenzaremos a encaminar toda esta teoría hacia el caso particular de los campos ciclotómicos.

Lema 3.4.1. *Sea p un número primo. Entonces, $Q(\mathbb{Q}(\zeta_p)) = 1$.*

Demostración: Sea $E = \mathbb{Z}[\zeta_p]^*$, W el grupo de raíces de la unidad que se encuentran en $\mathbb{Q}(\zeta_p)$, y E^+ el grupo de unidades del anillo de enteros de $\mathbb{Q}(\zeta_p)^+$. Entonces, $Q(\mathbb{Q}(\zeta_p)) = [E : WE^+]$. Considérese el homomorfismo $\phi : E \to W$, dado por $\phi(\varepsilon) := \dfrac{\varepsilon}{\overline{\varepsilon}}, \quad \forall\, \varepsilon \in E$. Notemos que, para todos los encajes σ de $\mathbb{Q}(\zeta_p)$ en $\mathbb{C}$, se tiene que $\sigma(\overline{\varepsilon}) = \overline{\sigma(\varepsilon)}$. En consecuencia, $|\sigma(\phi(\varepsilon))| = 1, \quad \forall\, \sigma$, de modo que, por el lema 3.2.1, tenemos que efectivamente $\phi(\varepsilon) \in W, \quad \forall\, \varepsilon \in E$.
Consideremos el epimorfismo canónico $\varphi : W \to W/W^2$, con ayuda del cual podemos construir el homomorfismo $\psi = (\varphi \circ \phi) : E \to W/W^2$. Afirmamos que $\ker(\psi) = WE^+$. En efecto, tomemos $\varepsilon \in WE^+$, de modo que podemos escoger $\zeta \in W$ y $\varepsilon_1 \in E^+$ tales que $\varepsilon = \zeta\varepsilon_1$. Entonces,

$$\phi(\varepsilon) = \frac{\varepsilon}{\overline{\varepsilon}} = \frac{\zeta\varepsilon_1}{\overline{\zeta}\overline{\varepsilon_1}} = \zeta^2,$$

pues $(\overline{\zeta})^{-1} = \zeta$ y $\varepsilon_1 \in \mathbb{R}$ dado que $E^+ \subseteq \mathbb{R}$. Así, $\phi(\varepsilon) \in W^2 \Rightarrow \varepsilon \in \ker(\psi) \Rightarrow WE^+ \subseteq \ker(\psi)$. Ahora bien, sea $\varepsilon \in \ker(\psi)$. Entonces, eso significa que $\phi(\varepsilon) \in W^2$, de modo que podemos escoger $\zeta \in W$ tal que $\frac{\varepsilon}{\overline{\varepsilon}} = \phi(\varepsilon) = \zeta^2$. Tomemos $\varepsilon_1 = \zeta^{-1}\varepsilon$. De esta forma, tenemos que $\varepsilon_1 = \varepsilon\zeta^{-1} = \overline{\varepsilon}\zeta = \overline{\varepsilon_1}$, con lo cual $\varepsilon_1 \in \mathbb{R}$, y claramente ε_1 es una unidad cuyo inverso también se encuentra en $\mathbb{R}$. Esto significa que $\varepsilon_1 \in E^+$. De ahí que $\varepsilon = \zeta\varepsilon_1 \in WE^+ \Rightarrow \ker(\psi) \subseteq WE^+$. Por consiguiente, $\ker(\psi) = WE^+$ y así, del Primer teorema de Isomorfismos para grupos, se sigue que $E/WE^+ \cong \psi(E) = \phi(E)/W^2$. De este modo, si lográramos demostrar que $\phi(E) = W^2$, tendríamos que $E/WE^+ \cong W^2/W^2 = \langle e\rangle$, con lo cual $Q(\mathbb{Q}(\zeta_p)) = [E : WE^+] = |E/WE^+| = 1$. Ahora bien, de acuerdo con la demostración del lema 3.2.2, dado $\varepsilon \in \mathbb{Z}[\zeta_p]^* = E$, entonces $\phi(\varepsilon) = \frac{\varepsilon}{\overline{\varepsilon}} = +\zeta_p^i$, en donde $W = \{\pm\zeta_p^i | 0 \leq i < p\}$. En consecuencia, es claro que $\phi(\varepsilon) \in W^2 \Rightarrow \phi(E) \subseteq W^2$, de donde se sigue lo pedido. □

Sea p un número primo. En adelante, por ω nos referiremos a un generador del grupo de caracteres de Dirichlet módulo p, $\mathcal{C}_p \cong (\mathbb{Z}/p\mathbb{Z})^*$, el cual, como hemos comentado anteriormente, es cíclico. Entonces, ω es de orden $p-1$, y $\mathcal{C}_p = \{\chi_0, \omega, \omega^2, \cdots, \omega^{p-2}\}$. Es claro que el campo perteneciente al grupo $\mathcal{C}_p$ no es otro que $\mathbb{Q}(\zeta_p)$, el cual no es real. De modo que $\mathcal{C}_p$ debe contener caracteres impares. En consecuencia, necesariamente se tiene que ω es un caracter impar, y los caracteres impares de $\mathcal{C}_p$ son $\omega, \omega^3, \cdots, \omega^{p-2}$; mientras que los caracteres pares son $\chi_0 = \omega^0, \omega^2, \cdots, \omega^{p-3}$.

Proposición 3.4.2. *Sea p un número primo, y n un número impar, con $n \not\equiv -1 \bmod (p-1)$. Si ω es un generador del grupo $\mathcal{C}_p$, entonces se tiene que B_{1,ω^n} es un p-entero, y más aún, se cumple la siguiente congruencia dentro de $\mathbb{Z}_{\langle p\rangle}$:*

$$B_{1,\omega^n} \equiv \frac{B_{n+1}}{n+1} \bmod p.$$

Demostración: Ver [20], capítulo 5, sección 3, corolario 5.15 (pp. 61). □

A continuación, enunciamos el que muy probablemente es el más importante resultado de la presente sección.

Proposición 3.4.3. *Sea p un número primo impar. Entonces, $p \mid h^-(\mathbb{Q}(\zeta_p)) \iff p|U_j$, para algún $j = 2, 4, \cdots, p-3$; en donde U_j es el numerador del j-ésimo número de Bernoulli B_j.*

Demostración: Tomemos ω un generador del grupo $\mathcal{C}_p$. Entonces, los caracteres impares correspondientes a $\mathbb{Q}(\zeta_p)$ son exactamente $\omega, \omega^3, \cdots, \omega^{p-2}$. Por otra parte, el lema 3.4.1 afirma que $Q(\mathbb{Q}(\zeta_p)) = 1$. Además, por el corolario 3.1.1, sabemos que el número de raíces de la unidad contenidas en $\mathbb{Q}(\zeta_p)$ es exactamente $2p$. En consecuencia, el teorema 3.4.5 nos garantiza que

$$h^-(\mathbb{Q}(\zeta_p)) = 2p \prod_{j=1}^{(p-1)/2} \left(-\frac{1}{2} B_{1,\omega^{2j-1}} \right).$$

Ahora bien, debido a la proposición 3.4.2, sabemos que

$$\prod_{j=1}^{(p-3)/2} \left(-\frac{1}{2} B_{1,\omega^{2j-1}} \right) \equiv \prod_{j=1}^{(p-3)/2} \left(-\frac{1}{2} \cdot \frac{B_{2j}}{2j} \right) \mod p.$$

En consecuencia, tenemos que

$$h^-(\mathbb{Q}(\zeta_p)) \equiv 2p \left(-\frac{1}{2} B_{1,\omega^{p-2}} \right) \prod_{j=1}^{(p-3)/2} \left(-\frac{1}{2} \cdot \frac{B_{2j}}{2j} \right) \mod p.$$

Por otra parte, es posible demostrar, utilizando la teoría de los enteros p-ádicos (ver [20], capítulo 5), que $pB_{1,\omega^{p-2}} \equiv p - 1 \equiv -1 \mod p$. De esta forma, se tiene que $2p\left(-\frac{1}{2} B_{1,\omega^{p-2}} \right) \equiv 1 \mod p$, y por lo tanto

$$h^-(\mathbb{Q}(\zeta_p)) \equiv \prod_{j=1}^{(p-3)/2} \left(-\frac{1}{2} \cdot \frac{B_{2j}}{2j} \right) \mod p.$$

Esto significa que $h^-(\mathbb{Q}(\zeta_p)) \equiv 0 \mod p \iff$ para algún $j = 2, 4, \cdots, p-3$, se tiene que $-\frac{1}{2} \cdot \frac{B_j}{j} \equiv 0 \mod p \iff 1 \leq \operatorname{ord}_p \left(-\frac{1}{2} \cdot \frac{B_j}{j} \right) = \operatorname{ord}_p (1/2) + \operatorname{ord}_p (B_j/j) = \operatorname{ord}_p (B_j/j) \iff p \mid U_j$. □

Proposición 3.4.4. *Sea p un número primo impar. Si $p \mid h^+(\mathbb{Q}(\zeta_p))$, entonces $p \mid h^-(\mathbb{Q}(\zeta_p))$.*

Demostración: [20], capítulo 5, sección 6, teorema 5.34 (pp. 78-79). □

Hasta la fecha, no se conoce ningún número primo p tal que $p \mid h^+(\mathbb{Q}(\zeta_p))$. Se cree que esto nunca ocurre, y dicha creencia recibe el nombre de **conjetura de**

Vandiver. Las dos proposiciones anteriores conducen al siguiente teorema, el cual es fundamental para establecer el resultado principal del presente capítulo.

Teorema 3.4.6. *Sea p un número primo impar. Entonces, $p \mid h(\mathbb{Q}(\zeta_p)) \iff p$ es un número primo irregular.*

Demostración: $p \mid h(\mathbb{Q}(\zeta_p)) = h^+(\mathbb{Q}(\zeta_p))h^-(\mathbb{Q}(\zeta_p)) \iff p \mid h^+(\mathbb{Q}(\zeta_p))$ o $p \mid h^-(\mathbb{Q}(\zeta_p))$. Por la proposición 3.4.4, cualquiera de los dos casos significa que $p \mid h^-(\mathbb{Q}(\zeta_p))$, y por la proposición 3.4.3 esto último es equivalente a la irregularidad de p. □

3.5. Un caso particular del último teorema de Fermat

Pierre de Fermat conjeturó que, si $n \in \mathbb{N}$, con $n \geq 3$, entonces la ecuación

$$x^n + y^n = z^n \tag{3.5.1}$$

no tiene solución, con $x, y, z \in \mathbb{Z}\backslash\{0\}$. Esta conjetura, que fue demostrada por Wiles, se conoce con el nombre de **último teorema de Fermat** (y ya recibía ese nombre desde antes de que se hubiera demostrado). La ecuación (3.5.1) recibe el nombre de **ecuación de Fermat**.

Supóngase que se tiene una solución de la ecuación (3.5.1), es decir, que existen los números $x, y, z \in \mathbb{Z}\backslash\{0\}$ tales que $x^n + y^n = z^n$, y sea $d = (x, y, z)$. Entonces, los enteros no nulos $x/d, y/d, z/d$ serán otra solución para la ecuación (3.5.1). Es por ello que, para probar el último teorema de Fermat, basta demostrar que dicha ecuación no admite soluciones enteras x, y, z cuando $(x, y, z) = 1$.

Ahora bien, supóngase que, para algún $n \in \mathbb{N}$, $n \geq 3$, la ecuación (3.5.1) tiene una solución en los enteros no nulos x, y, z. Entonces, esto implicará que la ecuación (3.5.1) tiene solución para todo exponente m tal que $m \mid n$. En efecto, si $m \mid n$, esto significa que $x^{n/m}, y^{n/m}, z^{n/m} \in \mathbb{Z}$, con $\left(x^{n/m}\right)^m + \left(y^{n/m}\right)^m = \left(z^{n/m}\right)^m$. Dado que cualquier número natural $n \geq 3$ es divisible ya sea por 4 o por un número primo impar, entonces basta demostrar que la ecuación (3.5.1) no tiene solución cuando $n = 4$ o n es un número primo impar. El caso $n = 4$ fue demostrado por Fermat mismo, y esta demostración es una de las dos únicas que se le llegaron a conocer.

En la presente sección, observaremos la demostración del caso particular cuando el exponente de la ecuación (3.5.1) es un número primo regular. En otras palabras,

se demuestra que la ecuación $x^p + y^p = z^p$ no tiene solución con $x, y, z \in \mathbb{Z}\backslash\{0\}$ cuando p es un número primo regular. Con ello, en virtud del teorema 2.3.3, se habrá demostrado la inexistencia de soluciones de la ecuación (3.5.1) para aproximadamente el 61 % de los exponentes que son números primos impares. Hablando informalmente, diríamos que se demuestra "más de la mitad" del último teorema de Fermat.

Obsérvese que, si se tiene una solución entera no nula x, y, z para la ecuación (3.5.1), y p es un número primo que divide a dos de los números x, y, z, entonces necesariamente p dividirá al tercero de ellos. En efecto, supóngase que, por ejemplo, $p \mid x$ y $p \mid y$. Entonces, se tendrá que $p^n \left(\left(\frac{x}{p} \right)^n + \left(\frac{y}{p} \right)^n \right) = z^n \Rightarrow p \mid z^n \Rightarrow p \mid z$. Si, en cambio, $p \mid x$ y $p \mid z$, entonces se tendrá que $p^n \left(\left(\frac{z}{p} \right)^n - \left(\frac{x}{p} \right)^n \right) = y^n$, de donde se sigue un resultado análogo. En consecuencia, es posible concluir que, si $x, y, z \in \mathbb{Z}\backslash\{0\}$ son una solución de la ecuación de Fermat, y dos de los números x, y, z no son primos relativos, entonces $(x, y, z) \neq 1$. En otras palabras, se tiene que $(x, y, z) = 1 \Rightarrow (x, y) = (y, z) = (z, x) = 1$.

Es por ello que, si acaso hubiera soluciones enteras x, y, z para la ecuación $x^p + y^p = z^p$, con p un número primo, entonces si se tiene que $(x, y, z) = 1$, será imposible que p divida a dos o más de los números x, y, z. En consecuencia, se tienen dos posibilidades: o bien $p \nmid xyz$, o bien p divide a uno y sólo uno de los números x, y, z. La primera posibilidad recibe el nombre de **primer caso del último teorema de Fermat**, mientras que la segunda se conoce como **segundo caso del último teorema de Fermat**. En este último caso, sin pérdida de generalidad, se puede suponer que $p \mid z$, $p \nmid xy$. A continuación demostraremos que el primer caso no puede ocurrir, cuando el exponente p es un número primo regular. Como la demostración es por contradicción, comenzaremos por suponer que se tiene una solución de la ecuación de Fermat, y observaremos las implicaciones de tal suposición hasta llegar a una contradicción.

Suposición. *Se tiene que p es un número primo regular; y se tienen $x, y, z \in \mathbb{Z}$, con $(x, y, z) = 1$ y $p \nmid xyz$, tales que $x^p + y^p = z^p$.*

Observemos las implicaciones de la Suposición. En primer lugar, como ya se mencionó, dado que $(x, y, z) = 1$, entonces se tiene que $(x, y) = (y, z) = (z, x) = 1$. Por otra parte, como p es un número primo irregular, entonces, por el teorema 3.4.6, se tiene que $p \nmid h(\mathbb{Q}(\zeta_p))$. Esto significa, como se mencionó en la sección 3.2, que si I es cualquier ideal del anillo $\mathbb{Z}[\zeta_p]$ tal que I^p es un ideal principal, entonces necesariamente se tendrá que I es también un ideal principal.

Ahora bien, recordando que $X^p - 1 = (X-1)(X-\zeta_p)(X-\zeta_p^2)\cdots(X-\zeta_p^{p-1})$, haciendo $X = -x/y$ y multiplicando a ambos lados por $(-y)^p$, se obtiene que $x^p + y^p = (x+y)(x+\zeta_p y)(x+\zeta_p^2 y)\cdots(x+\zeta_p^{p-1}y)$. Dado que $x^p + y^p = z^p$, se sigue que, a nivel de ideales en $\mathbb{Z}[\zeta_p]$, se tiene la siguiente igualdad de ideales

$$\langle x+y\rangle\langle x+\zeta_p y\rangle\langle x+\zeta_p^2 y\rangle\cdots\langle x+\zeta_p^{p-1}y\rangle = \langle z\rangle^p. \tag{3.5.2}$$

Lema 3.5.1. *Si $i \not\equiv j \bmod p$, entonces los ideales $\langle x+\zeta_p^i y\rangle$ y $\langle x+\zeta_p^j y\rangle$ de $\mathbb{Z}[\zeta_p]$ son primos relativos.*

Demostración: Sea $A = \langle x+\zeta_p^i y\rangle + \langle x+\zeta_p^j y\rangle$. Entonces, $(\zeta_p^j - \zeta_p^i)y = (x+\zeta_p^j y) - (x+\zeta_p^i y) \in A$. Asimismo $\zeta_p^j(x+\zeta_p^i y), \zeta_p^i(x+\zeta_p^j y) \in A$, de modo que $(\zeta_p^j - \zeta_p^i)x = (\zeta_p^j x + \zeta_p^{i+j}y) - (\zeta_p^i x + \zeta_p^{i+j}y) \in A$. Como $(x,y) = 1$, existen $r, s \in \mathbb{Z}$ tales que $rx + sy = 1$. Por consiguiente, $\zeta_p^j - \zeta_p^i = r(\zeta_p^j - \zeta_p^i)x + s(\zeta_p^j - \zeta_p^i)y \in A$. Podemos, sin pérdida de generalidad, suponer que $i > j$. De ahí se sigue que $1 - \zeta_p^{i-j} = \zeta_p^{p-j}(\zeta_p^j - \zeta_p^i) \in A$, razón por la cual tendremos que $\langle 1-\zeta_p^{i-j}\rangle \subseteq A$.
Sin embargo, del corolario 3.1.2, sabemos que el ideal $\langle 1-\zeta_p^{i-j}\rangle$ es un ideal maximal, de donde se desprende que o bien $A = \langle 1-\zeta_p^{i-j}\rangle$ o bien $A = \mathbb{Z}[\zeta_p]$. Ahora bien, de la ecuación 3.5.2 se sigue que $z^p \in A$. Así, si suponemos que $A = \langle 1-\zeta_p^{i-j}\rangle$, tendremos que $z^p \in \langle 1-\zeta_p^{i-j}\rangle$, por lo cual $z^p = \alpha(1-\zeta_p^{i-j})$ para algún $\alpha \in \mathbb{Z}[\zeta_p]$. Entonces, tomando normas a ambos lados de esta última igualdad, vemos que

$$z^{p(p-1)} = N(z^p) = N(\alpha)N(1-\zeta_p^{i-j}) = N(\alpha)p,$$

es decir, se tiene que $p \mid z^{p(p-1)}$ en $\mathbb{Z}$. Siendo p un número primo, necesariamente se sigue que $p \mid z$, lo cual contradice la Suposición. Por lo tanto, concluimos que $\langle x+\zeta_p^i y\rangle + \langle x+\zeta_p^j y\rangle = A = \mathbb{Z}[\zeta_p]$ y por ello los ideales en cuestión son primos relativos. □

Corolario 3.5.1. *Los ideales del anillo $\mathbb{Z}[\zeta_p]$ de la forma $\langle x+\zeta_p^t y\rangle$, con $t \in \mathbb{Z}$, son potencias p-ésimas perfectas.*

Demostración: Dado que el anillo $\mathbb{Z}[\zeta_p]$ es un dominio Dedekind, entonces en él se cumple la factorización única de ideales como producto de ideales primos. Escribamos, pues, para cada $0 \le t \le p-1$, $\langle x+\zeta_p^t y\rangle = P_{1t}^{\alpha_{1t}} P_{2t}^{\alpha_{2t}} \cdots P_{n_t t}^{\alpha_{n_t t}}$, con los P_{it} ideales primos distintos entre sí. De hecho, por el lema 3.5.1, se tiene que todos los P_{ij} son distintos entre sí. Ahora bien, escribamos $\langle z\rangle = Q_1^{\beta_1} Q_2^{\beta_2} \cdots Q_m^{\beta_m}$, con los Q_i ideales primos distintos entre sí. De la ecuación 3.5.2, observamos que

$$\begin{aligned}\left(P_{10}^{\alpha_{10}} P_{20}^{\alpha_{20}} \cdots P_{n_0 0}^{\alpha_{n_0 0}}\right)\left(P_{11}^{\alpha_{11}} P_{21}^{\alpha_{21}} \cdots P_{n_1 1}^{\alpha_{n_1 1}}\right)\cdots \\ \left(P_{1(p-1)}^{\alpha_{1(p-1)}} P_{2(p-1)}^{\alpha_{2(p-1)}} \cdots P_{n_{p-1}(p-1)}^{\alpha_{n_{p-1}(p-1)}}\right) &= Q_1^{p\beta_1} Q_2^{p\beta_2} \cdots Q_m^{p\beta_m}.\end{aligned}$$

Como ya lo mencionamos, este tipo de factorizaciones son únicas salvo orden. De modo y manera que necesariamente se tendrá que, para cada $1 \leq i \leq m$, $Q_i = P_{jt}$ para algunos j, t, con $p\beta_i = \alpha_{jt}$, y viceversa, para cada par $1 \leq t \leq p-1$, $1 \leq j \leq n_t$, se tendrá que $P_{jt} = Q_i$, para algún i, con $p\beta_i = \alpha_{jt}$. Así que, escogiendo adecuadamente los números $1 \leq i_1, i_2, \cdots, i_{n_t}$, tendremos que

$$\begin{aligned} \langle x + \zeta_p^t y \rangle &= P_{1t}^{\alpha_{1t}} P_{2t}^{\alpha_{2t}} \cdots P_{n_t t}^{\alpha_{n_t t}} = \\ &= Q_{i_1}^{p\beta_{i_1}} Q_{i_2}^{p\beta_{i_2}} \cdots Q_{i_{n_t}}^{p\beta_{i_{n_t}}} = \left(Q_{i_1}^{\beta_{i_1}} Q_{i_2}^{\beta_{i_2}} \cdots Q_{i_{n_t}}^{\beta_{i_{n_t}}} \right)^p \end{aligned}$$

y tal cosa es lo que se aspiraba a demostrar. □

Lema 3.5.2. *Existen los elementos $\beta \in \mathbb{Z}[\zeta_p], u \in \mathbb{Z}[\zeta_p]^* \cap \mathbb{R}$ tales que $x + \zeta_p y = \zeta_p^s u\beta$, con $s \in \mathbb{Z}$ y $\beta \equiv n \bmod p$, para algún $n \in \mathbb{Z}$.*

Demostración: Del corolario 3.5.1, sabemos que existe un ideal $\mathcal{U}$ de $\mathbb{Z}[\zeta_p]$ tal que $\langle x + \zeta_p y \rangle = \mathcal{U}^p$, de manera que $\mathcal{U}^p$ es un ideal principal. Además, como $p \nmid h(\mathbb{Q}(\zeta_p))$, se sigue que $\mathcal{U}$ también es un ideal principal. Por consiguiente podemos escoger $\alpha \in \mathbb{Z}[\zeta_p]$ tal que $\mathcal{U} = \langle \alpha \rangle$. De ahí que $\langle x + \zeta_p y \rangle = \mathcal{U}^p = \langle \alpha \rangle^p = \langle \alpha^p \rangle$, de modo y manera que $x + \zeta_p y$ y α^p son asociados. Por lo tanto, hay un elemento $\varepsilon \in \mathbb{Z}[\zeta_p]^*$ tal que $x + \zeta_p y = \varepsilon \alpha^p$.

Ahora bien, podemos representar a α como $\alpha = \sum_{i=0}^{p-2} a_i \zeta_p^i$, con $a_i \in \mathbb{Z}\ \forall\ 0 \leq i \leq p-2$, con lo cual se tendrá que $\alpha^p = \left(\sum_{i=0}^{p-2} a_i \zeta_p^i \right)^p \equiv \sum_{i=0}^{p-2} a_i \bmod p$. Así que escogemos $n = \sum_{i=0}^{p-2} a_i \in \mathbb{Z}$, $\beta = \alpha^p$, para tener que $\beta \equiv n \bmod p$. Además, por el lema 3.2.2 existe un $t \in \mathbb{Z}$ tal que $\zeta_p^t \varepsilon \in \mathbb{R}$, por ello, si escogemos $u = \zeta_p^t \varepsilon \in \mathbb{Z}[\zeta_p]^* \cap \mathbb{R}$ y $s = p - t \in \mathbb{Z}$, tendremos que

$$x + \zeta_p y = \varepsilon\beta = \zeta_p^{p-t} \zeta_p^t \varepsilon\beta = \zeta_p^s u\beta,$$

con s, u, β satisfaciendo las condiciones solicitadas. □

Lema 3.5.3. *p divide a $x + \zeta_p y - \zeta_p^{2s} x - \zeta_p^{2s-1} y$ dentro del anillo $\mathbb{Z}[\zeta_p]$, en donde s es como en el lema 3.5.2.*

Demostración: Por el lema 3.5.2, se tiene que $x + \zeta_p y = \zeta_p^s u\beta$ para $\beta \in \mathbb{Z}[\zeta_p], u \in \mathbb{Z}[\zeta_p]^* \cap \mathbb{R}, s \in \mathbb{Z}$ y $\beta \equiv n \bmod p$ para algún $n \in \mathbb{Z}$. Tomando complejos conjugados

a ambos lados, obtenemos que $x+\zeta_p^{-1}y = \zeta_p^{-s}u\overline{\beta}$. Por lo tanto, $\zeta_p^{-s}(x+\zeta_p y)-\zeta_p^{s}(x+\zeta_p^{-1}y) = u\beta - u\overline{\beta} = u(\beta-\overline{\beta})$; pero $\beta \equiv \overline{\beta} \equiv n \bmod p$, de manera que $\zeta_p^{-s}(x+\zeta_p y)-\zeta_p^{s}(x+\zeta_p^{-1}y) = u(\beta-\overline{\beta}) \equiv u(n-n) \equiv 0 \bmod p \Rightarrow p \mid \zeta_p^{-s}(x+\zeta_p y)-\zeta_p^{s}(x+\zeta_p^{-1}y)$ en $\mathbb{Z}[\zeta_p]$. $\therefore$ multiplicando por ζ_p^s, obtenemos que $p \mid x+\zeta_p y-\zeta_p^{2s}x-\zeta_p^{2s-1}y$. □

Lema 3.5.4. *Supóngase que* $\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2} \in \mathbb{Z}[\zeta_p]$, *con* $a_i \in \mathbb{Z}$, $\forall\ 0 \le i \le p-2$. *Si* $n \in \mathbb{Z}$ *es tal que* $n \mid \alpha$, *entonces* $n \mid a_j$ *en* $\mathbb{Z}$, $\forall\ 0 \le j \le p-2$.

Demostración: Como $n \mid \alpha$, tenemos que $\alpha = n\beta$, para algún $\beta \in \mathbb{Z}[\zeta_p]$. Si escribimos $\beta = b_0 + b_1\zeta_p + \cdots + b_{p-2}\zeta_p^{p-2}$, con $b_j \in \mathbb{Z}$, tendremos entonces que

$$0 = \alpha - n\beta = (a_0 - nb_0) + (a_1 - nb_1)\zeta_p + \cdots + (a_{p-2} - nb_{p-2})\zeta_p^{p-2}.$$

Dado que el conjunto $\left\{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}\right\}$ es un conjunto $\mathbb{Z}$-linealmente independiente de $\mathbb{Z}[\zeta_p]$, tenemos entonces que $a_j - nb_j = 0$, para todos los $0 \le j \le p-2$, en otras palabras, $nb_j = a_j$ o $n \mid a_j$, $\forall\ 0 \le j \le p-2$. □

Finalmente, todas las consecuencias de la Suposición se conjugan para dar lugar a una contradicción, llegando al teorema siguiente.

Teorema 3.5.1. *Sea* p *un número primo regular. Entonces, la ecuación*

$$x^p + y^p = z^p,$$

con $p \nmid xyz$, *no tiene solución en enteros.*

Demostración: Si $p = 3$, entonces, como $3 \nmid x$ se sigue que $x^3 \equiv \pm 1 \bmod 9$, y lo mismo ocurre para y y para z. De este modo, $z^3 \equiv \pm 1 \bmod 9$, mientras que $x^3 + y^3 \equiv -2, 0$ o $2 \bmod 9$, lo cual es contradictorio. Así pues, podemos suponer que $p > 3$.
Ahora bien, del lema 3.5.3, sabemos que, tomando s como en el lema 3.5.2, se tiene que $p \mid x+\zeta_p y-\zeta_p^{2s}x-\zeta_p^{2s-1}y$ en $\mathbb{Z}[\zeta_p]$. Si los enteros ciclotómicos $1, \zeta_p, \zeta_p^{2s}, \zeta_p^{2s-1}$ son distintos entre sí, entonces, como $p \ge 5$, del lema 3.5.4 tendremos que $p \mid x$ y $p \mid y$, lo cual contradice la Suposición. Así pues, los números mencionados no son todos ellos distintos entre sí. Como $1 \ne \zeta_p$ y $\zeta_p^{2s} \ne \zeta_p^{2s-1}$, tenemos entonces tres casos:

(1) $1 = \zeta_p^{2s}$: En este caso, el enunciado del lema 3.5.3 se traduce en $p \mid x+\zeta_p y - x - \zeta_p^{-1}y = \zeta_p y - \zeta_p^{p-1}y$. Esto último, por el lema 3.5.4, significará que $p \mid y$, una contradicción.

(2) $1 = \zeta_p^{2s-1}$, o, equivalentemente, $\zeta_p = \zeta_p^{2s}$: En este segundo caso, conviene comenzar por demostrar que, siempre que se cumpla la ecuación de Fermat $x^p + y^p = z^p$, se puede suponer, sin pérdida de generalidad, que $x \not\equiv y \bmod p$. En efecto, comencemos suponiendo que $x \equiv y \equiv -z \bmod p$. Entonces, de la ecuación de Fermat obtendremos $-2z^p \equiv z^p \bmod p$ que equivale a $p \mid 3z^p$, lo cual no puede ser, pues de antemano supusimos $p \neq 3, p \nmid z$. Así pues, nuestra suposición inicial no se cumple, de donde se debe de tener que alguna de las tres $x \not\equiv y \bmod p$, $y \not\equiv -z \bmod p$ o $-z \not\equiv x \bmod p$ se cumple. Sin embargo, la ecuación de Fermat contiene de manera simétrica a x y a y, razón por la cual podemos suponer, sin pérdida de generalidad, que simplemente alguna de las dos $x \not\equiv y \bmod p$ o $x \not\equiv -z \bmod p$ se cumple. Pero en el último caso, reescribimos la ecuación de Fermat como $x^p + (-z)^p = (-y)^p$, y de esta forma $-z$ toma el papel de y y $-y$ el de z. En cualquier caso, obtenemos que $x \not\equiv y \bmod p$.

Ahora bien, en el caso que estamos tratando, lo que el lema 3.5.3 dice puede escribirse como $p \mid (x-y) - (x-y)\zeta_p$. Por el lema 3.5.4, esto implicará que $p \mid x-y$, es decir, $x \equiv y \bmod p$. Sin embargo, esto último entra en contradicción con lo demostrado anteriormente.

(3) $\zeta_p = \zeta_p^{2s-1}$: Si esto ocurre, el lema 3.5.3 se escribe como $p \mid x+\zeta_p y-\zeta_p^2 x-\zeta_p y = x-\zeta_p^2 x$, de modo que por el lema 3.5.4, tendremos que $p \mid x$, lo cual es absurdo.

En cualquiera de los tres casos, obtuvimos contradicciones, todas ellas nacidas de la Suposición. Es por ello que tal Suposición debe ser falsa, y el teorema se sigue.

□

Demostrar el segundo caso del último teorema de Fermat, cuando p es un número primo regular es algo bastante más complicado de lo que fue el primer caso, y se requiere teoría profunda que sobrepasa la meta del presente trabajo. En consecuencia, sólo mencionaremos el resultado correspondiente.

Teorema 3.5.2. *Sea p un número primo regular. Entonces, la ecuación*

$$x^p + y^p = z^p,$$

con $p \nmid xy$, $p \mid z$, $z \neq 0$, no tiene solución en enteros.

Demostración: Ver [20], capítulo 9, sección 1 (pp. 167-173); y sección 2, teorema 9.3 (pp.173-174). □

Es fácil ver que los teoremas 3.5.1 y 3.5.2, juntos, dan como resultado el siguiente teorema, el cual es el resultado principal de todo este capítulo.

Teorema 3.5.3. *Si p es un número primo regular, entonces la ecuación*

$$x^p + y^p = z^p,$$

no tiene solución para $x, y, z \in \mathbb{Z}\backslash\{0\}$.

□

Conclusiones

Después de observar todo aquello que se menciona en el presente trabajo de tesis, no es difícil concluir que los números de Bernoulli (junto con sus derivados, tales como los polinomios de Bernoulli, los números primos regulares o los números de Bernoulli generalizados), lejos de constituir un concepto estéril, resultan ser una herramienta poderosa para atacar importantes problemas dentro de la Teoría de Números. El hecho de aplicarlos a estos problemas, ha desembocado en importantísimas consecuencias, tales como el caso particular del último teorema de Fermat que se muestra en el tercer capítulo, y que hasta antes de Wiles, era lo más importante que se había hecho a este respecto. Por otra parte, los valores que se encontraron para la función zeta de Riemann arrojan luz sobre dicha función, la cual resulta ser una de las más importantes dentro de la Teoría de Números. Así, los números de Bernoulli no sólo tienen aplicaciones en Teoría de Números, sino que aparecen en el corazón mismo de esta rama de la matemática, relacionándose con varias de las nociones fundamentales de ésta. Por otra parte, desde el punto de vista histórico, los números de Bernoulli pasean codo a codo con varios de los principales conceptos de la matemática actual, por ejemplo con el concepto de ideal que, como vimos, surgió a raíz de los intentos de Kummer por demostrar el último teorema de Fermat. Así, finalmente, podemos concluir que, como reza el título de la presente tesis, los números de Bernoulli resultan de gran importancia, y tienen como consecuencia numerosas aplicaciones fundamentales, hermosas e interesantes dentro de la Teoría de Números.

Bibliografía

[1] Barrera Mora, Fernando, *Introducción a la teoría de grupos*, Universidad Autónoma del Estado de Hidalgo, 2004.

[2] Edwards, Harold M., *Fermat's Last Theorem*, Graduate Texts in Mathematics (50), Springer-Verlag, 1977.

[3] Edwards, Harold M., *The background of Kummer's proof of Fermat's Last Theorem for regular primes*, Arch. Hist. Exact. Sci. **14** (**3**) (1975), 219-236.

[4] Edwards, Harold M., *Postscript to "The background of Kummer's proof ..."*, Arch. Hist. Exact. Sci. **17** (**4**) (1977), 381-394.

[5] Edwards, Harold M., *Riemann's Zeta Function*, Academic Press, New York, 1974.

[6] Hernández Arellano, Fabián M., *Cálculo de probabilidades*, Aportaciones Matemáticas (25), Sociedad Matemática Mexicana, 2003.

[7] Hernández-Lerma, Onésimo y Hernández-del-Valle, Adrián, *Elementos de probabilidad y estadística*, Aportaciones Matemáticas (21), Sociedad Matemática Mexicana, 2003.

[8] Hungerford, T. W., *Algebra*, Springer-Verlag New York Inc., 1974.

[9] Ireland, Kenneth y Rosen, Michael, *A classical introduction to modern number theory*, Graduate Texts in Mathematics (84), Springer-Verlag, 1982.

[10] Janusz, Gerald J., *Algebraic Number Fields*, Graduate Studies in Mathematics (7), American Mathematical Society, Second Edition 1996.

[11] Karpilovsky, Gregory, *Field Theory*, Monographs and Textbooks in Pure an Applied Mathematics (120), Marcel Dekker, 1988.

[12] Lang, Serge, *Algebraic Number Theory*, Graduate Texts in Mathematics (110), Springer-Verlag, 1982.

[13] Rademacher, Hans, *Topics in analytic number theory*, Springer-Verlag, 1973.

[14] Ribenboim, Paulo, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, 1979.

[15] Ribenboim, Paulo, *The Book of Prime Number Records*, Springer-Verlag, 1980.

[16] Riemann, Bernhard, *Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse* (en inglés: *On the Number of Prime Numbers less than a Given Quantity*, trad. David R. Wilkins) , Monatsberichte der Berliner Akademie, Noviembre de 1859.

[17] Rudin, Walter, *Real and Complex Analysis* Second Edition, Mc. Graw Hill, 1966.

[18] Silverman, Richard A., *Introductory complex analysis*, Prentice-Hall, 1967.

[19] Titchmarsh, E. C., *The theory of the Riemann zeta-function*, Oxford University Press, 1951.

[20] Washington, Lawrence C., *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics (83), Springer-Verlag, 1982.

Índice alfabético