Universidad Nacional Autónoma de México

Facultad de Ciencias

LA FUNCIÓN TAU DE RAMANUJAN

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

MATEMÁTICO

P R E S E N T A:

CÉSAR ERNESTO RODRÍGUEZ ANGÓN

TUTOR
DR. VÍCTOR CUAUHTÉMOC GARCÍA HERNANDÉZ

Ciudad Universitaria, Cd. Mx., 2018

Hoja de datos del jurado

1. Datos del alumno:	1. Datos del alumno
Apellido paterno:	Rodríguez
Apellido materno:	Angón
Nombres:	César Ernesto
Universidad:	Universidad Nacional Autónoma de México
Facultad:	Facultad de Ciencias
Carrera:	Matemáticas
2. Datos del tutor	2. Datos del tutor
Grado:	Doctor
Nombres:	Víctor Cuauhtémoc
Apellido paterno:	García
Apellido materno:	Hernández
3. Datos del sinodal 1	3. Datos del sinodal 1
Grado:	Doctor
Nombre:	Alejandro
Apellido paterno:	Aguilar
Apellido materno:	Zavoznik
4. Datos del sinodal 2	4. Datos del sinodal 2
Grado:	Doctor
Nombre:	Omar
Apellido paterno:	Antolín
Apellido materno:	Camarena
5. Datos del sinodal 3	5. Datos del sinodal 3
Grado:	Maestro
Nombres:	José Antonio
Apellido paterno:	Gómez
Apellido materno:	Ortega
6. Datos del sinodal 4	6. Datos del sinodal 4
Grado:	Doctor
Nombre:	Adrián
Apellido paterno:	Zenteno
Apellido materno:	Gutiérrez
7. Datos del trabajo escrito	7. Datos del trabajo escrito
Título:	La función Tau de Ramanujan
Número de páginas:	92 p
Año:	2018

A mi familia.

Agradecimientos

Finalizar este trabajo representa el cumplimiento de un gran objetivo y esto habría sido imposible sin el apoyo de un gran número de personas.

Antes que nada, quisiera agradecer especialmente a mi madre, mi padre, mis hermanos, mi tía Emilia, mi tío Jorge y a mis primos ya que no solamente el apoyo de cada uno de ustedes ha sido vital para mí, sino que además han sido todos un gran de ejemplo de responsabilidad, solidaridad, tenacidad, creatividad, constancia y valentía. Ha sido siempre un enorme privilegio tenerlos a mi lado.
Agradezco también al resto de mi familia, particularmente a mis sobrinos que con su curiosidad e irreverencia son siempre una fuente de inspiración y una gran motivación a hacer siempre todo lo mejor posible.

Quisiera también agradecer a las personas que me acercaron e hicieron que me interesara por las matemáticas. Al profesor Víctor Pérez que me preparó para mis primeros concursos de matemáticas. A mis entrenadores de la olimpiada de matemáticas en el DF, Leo, Diego, Marco, y principalmente a Fernando que fue siempre un guía en todo lo que tenía que ver con la olimpiada de matemáticas, a Álvaro que me tenía mucha paciencia y siempre nos mostraba conexiones entre distintas áreas de las matemáticas, y a Toño que con sus entrenamientos en geometría me mostró que las matemáticas podían ser simples y elegantes.
En general estoy muy agradecido con la Olimpiada Mexicana de Matemáticas pues fue gracias a ella que conocí a las matemáticas y está repleta de personas muy entusiastas, profesores, organizadores y participantes, de quienes se aprende todos los días y entre los cuales he hecho muchos buenos amigos. El encontrarme con estas personas en ese ambiente me hizo decidirme a dedicarme a las matemáticas y me dio habilidades invaluables para mi desarrollo profesional.

De manera especial quisiera agradecer a Fernanda de quien aprendí muchas cosas, entre ellas la importancia y valor de la constancia y a caminar siempre en la dirección de mis sueños y metas.
De una forma más general, y ya que al tratar de hacer una lista seguramente omitiría algún nombre, quiero agradecer a todos mis amigos, que han estado en las buenas y las no tan buenas. La mayoría son siempre muy alegres y optimistas y eso se contagia. Muchas veces, hagan o no matemáticas, son ustedes quienes

me motivan a tratar de mejorar en lo que hago y en general a ser mejor persona.

Al mismo tiempo que este trabajo marca el fin de un proceso, también marca el inicio de una nueva etapa en mi desarrollo profesional por lo cual quiero agradecer a Víctor, por guiarme dentro de la teoría de números analítica y mostrarme algunas de las corrientes que esta ha tomado recientemente. Particularmente quiero agradecerle por proponerme el tema de esta tesis que por sus conexiones con distintas áreas y personajes de las matemáticas me ha resultado fantástico. El realizar este trabajo ha marcado un camino hacia donde me gustaría dirigirme profesionalmente en un futuro cercano. También quiero agradecer a Víctor por su gran disposición para platicar sobre la tesis y sobre matemáticas en general.

De igual forma agradezco a mis sinodales, Alejandro, Omar, José Antonio y Adrián por tan buena disposición para revisar mi tesis. Por sus observaciones y comentarios que ayudaron a mejorar este trabajo. Es para mí muy gratificante encontrarme con profesionales con tan buena relación con las matemáticas y que se dedican con mucho gusto a ellas.

Finalmente quiero agradecer a Denisse por ayudarme de tantas maneras a realizar este trabajo. Por su gran apoyo moral, por escucharme y ayudarme a ordenar las ideas, por apoyarme en corregir lo que ya estaba escrito, por su paciencia y tolerancia durante los días que mi carga de trabajo fue mayor. Además, agradezco a Michi, Mao y Juli quienes literalmente me acompañaron días y noches mientras escribía este trabajo.

¡Muchas gracias a todos!

Índice general

Introducción

En la publicación clásica [10] de 1916, Ramanujan introdujo la función τ, la cual está definida por la expansión en serie de potencias de un producto infinito:

$$\sum_{n=1}^{\infty} \tau(n) q^n = q \prod_{n=1}^{\infty} (1 - q^n)^{24}$$

que converge para $|q| < 1$. La función $\tau(n)$ es entonces una función que va de los enteros positivos a los enteros. En esta misma publicación, Ramanujan conjeturó propiedades aritméticas, recursivas y una estimación del orden de la función $\tau(n)$. Concretamente conjeturó:

1. $\tau(nm) = \tau(n)\tau(m)$ si $(n, m) = 1$, es decir que la función τ es multiplicativa.

2. Si p es un primo, entonces $\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1})$, para $n > 1$.

3. Si p es un primo, entonces $|\tau(p)| \leq 2p^{11/2}$.

Las primeras dos conjeturas de Ramanujan fueron probadas por Mordell en [9] en el año 1917. Sin embargo, la tercera conjetura permaneció sin prueba después de varios intentos por métodos analíticos hasta 1974, cuando Deligne la demostró como una consecuencia de su prueba de las conjeturas de Weil en [4]. Es decir, la prueba de la tercera conjetura de Ramanujan se obtuvo con métodos algebraicos.

Las conjeturas de Ramanujan y sus pruebas surgieron relacionadas a las formas modulares. En el siglo anterior al que Ramanujan realizó dichas conjeturas, Jacobi demostró que el producto infinito que determina los valores de la función τ es una forma modular cuspidal de peso 12. Las formas modulares a su vez, surgieron de manera natural dentro del estudio de Weierstrass de las funciones elípticas.

Demostrar que el producto infinito que define a la función τ converge sigue ideas naturales del análisis. Sin embargo no es tan simple ver que dicho producto es una forma modular cuspidal de peso 12, lo cual es esencial para poder probar las conjeturas de Ramanujan. De hecho, las propiedades de la función τ y los métodos para probar dichas propiedades pueden ser generalizados a los coeficientes de otras formas modulares y es en este sentido que la función τ de

Ramanujan cobra importancia. Por un lado, históricamente, las conjeturas de Ramanujan sobre la función τ y las pruebas dadas por Mordell de las primeras dos conjeturas mostraron la rica teoría que había detrás de las formas modulares y señalaron también un camino para su estudio sistemático. La prueba dada por Mordell de las conjeturas de Ramanujan fue retomada por Hecke y generalizada hasta definir lo que hoy se conoce como los operadores de Hecke. Por otro lado para poder definir con toda claridad la función τ necesitaremos desarrollar resultados y herramientas generales sobre las formas y las funciones modulares. Por lo anterior podríamos decir que la función τ fue una guía para el estudio de las formas modulares y en ese mismo sentido guiará este trabajo.

El objetivo principal de este trabajo es dar una demostración para las dos primeras conjeturas de Ramanujan sobre la función τ abordando el problema de manera elemental. También se presenta la demostración de Hecke para la estimación de coeficientes de formas modulares, en particular se sigue que $|\tau(p)| \leq Cp^6$, donde C es una constante absoluta positiva. Como aportación adicional esta tesis recupera algunas demostraciones que, si bien son referidas o esbozadas en la literatura de formas modulares, en general es difícil acceder a las referencias dadas, por lo que para escribir este trabajo reconstruimos algunas pruebas siguiendo los esbozos encontrados en [13] y [2]. A diferencia de otros textos que utilizan la teoría de funciones elípticas o de funciones en latices para desarrollar los resultados básicos sobre formas modulares como [2] o [13], en esta tesis obtendremos dichos resultados con herramientas de análisis complejo en una variable que en general son cubiertos en un primer curso de variable compleja.
La presente tesis ha sido divida en dos capítulos. El primero de ellos trata sobre formas modulares en general y en el segundo fijamos nuestra atención en la función τ de Ramanujan. Se ha procurado que el trabajo sea autocontenido.

En el Capítulo 1 introducimos las funciones modulares, que tienen como dominio el semiplano superior H de $\mathbb{C}$, para lo cual primero será necesario definir el grupo modular G. Haremos actuar al grupo modular G en H y mostraremos que bajo esta acción $D = \{z \in H : |z| \geq 1, |\Re(z)| \leq 1/2\}$ es un dominio fundamental para la acción de G en H. Posteriormente veremos que, por definición, una función modular $f(z)$ es holomorfa en H y tiene periodo 1, lo cual nos permitirá asociarle a $f(z)$ la función $\tilde{f}(q)$ con $q = e^{2\pi i z}$ de tal manera que $f(z) = \tilde{f}(q)$ que a su vez nos permitirá definir el valor de f en ∞ y asociarle a f una serie de potencias en q. Introduciremos las series de Eisenstein G_k y probaremos que G_k es una forma modular de peso $2k$. Después estudiaremos los espacio de las formas modulares de peso $2k$, calcularemos su dimensión y daremos una base para ellos que depende de las series de Eisenstein G_k. Además veremos que salvo múltiplos escalares, existe una única forma modular cuspidal de peso 12, $\Delta(z)$. Aprovecharemos para introducir el invariante modular j que, aunque no será de gran importancia para el trabajo en general, nos servirá para ejemplificar cómo se obtienen algunas relaciones entre funciones modulares. Encontraremos las expansiones de las series de Eisenstein $G_k(z) = \tilde{G}_k(q)$, con $q = e^{2\pi i z}$, alrededor de $q = 0$ y con ello daremos estimaciones del orden de los coeficientes de una forma modular. Finalmente probaremos que el producto infinito

$$q\prod_{n=1}^{\infty}(1-q^n)^{24}$$

es una forma modular cuspidal de peso 12, reconstruyendo la prueba esbozada por Serre en [13] y con esto veremos que al tener coeficiente en q igual a 1 y dado que el espacio de las formas modulares cuspidales de peso 12 es de dimensión 1, entonces dicho producto infinito determina los valores de la función $\tau(n)$.

En el Capítulo 2 reconstruiremos las pruebas de Mordell guiadas por Apostol en [2] sobre las primeras dos conjeturas de Ramanujan acerca de la función $\tau(n)$. Para ello nos fijaremos primero en el subgrupo asociado a N del grupo modular G, donde N es cualquier número natural. Además de probar que la función $\tau(n)$ es multiplicativa, daremos una identidad más fuerte que la multiplicatividad. Mostraremos, usando el espacio de las formas modulares de peso 12, la congruencia $\tau(n) \equiv \sigma_{11}(n) \pmod{691}$ y a la vez daremos una formula de recurrencia para encontrar los coeficientes del invariante modular j en términos de $\tau(n)$. Finalmente daremos algunos resultados que se obtienen al usar la formula de recurrencia

$$\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1})$$

y tratarla como una recurrencia lineal de grado 2 con términos enteros. Con esto y usando $|\tau(p)| \leq 2p^{11/2}$, hablaremos sobre la conjetura de Lehmer, que dice que $\tau(n) \neq 0$ para todo entero positivo n y veremos que el estudio sobre la conjetura de Lehmer se reduce a ver que para los primos p tales que $p \mid \tau(p)$ se tiene que $\tau(p) \neq 0$.

Capítulo 1

Formas modulares

1.1. El Grupo Modular

Denotamos con H el semiplano superior de $\mathbb{C}$, es decir el conjunto de los números complejos z con $\Im(z) > 0$.

Sea $SL_2(\mathbb{R})$ el grupo de las matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, con coeficientes reales tales que $ad - bc = 1$. Hacemos a $SL_2(\mathbb{R})$ actuar en $\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ de la siguiente forma: si $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ es un elemento de $SL_2(\mathbb{R})$, y si $z \in \overline{\mathbb{C}}$, hacemos $g(z) = \frac{az+b}{cz+d}$. Con la convención usual de que $z/0 = \infty$ si $z \neq 0$. Es claro que $g(z)$ está bien definida para todo $z \in \overline{\mathbb{C}}$ excepto para $z = -\frac{d}{c}$ y ∞. Extendemos nuestra definición para todo $z \in \overline{\mathbb{C}}$ haciendo:

$$f\left(-\frac{d}{c}\right) = \infty, \quad \text{y} \quad f(\infty) = \frac{a}{c}$$

Veamos que cuando hacemos a $SL_2(\mathbb{R})$ actuar de esta forma en $\overline{\mathbb{C}}$ obtenemos un automorfismo, y además $\Im(g(z)) = \frac{\Im(z)}{|cz+d|^2}$.

Lema 1.1.1. *Si $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ es un elemento de $SL_2(\mathbb{R})$, entonces g induce un automorfismo en $\overline{\mathbb{C}}$ y $\Im(gz) = \frac{\Im(z)}{|cz+d|^2}$ para todo $z \in \mathbb{C}\backslash\{-\frac{d}{c}\}$.*

Demostración. Supongamos que $z \neq \infty, -\frac{d}{c}$. Veamos primero que $2\Im(g(z)) = g(z) - \overline{g(z)}$, es decir $2\Im(g(z)) = \frac{az+b}{cz+d} - \frac{a\bar{z}+b}{c\bar{z}+d}$ ya que al ser a, b, c y d reales tenemos que $\overline{g(z)} = g(\bar{z})$, de donde tenemos que:

$$\begin{aligned} 2\Im(g(z)) &= \frac{az+b}{cz+d} - \frac{a\bar{z}+b}{c\bar{z}+d} \\ &= \frac{ac|z|^2 + bc\bar{z} + adz + bd - ac|z|^2 - bcz - ad\bar{z} - bd}{(cz+d)(\overline{cz+d})} \end{aligned}$$

lo cual al simplificar nos queda $\frac{(ad-bc)(z-\bar{z})}{|cz+d|^2}$ y al ser $ad-bc=1$ y $z-\bar{z}=2\Im(z)$ tenemos:

$$2\Im(g(z)) = \frac{2\Im(z)}{|cz+d|^2} \quad \text{lo cual implica que}$$

$$\Im(g(z)) = \frac{\Im(z)}{|cz+d|^2} \tag{1.1}$$

Lo anterior implica que si $g \in SL_2(\mathbb{R})$ y $z \in H$, entonces $g(z) \in H$. Por otro lado como

$$\begin{aligned} g(x) - g(y) &= \frac{ax+b}{cx+d} - \frac{ay+b}{cy+d} \\ &= \frac{acxy + bcy + adx + bd - acxy - bcx - ady - bd}{(cx+b)(cy+b)} \\ &= \frac{(ad-bc)(x-y)}{(cx+d)(cy+d)} = \frac{x-y}{(cx+d)(cy+d)} \end{aligned} \tag{1.2}$$

se tiene que g es inyectiva, pues si $z \neq \infty, -\frac{d}{c}$, entonces $g(x) = g(y)$ si y solo si (1.2) es igual a cero si y solo si $x = y$, además $g(z) = \infty$ si y solo si $z = -\frac{d}{c}$ y $g(z) = \frac{az+b}{cz+d} = \frac{a}{c} = g(\infty)$ $(z \in \mathbb{C})$ si y solo si $ad - bc = 0$ lo cual es una contradicción.
Finalmente sea $w \in \overline{\mathbb{C}}$ queremos encontrar $z \in \overline{\mathbb{C}}$ tal que $g(z) = w$. Si $w = \infty$, tenemos $g\left(-\dfrac{d}{c}\right) = \infty$ y $g^{-1}(\infty) = -\dfrac{d}{c}$. Si $w = \frac{a}{c}$ tenemos $g(\infty) = \dfrac{a}{c}$ y $g^{-1}\left(\dfrac{a}{c}\right) = \infty$. Si $w \neq \dfrac{a}{c}, \infty$, entonces queremos $w = \frac{az+b}{cz+d}$ pero, esto sucede si y solo si $czw + dw = az + b$ si y solo si $z(cw - a) = -dw + b$ si y solo si $z = \frac{-dw+b}{cw-a}$, esta última expresión es de hecho $g^{-1}(w)$ de donde la z buscada existe, por lo que g es suprayectiva en $\overline{\mathbb{C}}$ y además con lo anterior es fácil ver que $g^{-1}(g(z)) = z$, lo que nos dice que la acción está bien definida.
En resumen tenemos que la acción de $SL_2(\mathbb{R})$ en $\overline{\mathbb{C}}$ está bien definida, que si $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ es un elemento de $SL_2(\mathbb{R})$, entonces g induce un automorfismo en $\overline{\mathbb{C}}$ y como $g(z) \in H$ si $z \in H$, entonces de hecho g induce un automorfismo en su restricción en H.
Además obtuvimos la identidad

$$\Im(gz) = \frac{\Im(z)}{|cz+d|^2}$$

valida para todo $z \in H$ que será utilizada en varias ocasiones. ■

Notamos ahora que el elemento $-I_2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$ actúa trivialmente en H. Si $\mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{\pm I_2\}$ podemos considerara que es este grupo el que opera. Sea $SL_2(\mathbb{Z})$ el subgrupo de $SL_2(\mathbb{R})$ que consiste de matrices con elementos en $\mathbb{Z}$, tenemos la siguiente definición:

Definición 1.1.1. *El grupo $G = SL_2(\mathbb{Z})/\{\pm I_2\}$ es llamado el grupo modular; es la imagen de $SL_2(\mathbb{Z})$ en $PSL_2(\mathbb{R})$.*

Si $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ es un elemento de $SL_2(\mathbb{Z})$, usaremos frecuentemente el mismo símbolo para denotar su imagen en el grupo modular G.

Sean S y T los elementos de G definidos respectivamente por $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ y $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Se tiene que $S(z) = -1/z$, $T(z) = z + 1$, $S^2 = 1$ (es decir $S(S(z)) = z$) y $(ST)^3 = 1$. Todas estas afirmaciones son claras de la definición de S y T, excepto la última, veamos que es cierta pues:

$$\begin{aligned}
ST(z) &= S(T(z)) = S(z+1) = -\frac{1}{z+1} \\
(ST)^2(z) &= ST\Big(-\frac{1}{z+1}\Big) = S(T\Big(-\frac{1}{z+1}\Big) = S\Big(-\frac{1}{z+1}+1\Big) \\
&= S\Big(\frac{-1+z+1}{z+1}\Big) = S\Big(\frac{z}{z+1}\Big) = \frac{-1}{\frac{z}{z+1}} = \frac{-z-1}{z}
\end{aligned}$$

finalmente tenemos que

$$\begin{aligned}
(ST)^3(z) &= S\Big(T\Big(\frac{-z-1}{z}\Big)\Big) = S\Big(\frac{-z-1}{z}+1\Big) \\
&= S\Big(\frac{-z-1+z}{z}\Big) = S(-1/z) = \frac{-1}{\frac{-1}{z}} = z
\end{aligned}$$

como queríamos (de paso aquí vimos que $S^2 = 1$).

Por otro lado sea D el subconjunto de H formado por todos los puntos z tales que $|z| \geq 1$ y $|\Re(z)| \leq 1/2$. La siguiente figura muestra las transformaciones de D por los elementos $\{I_2, T, TS, ST^{-1}S, S, ST, STS, T^{-1}S, T^{-1}\}$ de G.

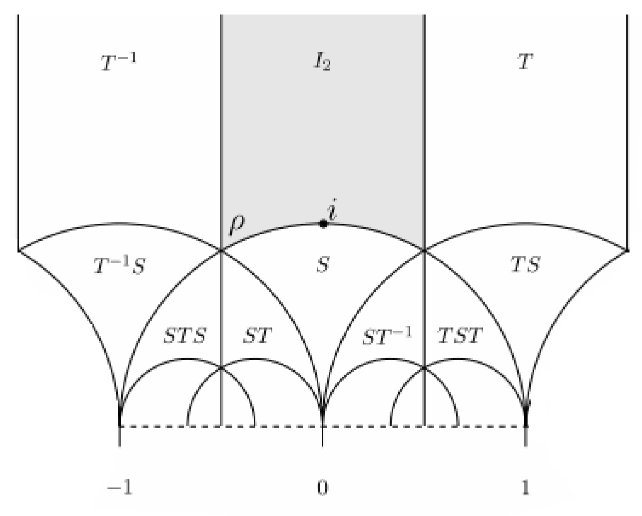

Figura 1.1: Transformaciones de D por elementos de G

Sean $z, z' \in H$, observemos que la relación $z \sim z'$ si existe $g \in G$ tal que $g(z) = z'$ es una relación de equivalencia. Lo anterior se sigue del hecho de que G es un grupo:

1. Es reflexiva. Para todo $z \in H$ se tiene $z \sim z$ pues $I_2(z) = z$.

2. Es transitiva. Si z, z' y z'' pertenecen a H y son tales que $z \sim z'$ y $z' \sim z''$, es decir, existen $g_1, g_2 \in G$ que cumplen $g_1(z) = z'$ y $g_2(z') = z''$, entonces $z \sim z''$ pues se tiene que $g_2(g_1(z)) = z''$ con $g_2\, g_1 = g_2 \circ g_1 \in G$ pues G es un grupo.

3. Es simétrica. Si $z, z' \in H$ y $g \in G$ tales que $g(z) = z'$ entonces, como G es un grupo, existe $g^{-1} \in G$ tal que $g^{-1}\, g = I_2$ y por lo tanto $z = g^{-1}(z')$ por lo que $z \sim z'$ si y solo si $z' \sim z$.

Vamos a demostrar que D es un dominio fundamental para la acción de G en el semiplano H. Más precisamente, probaremos que para todo $z \in H$ existe $g \in G$ tal que $g(z)$ pertenece a D, es decir todo $z \in H$ tiene un representante en D de su clase de equivalencia bajo la acción de H en G y además no existen dos elementos de D que pertenezcan a la misma clase de equivalencia de H/G, excepto para los elementos de la frontera de D. Lo anterior sera precisado en el siguiente teorema.

Teorema 1.1.2. *Sean H el semiplano superior y D la región fundamental.*

1. *Para toda $z \in H$ existe $g \in G$ tal que $g(z) \in D$.*

2. *Supongamos que dos puntos distintos z y z', de D son congruentes modulo G, entonces, $\Re(z) = \pm\frac{1}{2}$ y $z = z' \pm 1$ o $|z| = 1$ y $z' = -1/z$.*

3. *Sea $z \in D$ y sea $I(z) = \{g \in G : g(z) = z\}$, el estabilizador de z en G, se tienen $I(z) = 1$ excepto en los siguientes tres casos:*

   $z = i$, en cuyo caso I(z) es el grupo de orden dos generado por S;

   $z = \rho = e^{2\pi i/3}$, en cuyo caso $I(z)$ es el grupo de orden tres generado por ST;

   $z = -\bar{\rho} = e^{\pi i/3}$, en cuyo caso $I(z)$ es el grupo de orden tres generado por TS.

Demostración. Sea G' el subgrupo de G generado por S y T y sea $z \in H$. Vamos a demostrar que existe $g' \in G'$ tal que $g'(z) \in D$ y esto probará la primer afirmación del teorema. Si $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ es un elemento de G', entonces $\Im(gz) = \frac{\Im(z)}{|cz+d|^2}$, como c y d son enteros, el número de parejas (c, d) tales que $|cz + d|$ es menor que un número dado r son finitas ya que si $z = x + iy$, entonces $|cz + d|^2 = |(cx + d) + icy|^2 = (cx + d)^2 + (cy)^2$ lo que implica que si $|cy| > r$ entonces $|cz + d| > r$, por lo tanto existe finitos valores enteros de c tales que $|cz + d| < r$ y como se debe tener que $(cx + d)^2 < r^2$ y x es fijo, hay para cada c una cantidad finita de valores para d tales que la desigualdad se cumple y como hay solamente una cantidad finita de valores para c tales que se cumple la desigualdad, entonces hay una cantidad finita de parejas (c, d) tales que $|cz + d| < r$. Usando lo anterior podemos ver que existe $g \in G'$ tal que $\Im(g(z))$ es máxima, pues sea $r = 1$, como ya vimos existe una cantidad finita de parejas (c, d) tales que $|cz + d| < 1$, con c y d enteros y como $\Im(gz) = \frac{\Im(z)}{|cz+d|^2}$, existe por lo tanto un número finito de valores que puede tomar $\Im(g(z))$ tales que $\Im(g(z)) > \Im(z)$, pues si $|cz+d| \geq 1$, entonces $\Im(gz) = \frac{\Im(z)}{|cz+d|^2} \leq \frac{\Im(z)}{1} = \Im(z)$ y por lo tanto al haber solamente un número finito de valores para $\Im(g(z))$ tales que $\Im(g(z)) > \Im(z)$, entonces existe un valor máximo y por lo tanto un $g \in G'$ tal que $\Im(g(z))$ es máxima.

Elegimos $g \in G$ tal que $\Im(g(z))$ es máxima, y un n tal que $T^n \circ g(z)$ tiene parte real entre $-\frac{1}{2}$ y $\frac{1}{2}$. El elemento $z' = T^n \circ g(z)$ pertenece a D; de hecho es suficiente ver que $|z'| \geq 1$, pero, si $|z'| < 1$, entonces el elemento $-\frac{1}{z'} = S(z')$ tendría parte imaginaria estrictamente mayor que $\Im(z')$ y esto contradice el hecho de que $\Im(g(z)) = \Im(T^n \circ g(z))$ es máxima. Así, el elemento $g' = T^n \circ g \in G' \subset G$ cumple que $(T^n \circ g(z)) \in D$ lo cual demuestra (1).

Ahora demostraremos las afirmaciones (2) y (3) del teorema. Sean $z \in D$ y $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$, tal que $g(z) \in D$. Siendo libres de reemplazar (z, g) por $(g(z), g^{-1})$, podemos suponer, sin perdida de generalidad que $\Im(g(z)) \geq \Im(z)$ (pues si no, entonces $\Im(z) > \Im(g(z))$, es decir, tendríamos $\Im(g^{-1} \circ (g(z)) \geq \Im(g(z))$ y reemplazando obtendríamos nuevamente una expresión de la forma $\Im(g(w)) \geq \Im(w)$. Tenemos que $\Im(g(z)) = \frac{\Im(z)}{|cz+d|^2} \geq \Im(z)$, es decir $|cz + d| \leq 1$, y como $|cz + d| \geq |\Im(cz + d)| = |\Im(cz)| = |c|\Im(z) \geq |c|$, pues $\Im(z) \geq 1$, debemos tener $c = 0, 1$ o -1.

Resolveremos cada uno de esos casos de manera similar, donde lo que haremos será que dado c, acotaremos d y en caso de obtener algunos valores para d, separaremos nuevamente en casos, y una vez que tengamos un valor dado para d, entonces usaremos el hecho de que $ad - bc = 1$ para encontrar los posibles valores para a y b y recordando que como $\Re(z)$ está entre $-\frac{1}{2}$ y $\frac{1}{2}$, si z y z' son puntos de D tales que uno se obtiene del otro por una traslación (y por lo tanto son congruentes modulo G), entonces dicha traslación debe ser por 0, 1 o -1 para que tanto z como z' tengan parte real en $[-\frac{1}{2}, \frac{1}{2}]$ (recordemos que nuestras traslaciones son por números enteros). También, usaremos que $\rho + 1 = -\overline{\rho}$, que se sigue directamente del hecho de que $\rho = e^{2\pi i/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ y $-\overline{\rho} = e^{\pi i/3} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$ (lo cual también usaremos) y que $\rho = -\frac{1}{-\bar{\rho}}$, que equivale a $S(-\bar{\rho}) = \rho$ y $-\frac{1}{\rho} = S(\rho) = -\bar{\rho}$, que se siguen de multiplicar por $\bar{\rho}$ y ρ, respectivamente y de que $|\rho| = |\bar{\rho}| = 1$.

Caso $c = 0$. Si $c = 0$, entonces $d = \pm 1$, pues queremos $|0 \cdot c + d| = |d| \leq 1$ y como $(c, d) = 1$ (pues $ad - bc = 1$), se debe tener $d = \pm 1$. Ahora, usando que $ad - bc = 1$ y $c = 0$, $d = \pm 1$, tenemos que $ad = 1$ y por lo tanto $a = d = \pm 1$, y como $g \sim -g$ en G, podemos suponer sin perdida de generalidad que $g = \left(\begin{smallmatrix} 1 & \pm b \\ 0 & 1 \end{smallmatrix}\right)$, es decir $g(z) = z \pm b$ y entonces g es la traslación por $\pm b$. Por lo mencionado anteriormente $b = 0$ y entonces $g = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = I_2$ o $b = \pm 1$ y $g = \left(\begin{smallmatrix} 1 & \pm 1 \\ 0 & 1 \end{smallmatrix}\right) = T^{\pm 1}$, en cuyo caso uno de los números $\Re(z)$, $\Re(g(z))$ debe ser igual a $-1/2$ y el otro igual a $1/2$.

Caso $c = 1$. Si $c = 1$, tenemos $|cz + d| = |z + d| \leq 1$, y si $z = x + iy$, tenemos entonces que $x^2 + 2xd + d^2 + y^2 \leq 1$ y como $x^2 + y^2 = |z|^2 \geq 1$ y $|x| = |\Re(z)| \leq 1/2$, tenemos que $d^2 + 2xd \geq d^2 - \sqrt{d^2} = d^2 - |d| \geq 0$ (pues $d = 0$ o $|d| \geq 1$), y entonces $1 \geq x^2 + 2xd + d^2 + y^2 \geq 1 + 0 = 1$ por lo que las desigualdades deben ser igualdades y debe suceder que $d^2 + 2xd = d(d+2x) = 0$ y $x^2 + y^2 = 1$, por lo que se debe cumplir que $|z| = 1$ y $d = 0$ o $d + 2x = 0$ que sucede si y solo si $2x = -d$, como $x = \Re(z) \in [-\frac{1}{2}, \frac{1}{2}]$ y d es un entero, tenemos que $d = \pm 1$ (o $d = 0$ que ya fue contemplado).

Subcaso $c = 1, d = 0$. En este caso como nuestra restricción es que $|cz+d| \leq 1$ y substituyendo los valores de c y d tenemos simplemente $|z| \leq 1$ pero $|z| \geq 1$ porque $z \in D$, debemos tener $|z| = 1$ y $g = \left(\begin{smallmatrix} a & b \\ 1 & 0 \end{smallmatrix}\right)$, por lo que $a \cdot 0 - b \cdot 1 = 1$ y entonces $b = -1$, y así $g(z) = \frac{az-1}{z} = a - \frac{1}{z}$ y dado que $|z| = 1$ y $\Re(z) \in [-\frac{1}{2}, \frac{1}{2}]$, entonces $-1/z \in D$ ($|\frac{-1}{z}| = \frac{1}{|z|} = 1$ y $\Re(\frac{-1}{z}) = -\Re(z)$). Por lo tanto y por lo mencionado anteriormente para los puntos congruentes modulo una traslación en D, $a = 0$ y entonces $g = S$, excepto si $z = \rho$ o $z = -\overline{\rho}$. Si $z = \rho$, tenemos $g(\rho) = a - \frac{1}{\rho} = a - \overline{\rho}$ y entonces $a = 0$ (que ya se consideró y da $g = S$ o $a = -1$ y $g(\rho) = \rho$ y $g = \left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right) = (ST)^2$. Si $z = \overline{\rho}$, $g(-\overline{\rho}) = a - \frac{1}{\overline{\rho}} = a + \rho$ y nuevamente se debe tener $a = 0$ y $g = S$ o $a = 1$ y entonces $g(-\overline{\rho}) = -\overline{\rho}$ y $g = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right) = TS$

Subcaso $c = 1$, $d = 1$. En este subcaso, como ya teníamos que $2x = -d$, (o $d = 0$, pero en este subcaso eso no es posible) entonces $x = -1/2$ y como $|z| = 1 = x^2 + y^2$, al substituir el valor de x encontramos que $y = \pm\frac{\sqrt{3}}{2}$ pero, como $z \in H$, entonces $y > 0$ por lo que $y = \frac{\sqrt{3}}{2}$ y, tenemos que el único z tal que $z \in D$ y $|z+1| \leq 1$ es $z = \rho = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Tenemos en este caso que $g = \left(\begin{smallmatrix} a & b \\ 1 & 1 \end{smallmatrix}\right)$, que implica que $a \cdot 1 - 1 \cdot b = 1$, que a su vez implica que $b = a - 1$. Usando lo anterior tenemos que $g(\rho) = \frac{a\rho+b}{\rho+1} = \frac{a\rho+a-1}{\rho+1} = \frac{a(\rho+1)-1}{\rho+1} = a + -\frac{1}{\rho+1} = a - \frac{1}{-\overline{\rho}} = a + \rho$ y para que esto pertenezca a D, se debe tener $a = 0$ o $a = 1$. Si $a = 0$, entonces $g(\rho) = \rho$ y tenemos $0 \cdot 1 - b \cdot 1 = 1$ y entonces $b = -1$ y en este caso $g = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right) = ST$. Si $a = 1$, tenemos $1 \cdot 1 - 1 \cdot b = 1$ por lo que $b = 0$ y $g = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ y $g(\rho) = 1 + \rho = -\overline{\rho}$.

Subcaso $c = 1$ $d = -1$. Nuevamente en este subcaso, de manera análoga al subcaso anterior deducimos que $x = 1/2$ y $y = \frac{\sqrt{3}}{2}$, por lo que el único z tal que $z \in D$ y $|z - 1| \leq 1$ es $z = -\overline{\rho} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$. Tenemos en este caso que $g = \left(\begin{smallmatrix} a & b \\ 1 & -1 \end{smallmatrix}\right)$, que implica que $a \cdot (-1) - 1 \cdot b = 1$, que a su vez implica que $b = -a - 1$. Usando lo anterior tenemos que $g(-\overline{\rho}) = \frac{a\cdot(-\overline{\rho})+b}{-\overline{\rho}-1} = \frac{a\cdot(-\overline{\rho})-a-1}{-\overline{\rho}-1} = \frac{a(-\overline{\rho}-1)-1}{-\overline{\rho}-1} = a - \frac{1}{-\overline{\rho}-1} = a - \frac{1}{\rho} = a - \overline{\rho}$ y para que esto pertenezca a D se debe tener $a = 0$ o $a = -1$. Si $a = 0$, entonces $g(-\overline{\rho}) = -\overline{\rho}$ y $g = \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right) = (TS)^2$. Si $a = -1$, entonces $g(-\overline{\rho}) = -1 - \overline{\rho} = \rho$ y $(-1) \cdot (-1) - b \cdot 1$, de donde $b = 0$ y $g = \left(\begin{smallmatrix} -1 & 0 \\ 1 & -1 \end{smallmatrix}\right)$.

El Caso $c = -1$ se obtiene del caso $c = 1$ al cambiar los signos en a, b, c, d, que no cambia a g como elemento de G.

Lo anterior en efecto concluye la demostración de (2) y (3) pues, en los párrafos anteriores hemos demostrado que si un $z' = g(z)$ con $z, z' \in D$ (es decir si z es congruente a z' modulo G y ambos están en D), entonces $g = I$, $g = T^{\pm 1}$ o $|z| = 1$ y $g = S$, excepto si $z = \rho$ o $z = -\overline{\rho}$ y en estos caso $g(\rho) = \rho$, $g(\rho) = -\overline{\rho}$, $g(-\overline{\rho}) = \rho$ o $g(-\overline{\rho}) = -\overline{\rho}$. Los elementos de G que fijan ρ son I, ST y $(ST)^2$, es decir el subgrupo de orden 3 generado por ST. Los elementos de G que fijan a $-\overline{\rho}$ son I, TS y $(TS)^2$, es decir el subgrupo de orden 3 generado por TS. Finalmente notamos que $T^{\pm 1}$ no deja puntos fijos y que si $S(z) = z$, entonces $z = -\frac{1}{z}$ si y solo si $z^2 = -1$ si y solo si $z = \pm i$ y como sólo estamos considerando $z \in H$ entonces, $z = i$ es el único punto fijo de S. ■

Corolario 1.1.2.1. *El mapeo canónico $D \to H/G$ es suprayectivo y su restricción al interior de D es inyectivo.*

Demostración. El inciso 1 del (1.1.2) garantiza que el mapeo canónico $D \to G/H$ es suprayectivo y el inciso 2 del mismo teorema nos dice que si hay dos puntos en D congruentes, entonces pertenecen a la frontera de D, por lo tanto la restricción del mapeo al interior es inyectiva. ■

El corolario anterior nos dice justamente que D es un dominio fundamental para la acción de G en H.

Teorema 1.1.3. *El grupo G está generado por S y T.*

Demostración. Si G' es el subgrupo de G generado por S y T, vimos en la demostración del teorema 1 que para todo $z \in H$ existe $g \in G'$ tal que $g(z) \in D$. Si $g \in G$, elegimos un punto z_0 en el interior de D y sean $z = g(z_0)$ y $g' \in G'$ tal que $g'(z) \in D$, los puntos z_0 y $g'(z) = g' \circ g(z_0)$ son congruentes modulo G y uno de ellos es interior a D, la parte (2) del teorema 1 nos dice que debe ser $g'(z) = g' \circ g(z_0) = z_0$ y como z_0 es interior, por la parte (3) del Teorema 1 se tiene que $g' \circ g = I$, por lo tanto $g \in G'$ y entonces $G \subset G' \subset G$ y así $G = G' = \langle S, T \rangle$. ■

1.2. Funciones modulares

Definición 1.2.1. *Sea k un entero, decimos que una función es débilmente modular de peso $2k$ si es meromorfa en el semiplano H y verifica la relación*

$$f(z) = (cz+d)^{-2k} f\left(\frac{az+b}{cz+d}\right) \text{ para toda } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \tag{1.3}$$

Dado que sabemos que G está generado por S y T, es suficiente revisar la invarianza por S y T, es decir tenemos la siguiente proposición.

Proposición 1.2.1. *Si f es meromorfa en H, entonces la función f es una función débilmente modular de peso $2k$ si y solo si satisface las siguientes dos relaciones*

$$f(z+1) = f(T(z)) = f(z) \tag{1.4}$$

$$f(-1/z) = f(S(z)) = z^{2k} f(z) \tag{1.5}$$

Demostración. Lo anterior se sigue de la definición 1.2.1 y del hecho de que S y T generan G. Para hacer esto más claro supongamos que

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

y que se cumple

$$f(z) = (cz+d)^{-2k} f\left(\frac{az+b}{cz+d}\right)$$

si $g_1 = T^k g$ y $g_2 = Sg$, entonces

$$g_1 = \begin{pmatrix} a+kc & b+kd \\ c & d \end{pmatrix}$$
$$g_2 = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}$$

y dado que por hipótesis se tiene $f(g_1(z)) = f(T^k g(z)) = f(g(z))$ y $f(g_2(z)) = f(Sg(z)) = g(z)^{2k} f(g(z))$, entonces

$$\begin{aligned} f(g_1(z)) &= f(g(z)) = (cz+d)^{2k} f(z) \\ f(g_2(z)) &= \left(\frac{az+b}{cz+d}\right)^{2k} \cdot f(g(z)) \\ &= \left(\frac{az+b}{cz+d}\right)^{2k} \cdot (cz+d)^{2k} f(z) \\ &= (az+b)^{2k} f(z) \end{aligned}$$

de donde se sigue que si g cumple la ecuación (1.3), entonces también la cumplen $T^k g$ y Sg y como S y T generan G, se tiene el resultado. ■

Supongamos que f es meromorfa en H y la relación (1.4) se cumple. Dado que

$$e^{2\pi iz} = e^{2\pi iz'} \iff e^{2\pi i(z-z')} = 1 \iff z - z' \in \mathbb{Z}$$

si consideramos $R = \{z \in H : -1/2 < \Re(z) \leq 1/2\}$, la función $q(z) = e^{2\pi iz}$, establece una biyección analítica (un biholomorfismo) entre la región R y el disco unitario sin el cero U^*. Lo anterior es cierto ya que no hay dos elementos de R tales que su diferencia sea un entero, entonces el mapeo $q(z) = e^{2\pi iz}$ con dominio R es inyectivo y claramente es una función holomorfa. Más aún si $z \in R$ con $z = x + iy$, entonces

$$q(z) = e^{-2\pi y + 2\pi ix}$$

y como $-1/2 < x = \Re(z) \leq 1/2$, entonces $-\pi < 2\pi x \leq \pi$, es decir el argumento de $q(z)$ puede tomar cualquier valor en $(-\pi, \pi]$. Por otro lado $0 < y$ puede tomar

cualquier valor positivo, por lo que el modulo de $q(z)$ puede tomar cualquier valor en $(0,1)$. Se sigue que $q : H \to U^*$ es suprayectiva y al ser inyectiva y holomorfa, se tiene que la inversa está bien definida y es holomorfa.
Sea $q \in U^*$, vimos que existe un único $z \in R$ tal que $q = e^{2\pi iz}$ y por lo tanto la función $\tilde{f}(q) := f(z)$ está bien definida en U^* y más aún, dado que el mapeo definido que transforma R en U^* es una biyección analítica y f es meromorfa en R, entonces $\tilde{f}(q)$ es meromorfa en U^*. Finalmente como estamos suponiendo que $f(z+1) = f(z)$ y $e^{2\pi i(z+1)} = e^{2\pi iz}$, podemos ahora extender nuestra definición para todo $z \in H$ haciendo $q = e^{2\pi iz}$ y haciendo $\tilde{f}(q) := f(z)$ y trabajar equivalentemente con $f : H \to \overline{\mathbb{C}}$ o $\tilde{f} : U^* \to \overline{\mathbb{C}}$, ya que si $z_1 \in H$, entonces existen $z \in R$ y $k \in \mathbb{Z}$ tales que $z_1 = z + k$ y por lo tanto para todo $z_1 \in H$ se tiene

$$f(z_1) = f(z+k) = f(z) = \tilde{f}(e^{2\pi iz}) = \tilde{f}(e^{2\pi i(z+k)}) = \tilde{f}(e^{2\pi iz_1})$$

Observe que si $z \in H$, entonces $z \to \infty$, si y sólo si $q \to 0$.
Si $\tilde{f}$ se extiende a una función meromorfa (respectivamente holomorfa) en el origen, diremos, por abuso de lenguaje, que f es meromorfa (respectivamente holomorfa) en infinito. Esto significa que $\tilde{f}$ admite una expansión de Laurent[1] en una vecindad del origen:

$$\tilde{f}(q) = \sum_{-\infty}^{\infty} a_n q^n$$

donde los a_n son 0 para n suficientemente pequeña (respectivamente para $n < 0$).

También nos referiremos a $\tilde{f}$ como la expansión de Fourier de f. Algunas de las razones para esto son: ser menos repetitivos con la terminología, que dicho término es de uso frecuente en la literatura relacionada al tema y, por supuesto que de hecho al ser f $1-periodica$ la expansión de $\tilde{f}$ es la expansión de Fourier de f como se puede consultar en [1] pp. 263-264.

Definición 1.2.2. *Una función débilmente modular es llamada modular si es meromorfa en infinito. Cuando f es holomorfa en infinito, definimos $f(\infty) = \tilde{f}(0)$. Este es el valor de f en infinito.*

Definición 1.2.3. *Una función modular que es holomorfa en todos los puntos (incluyendo en infinito) es llamada una forma modular; si tal función es cero en infinito, diremos que es una forma cuspidal.*
Una forma modular de peso $2k$ está entonces dada por una serie

$$f(z) = \sum_{n=0}^{\infty} a_n q^n = \sum_{n=0}^{\infty} a_n e^{2\pi inz} \tag{1.6}$$

la cual converge para $|q| < 1$ (es decir para $\Im(z) > 0$), y la cual verifica la identidad

$$f(-1/z) = z^{2k} f(z) \tag{1.7}$$

[1] Para más detalles sobre la expansión de Laurent se puede consultar [11] pp. 305-306 o [3] pp. 107-109

y es una forma cuspidal si $a_0 = 0$.

Un caso sencillo pero que vale la pena notar, es la siguiente proposición.

Proposición 1.2.2. *Si* f *y* f' *son formas modulares de pesos* $2k$ *y* $2k'$*, respectivamente, entonces* ff' *es una forma modular de peso* $2k + 2k'$ *y si* $k = k'$*, entonces* $f + f'$ *es una forma modular de peso* $2k$*.*

Demostración. La proposición se sigue directamente de la ecuación (1.3) y de que f y f' son ambas formas modulares de pesos $2k$ y $2k'$, respectivamente, ya que en ese caso se tiene

$$f(z) = (cz+d)^{-2k} f\left(\frac{az+b}{cz+d}\right) \quad \textit{para toda} \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$$
$$f'(z) = (cz+d)^{-2k'} f\left(\frac{az+b}{cz+d}\right) \quad \textit{para toda} \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$$

de donde se sigue que

$$\begin{aligned} f(z)f'(z) &= (cz+d)^{-2k}(cz+d)^{-2k'} f\left(\frac{az+b}{cz+d}\right) f'\left(\frac{az+b}{cz+d}\right) \\ &= (cz+d)^{-2(k+k')} f\left(\frac{az+b}{cz+d}\right) f'\left(\frac{az+b}{cz+d}\right) \end{aligned}$$
$$\textit{para toda} \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$$

además si $k = k'$ se tiene

$$\begin{aligned} f(z) + f'(z) &= (cz+d)^{-2k} f\left(\frac{az+b}{cz+d}\right) + (cz+d)^{-2k} f'\left(\frac{az+b}{cz+d}\right) \\ &= (cz+d)^{-2k}\left(f\left(\frac{az+b}{cz+d}\right) + f'\left(\frac{az+b}{cz+d}\right)\right) \end{aligned}$$
$$\textit{para toda} \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$$

■

Observemos que 0 es una forma modular de peso $2k$ para todo entero $k > 1$ y que si f es una forma modular de peso $2k$, entonces $-f$ es una forma modular de peso $2k$. Lo anterior, combinado con la proposición 1.2.2, nos dice que las formas modulares de peso $2k$ forman un $\mathbb{C}-$espacio vectorial.

1.2.1. Serie de Eisenstein

Ahora introduciremos las series de Eisenstein $G_k(z)$ que están definidas para todo entero $k > 1$. Como veremos a continuación la serie de Eisenstein $G_k(z)$

es una forma modular de peso $2k$. Las series de Eisenstein juegan un papel importante dentro de las formas modulares y fueron por mucho tiempo las únicas formas modulares conocidas de manera explícita. Con ellas se pueden obtener más formas modulares usando la proposición 1.2.2, de hecho, como se verá más adelante, nos bastarán G_2 y G_3 para generar el espacio de las formas modulares de peso $2k$ para todo entero k.

Definición 1.2.4. *Sea k un entero mayor que 1 y $z \in H$. Definimos la serie de Eisenstein de peso k como*

$$G_k(z) = \sum_{\substack{n,m\in\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{(mz+n)^{2k}} \tag{1.8}$$

donde n y m corren sobre todas las parejas de enteros no ambos cero.

Esperando que no haya confusión y con el fin de simplificar la notación usaremos también la siguiente notación para la serie de Eisenstein:

$$G_k(z) = \sum_{n,m} \frac{1}{(mz+n)^{2k}} \tag{1.9}$$

ya que las series de Eisenstein aparecerán frecuentemente a lo largo del trabajo. Notemos que en la definición de la serie de Eisenstein de peso $2k$ no se ha especificado un orden en el que la suma

$$G_k(z) = \sum_{\substack{n,m\in\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{(mz+n)^{2k}}$$

debe efectuarse. Lo anterior es porque, como veremos en el lema siguiente, la serie de Eisenstein de peso $2k$ con k un entero mayor que 1, converge absolutamente en H y por lo tanto el valor de $G_k(z)$ es independiente de el orden en el que se efectúe la suma de sus términos.

Lema 1.2.1. *Para todo $z \in H$ se tiene que*

$$G_{\alpha/2}(z) = \sum_{\substack{n,m\in\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{(mz+n)^{\alpha}}$$

converge absolutamente si y solo si $\alpha > 2$

Demostración. Sea k un entero positivo consideremos los paralelogramos

$$P_k = \{mz+n \,:\, -k \leq m,n \leq k,\, (m,n) \neq (0,0)\}$$

que tienen sus vértices de la forma $\pm kz \pm k$ (obsérvese la figura 2.2) y contemos cuantos w de la forma $w = mz + n$ están sobre el perímetro de P_k. Los puntos

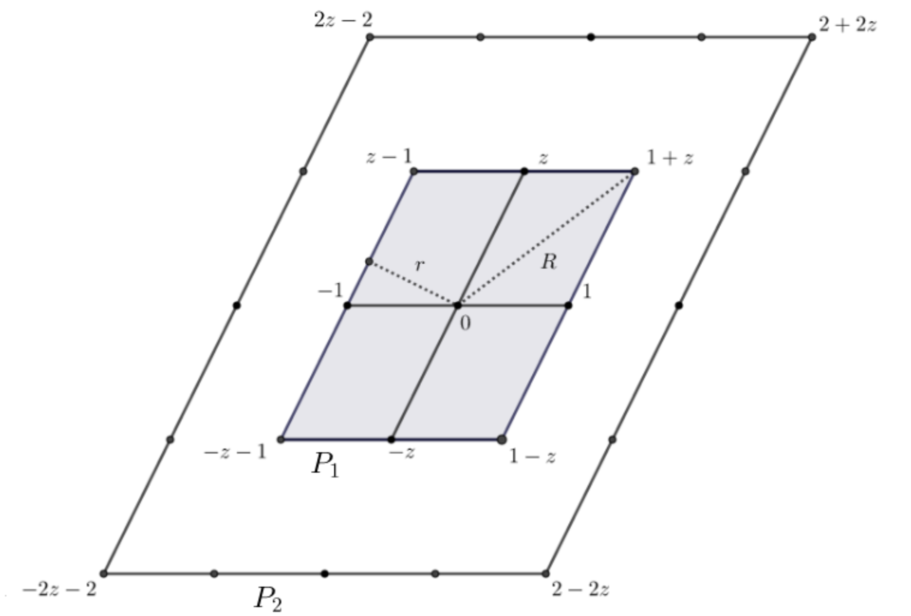

Figura 1.2: Paralelogramos P_1 y P_2

sobre el perímetro de P_k de esta forma son precisamente aquellos de la forma $\pm kz+j$ o $jz\pm k$ con j entero tal que $0 \leq |j| \leq k$, por lo tanto en cada uno de los casos anteriores hay $2k+1$ opciones para j y por lo tanto, al contar todos estos puntos hay $2(2k+1)+2(2k+1) = 4(2k+1)$ puntos de la forma $w = mz+n$ sobre el perímetro de P_k y ninguno de ellos se ha contado más de una vez excepto las esquinas $\pm kz \pm k$, que se contaron dos veces, por lo que hay exactamente $4(2k) = 8k$ puntos distintos de la forma $w = mz + n$ sobre el perímetro de P_k. Sean r y R la menor y la mayor distancia desde el 0 a un punto del perímetro de P_1, respectivamente. Dado que claramente, por la construcción de P_k se tiene que P_k y P_1 son homotéticos en razón k, se tiene que la menor y la mayor distancia de 0 a un punto en el perímetro de P_k son kr y kR, respectivamente. Se tiene entonces que para cada uno de los $8k$ puntos de la forma $w = mz + n$ sobre el perímetro de P_k se cumple

$$\frac{1}{(kR)^\alpha} \leq \frac{1}{|w|^\alpha} \leq \frac{1}{(kr)^\alpha} \tag{1.10}$$

Con lo anterior veremos que la serie

$$G_{\alpha/2}(z) = \sum_{\substack{n,m\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(mz+n)^\alpha}$$

converge absolutamente (y por lo tanto converge) si $\alpha > 2$. Dado que una serie se dice absolutamente convergente si la serie formada por sus módulos converge, entonces $G_{\alpha/2}(z)$ converge absolutamente si y solo si la serie

$$G'_{\alpha/2}(z) = \sum_{\substack{n,m\in\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{|mz+n|^{\alpha}}$$

converge. Como los términos de la serie $G'_{\alpha/2}$ son números reales positivos, entonces la serie $G'_{\alpha/2}$ converge al número real l si y solo si la serie formada por cualquier permutación de sus términos converge a l. Así para ver que la serie $G'_{\alpha/2}$ converge (es decir que la serie $G_{\alpha/2}$ converge absolutamente), nos bastaría ver que si

$$S(k) = \sum_{w\in P_k} \frac{1}{|w|^{\alpha}}$$

entonces

$$\lim_{k\to\infty} S(k) = \lim_{k\to\infty} \sum_{w\in P_k} \frac{1}{|w|^{\alpha}}$$

existe.
Retomando la ecuación (1.10), usando nuestra definición de $S(k)$ y dado que hemos demostrado que P_k tiene exactamente $8k$ puntos w de la forma $w = mz+n$ sobre su perímetro y claramente $P_i \subset P_k$ para todo $1 \leq i \leq k$ y cada punto en P_k pertenece al perímetro de exactamente un P_i, tenemos:

$$\frac{8}{R^{\alpha}} + \cdots + \frac{8k}{(kR)^{\alpha}} \leq S(k) \leq \frac{8}{r^{\alpha}} + \cdots + \frac{8k}{(kr)^{\alpha}} \tag{1.11}$$

o más concretamente

$$\frac{8}{R^{\alpha}} \sum_{i=1}^{k} \frac{1}{(k)^{\alpha-1}} \leq S(k) \leq \frac{8}{r^{\alpha}} \sum_{i=1}^{k} \frac{1}{(k)^{\alpha-1}} \tag{1.12}$$

Esto muestra que las sumas parciales $S(k)$ están acotadas por arriba por $8\zeta(\alpha-1)/r^{\alpha}$ si $\alpha > 2$ lo cual, ya que $S(k)$ es no decreciente, implica que el limite de cuando k tiende a infinito de $S(k)$ existe, es decir

$$G_{\alpha/2}(z) = \sum_{\substack{m,n\in\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{|mz+n|^{\alpha}}$$

converge. Además la cota inferior de $S(k)$ demuestra que si $\alpha \leq 2$ entonces $S(k)$ diverge ■

Hemos visto que $G_k(z)$ define una función en H. Nuestra intención ahora es probar que la serie de Eisenstein, $G_k(z)$, es una forma modular de peso $2k$. Según la definición 1.2.1 y la definición 1.2.3, bastará verificar que $G_k(z)$ satisface la ecuación (1.3) y que $G_k(z)$ es holomorfa en H y en infinito. El lema siguiente prueba que $G_k(z)$ satisface la ecuación (1.3).

Lema 1.2.2. *Sea k un entero mayor que 1, entonces*

$$G_k(z) = (cz+d)^{-2k} G_k\left(\frac{az+b}{cz+d}\right)$$

para toda $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$.

Demostración. Tenemos que

$$\begin{aligned} G_k\left(\frac{az+b}{cz+d}\right) &= \sum_{n,m} \frac{1}{(m\frac{az+b}{cz+d}+n)^{2k}} \\ &= \sum_{n,m} \frac{1}{(\frac{amz+bm}{cz+d}+n)^{2k}} = \sum_{n,m} \frac{1}{(\frac{amz+bm+cnz+dn}{cz+d})^{2k}} \\ &= (cz+d)^{2k} \sum_{n,m} \frac{1}{((am+cn)z+(bm+dn))^{2k}} \end{aligned} \tag{1.13}$$

pero $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$ tiene entradas enteras y determinante 1 por lo que representa una transformación biyectiva de $\mathbb{Z}^2$ en si mismo que envía el par (m, n) al par $(am + cn, bm + dn)$ por lo tanto la última suma en (1.13) es igual a

$$(cz+d)^{2k} \sum_{n,m} \frac{1}{(mz+n)^{2k}} = (cz+d)^{2k} G_k(z) \tag{1.14}$$

de donde concluimos que (1.15)

$$G_k(z) = (cz+d)^{-2k} G_k\left(\frac{az+b}{cz+d}\right) \text{ para toda } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \tag{1.16}$$

■

Con la ayuda de los lemas 1.2.1 y 1.2.2, podemos probar que la serie de Eisenstein, $G_k(z)$, es una forma modular de peso $2k$. Veamos esto en el siguiente teorema.

Teorema 1.2.3. *Sea k un entero mayor a 1. La serie de Eisenstein $G_k(z)$ es una forma modular de peso $2k$. Además se tiene que $G_k(\infty) = 2\zeta(2k)$ donde ζ denota la función zeta de Riemann.*

Demostración. Los lemas 1.2.1 y 1.2.2 implican que $G_k(z)$ es débilmente modular de peso $2k$ para todo entero k mayor que 1. Veamos que G_k es holomorfa en todas partes (incluyendo en infinito).

Vamos a demostrar que la serie

$$G_k(z) = \sum_{\substack{n,m\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(mz+n)^{2k}} \tag{1.17}$$

converge absolutamente y uniformemente en cada franja de la forma

$$S_{A,\delta} = \{z : |\Re(z)| \leq A,\, \Im(z) \geq \delta > 0\}$$

donde A y δ son cualesquiera reales positivos. Para ver esto encontraremos una constante $M > 0$ que depende solamente de A y δ y es tal que

$$\frac{1}{|mz+n|^{2k}} \leq \frac{M}{|mi+n|^{2k}} \tag{1.18}$$

para todo $z \in S_{A,\delta}$ y todo $(m,n) \neq (0,0)$. Dado lo anterior, ya que por el lema (1.2.1) la serie

$$G_k(i) = \sum_{\substack{n,m\in\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{|mi+n|^{2k}}$$

converge y M es una constante, podemos deducir por la prueba M de Weierstrass[2] que la serie

$$G_k(z) = \sum_{\substack{n,m\in\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{(mz+n)^{2k}}$$

converge absolutamente y uniformemente en $S_{A,\delta}$ y dado que las funciones

$$g_{m,n,k}(z) = \frac{1}{(mz+n)^{2k}}$$

son holomorfas en $S_{A,\delta}$, entonces

$$G_k(z) = \sum_{\substack{n,m\in\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{(mz+n)^{2k}}$$

es holomorfa en $S_{A,\delta}$. Como para cada $z \in H$ existen A y δ tales que $z \in S_{A,\delta}$, esto prueba que G_k es holomorfa en H.
Veamos ahora la existencia de la constante M que satisface la ecuación (1.18). Para probar la existencia de dicha constante es suficiente probar que existe una constante $K > 0$ que depende solo de A y δ tal que

$$|mz+n|^2 > K|mi+n|^2 \tag{1.19}$$

Si escribimos $z = x + iy$, la ecuación (1.19) se convierte en

$$(mx+n)^2 + (my)^2 > K(m^2+n^2) \tag{1.20}$$

Si $m = 0$ la desigualdad anterior se satisface para toda $0 < K < 1$. Si $m \neq 0$ hacemos $r = n/m$. Dividiendo (1.20) entre m^2, observamos que probar (1.20) es equivalente a probar

[2] Véase por ejemplo [3] pág. 29.

$$\frac{(r+x)^2+y^2}{1+r^2} > K \tag{1.21}$$

para algún $K > 0$. Probaremos que la ecuación (1.21) se satisface para todo número real r si $|x| \leq A$ y $y > \delta$ y si

$$K = \frac{\delta^2}{1+(A+\delta)^2}$$

Si $|r| \leq A+\delta$ entonces

$$\frac{(r+x)^2+y^2}{1+r^2} \geq \frac{y^2}{1+r^2} > \frac{\delta^2}{1+(A+\delta)^2} = K$$

Si $|r| > A+\delta$ entonces $|x/r| < |x|/(A+\delta) \leq A/(A+\delta) < 1$ y entonces

$$\left|1+\frac{x}{r}\right| \geq 1 - \left|\frac{x}{r}\right| > 1 - \frac{A}{A+\delta} = \frac{\delta}{A+\delta}$$

por lo tanto

$$|r+x| \geq \frac{r\delta}{A+\delta}$$

que implica

$$(r+x)^2 \geq \frac{r^2\delta^2}{(A+\delta)^2}$$

de donde tenemos

$$\frac{(r+x)^2+y^2}{1+r^2} \geq \frac{\delta^2}{(A+\delta)^2} \cdot \frac{r^2}{1+r^2} \tag{1.22}$$

Ahora, dado que la función $r^2/(1+r^2)$ es una función creciente de r^2 y $r^2 > (A+\delta)^2$, entonces

$$\frac{r^2}{1+r^2} \geq \frac{(A+\delta)^2}{1+(A+\delta)^2} \tag{1.23}$$

Usando la ecuación (1.23) en la ecuación (1.22), tenemos

$$\frac{(r+x)^2+y^2}{1+r^2} \geq \frac{\delta^2}{(A+\delta)^2} \cdot \frac{(A+\delta)^2}{1+(A+\delta)^2} = \frac{\delta^2}{1+(A+\delta)^2} = K$$

lo que demuestra que G_k es holomorfa en H.

Resta probar que G_k tiene un limite cuando $\Im(z) \to \infty$, pero podemos suponer que z permanece en el dominio fundamental D, pues si $\Im(z) \geq 1$, siempre existe un n tal que $T^n(z) \in D$, donde T es la traslación y como G_k es débilmente modular, entonces $G_k(T^n(z)) = G_k(z)$. Ahora suponiendo que z permanece en D, dada la convergencia uniforme allí de $G_k(z)$, podemos pasar al limite término por término. Los términos con $m \neq 0$ tienden a 0; los otros tienen el limite $1/n^{2k}$, por lo que se tiene

$$\lim_{\Im(z)\to\infty} G_k(z) = \sum_{\substack{n\in\mathbb{Z}\\ n\neq 0}} \frac{1}{n^{2k}} = 2\sum_{n=1}^{\infty} \frac{1}{n^{2k}} = 2\zeta(2k)$$

■

Las series de Eisenstein de menor peso son G_2 y G_3, que son de pesos 4 y 6, respectivamente. Es conveniente (por la teoría de curvas elípticas) reemplazarlas por sus múltiplos:

$$g_2 = 60G_2, \quad g_3 = 140G_3 \tag{1.24}$$

Tenemos que $g_2(\infty) = 120\,\zeta(4)$ y $g_3(\infty) = 280\,\zeta(6)$. Usando los valores conocidos para $\zeta(4)$ y $\zeta(6)$[3], encontramos:

$$g_2(\infty) = \frac{4}{3}\,\pi^4, \quad g_3(\infty) = \frac{8}{27}\,\pi^6 \tag{1.25}$$

si hacemos

$$\Delta = g_2^3 - 27g_3^2 \tag{1.26}$$

tenemos entonces que $\Delta(\infty) = 0$, es decir, Δ es una forma cuspidal de peso 12. Nos referiremos frecuentemente a Δ como el discriminante modular, por razones que serán explicadas posteriormente.

1.3. El espacio de las formas modulares

Estudiaremos ahora propiedades sobre el espacio de las formas modulares.

Definición 1.3.1. *Sea f una función meromorfa en una región R, al entero n tal que $\dfrac{f(z)}{(z-p)^n}$ es holomorfa y no cero en p lo llamamos el orden de f en p y lo denotamos como $\upsilon_p(f)$.*

Si f es una función modular tenemos el siguiente lema.

Lema 1.3.1. *Sean f una función modular de peso $2k$ y $g \in G$ se tiene que $\upsilon_p(f) = \upsilon_{g(p)}(f)$*

Demostración. Sea $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ tenemos que $m = \upsilon_{g(p)}(f) = \upsilon_p(f\circ g)$ es tal que $\dfrac{f(g(z))}{(z-p)^m} = (cz+d)^{2k}\cdot\dfrac{f(z)}{(z-p)^m}$ es holomorfa y no cero en p. Como $cp + d \neq 0$ en H, debemos tener que $\dfrac{f(z)}{(z-p)^m}$ es holomorfa y no cero en p pero, esta es la definición de el orden de f en p y por lo tanto $\upsilon_p(f) = \upsilon_{g(p)}(f)$ ■

[3]Ver por ejemplo el corolario 1.4.1.1.

El lema anterior nos dice que si f es una función modular, entonces el orden de f en p es un concepto que se puede estudiar en H modulo G, es decir para estudiarlo podemos restringir nuestro trabajo nuevamente al dominio fundamental D.
Por otro lado si f es una función modular, entonces su función asociada, $\tilde{f}$, es meromorfa en el interior del disco unitario y por lo tanto $\upsilon_0(\tilde{f})$ está bien definido y podemos definir $\upsilon_\infty(f) = \upsilon_0(\tilde{f})$.

Antes de probar el teorema que nos permitirá estudiar el espacio de las formas modulares probaremos el siguiente lema.

Lema 1.3.2. *Sea f un función modular de peso $2k$, no idénticamente cero, entonces f tiene solamente un número finito de ceros y polos modulo G.*

Demostración. Como f no es idénticamente cero, entonces $\tilde{f}$ tampoco lo es. Por otro lado, dado que $\tilde{f}$ es meromorfa en 0, existe $R_1 > 0$ tal que $\tilde{f}$ es holomorfa en la región $0 < |q| < R_1$. Además, el Teorema de la identidad[4] y las hipótesis en $\tilde{f}$ garantizan que el origen no puede ser un punto de acumulación de ceros de $\tilde{f}$. Por lo tanto, existe R_2, con $0 < R_2 < R_1 < 1$ tal que $\tilde{f}$ es holomorfa y distinta de cero en la región $0 < |q| < R_2$. Recordando que $f(z) = \tilde{f}(q)$ con $q = e^{2\pi i z}$, tenemos que $e^{-2\pi\Im(z)} = |e^{2\pi i z}| = |q| < R_2$ si y solo si $-2\pi\Im(z) < \log(R_2)$ si y solo si $\Im(z) > \dfrac{\log(R_2^{-1})}{2\pi} = R' > 0$, es decir existe $R' > 0$ tal que si $\Im(z) > R'$, entonces f es holomorfa y no cero en z. Consideremos ahora el conjunto $D_{R'} = \{z | z \in D, \Im(z) \leq R'\}$, como $D_{R'}$ es compacto, y f es holomorfa y no idénticamente cero en $D_{R'}$, entonces, nuevamente por el Teorema de la identidad y por la compacidad, f tiene solo un número finito de ceros y polos en $D_{R'}$ y como f no tiene ceros ni polos fuera de $D_{R'}$ concluimos que f tiene solo un número finito de ceros y polos modulo G. ■

Veamos ahora el siguiente teorema que será la clave para obtener las dimensiones de los espacios de las formas modulares de peso $2k$.

Teorema 1.3.3. *Sea f un función modular de peso $2k$, no idénticamente cero, se tiene*

$$\upsilon_\infty(f) + \sum_{p \in H/G} \frac{1}{e_p} \upsilon_p(f) = \frac{k}{6} \tag{1.27}$$

donde e_p denota el orden del estabilizador del punto p bajo la acción de G, que, como vimos anteriormente, se tiene que $e_i = 2$, $e_\rho = 3$ y $e_p = 1$ en cualquier otro caso, por lo que la identidad anterior se puede escribir también de la siguiente forma:

$$\upsilon_\infty(f) + \frac{1}{2}\upsilon_i(f) + \frac{1}{3}\upsilon_\rho(f) + \sum_{p \in H/G}^{*} \upsilon_p(f) = \frac{k}{6} \tag{1.28}$$

[4]Véase por ejemplo [11] pág 227.

donde el símbolo $\sum^*$ *significa que la suma se toma sobre los puntos de* H/G *distintos de las clases de* i *y* ρ.

Demostración. Para probar el teorema integraremos $\frac{1}{2i\pi}\frac{df}{f}$ en un contorno que es una modificación de la frontera del compacto $D_{R'} = \{z|z \in D, \Im(z) \leq R'\}$ que definimos en la prueba del lema 1.3.2, como se ve en la figura 1.3. Recordemos que $D_{R'}$ contiene todos los ceros y polos de f que están en D y que dichos ceros y polos son una cantidad finita por el lema 1.3.2. Dado que D es un dominio fundamental para la acción de G en H, entonces $D_{R'}$ contiene representantes de todos los ceros y polos de f en H/G. Aplicaremos el principio del argumento de Cauchy[5] en esta modificación de la frontera de $D_{R'}$. Más precisamente, modificaremos la frontera de $D_{R'}$ para rodear los vértices ρ, i y $-\bar{\rho}$ con arcos de radios pequeños (y haremos esos radios tender a cero), además primero supondremos que f no tiene ceros ni polos en dicho contorno de integración, el cual llamaremos simplemente R.

Se tiene entonces por el principio del argumento la identidad:

$$\frac{1}{2i\pi}\int_R \frac{df}{f} = \sum_{p\in H/G}^{*} \upsilon_p(f) \tag{1.29}$$

Por otro lado, podemos calcular la integral en el contorno por partes siguiendo la figura 1.3.

a) Tenemos que el cambio de variable $q = e^{2\pi i z}$ transforma el arco EA en una circunferencia γ centrada en $q = 0$ con orientación negativa, pues en el arco EA la parte imaginaria de z permanece constante y la parte real varía de $1/2$ a $-1/2$. Dicha circunferencia, por la elección de EA no encierra ceros ni polos de $\tilde{f}$ excepto posiblemente en $q = 0$. Además tenemos que $f(z) = \tilde{f}(q)$ de donde se tiene que $f'(z) = \tilde{f}'(q)\,\frac{dq}{dz}$ y por lo tanto $\frac{f'(z)}{f(z)}\,dz = \frac{\tilde{f}'(q)}{\tilde{f}(q)}\,dq$, de donde podemos concluir que:

$$\frac{1}{2i\pi}\int_E^A \frac{f'(z)}{f(z)}\,dz = \frac{1}{2i\pi}\int_\gamma \frac{\tilde{f}'(q)}{\tilde{f}(q)}\,dq = -\upsilon_\infty(f) \tag{1.30}$$

b) Dado que la traslación T transforma el arco AB en $D'E$ recorridos en sentidos opuestos y $f(z) = f(Tz)$, se sigue que:

$$\frac{1}{2i\pi}\int_A^B \frac{df}{f} + \frac{1}{2i\pi}\int_{D'}^E \frac{df}{f} = 0 \tag{1.31}$$

Ahora usaremos el siguiente lema para calcular las integrales en los arcos BB', CC' y DD'.

[5] Véase por ejemplo [1] pág. 152 o [3] pág. 123

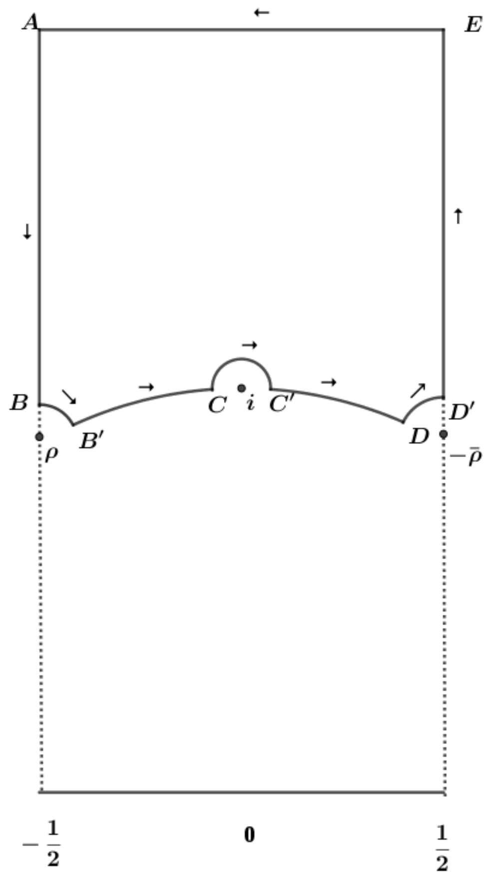

Figura 1.3: Contorno de integración R

Lema 1.3.4. *Sea γ un arco de la circunferencia centrada en p y de radio r tal que el ángulo central que subtiende a γ es α' y sea f una función meromorfa y no idénticamente cero en $D(p,r)$, el disco cerrado centrado en p de radio r. Si $\lim_{r\to 0} \alpha' = \alpha$ se tiene:*

$$\lim_{r\to 0} \frac{1}{2i\pi} \int_\gamma \frac{f'(z)}{f(z)}\, dz = \frac{\alpha}{2\pi} \upsilon_p(f) \tag{1.32}$$

donde γ es recorrida en sentido negativo.

Demostración. Como f es meromorfa y no idénticamente cero en $D(p,r)$, podemos suponer sin perdida de generalidad que f no tiene otro cero ni un polo en $D(p,r)$, pues ya que estamos tomando el limite cuando r tiende a *cero* de cualquier manera existirá un r' menor o igual a r con dicha propiedad. Como f es meromorfa en p se tiene que existe una función holomorfa g tal que cerca de p se cumple que $f(z) = (z-p)^{-\upsilon_p(f)}g(z)$, nuevamente, sin perdida de generalidad, podemos suponer que se tiene esta identidad en $D(p, r)$. Se cumple entonces que $f'(z) = -\upsilon_p(f)(z-p)^{-\upsilon_p(f)-1}g(z) + (z-p)^{-\upsilon_p(f)}g'(z)$ y por lo tanto:

$$\frac{f'(z)}{f(z)} = \frac{-\upsilon_p(f)(z-p)^{-\upsilon_p(f)-1}g(z)}{(z-p)^{-\upsilon_p(f)}g(z)} + \frac{(z-p)^{-\upsilon_p(f)}g'(z)}{(z-p)^{-\upsilon_p(f)}g(z)} = \frac{-\upsilon_p(f)}{z-p} + \frac{g'(z)}{g(z)} \tag{1.33}$$

Hacemos $z - p = re^{i\theta}$, entonces podemos parametrizar el arco γ como $re^{i\theta}$ para $0 \leq \beta_2 \leq \theta \leq \beta_1 \leq 2\pi$. Usando (1.33) e integrando ambos lados tenemos:

$$\begin{aligned}
\frac{1}{2\pi i}\int_\gamma \frac{f'(z)}{f(z)}\,dz &= \frac{1}{2\pi i}\int_\gamma \frac{-\upsilon_p(f)}{z-p} + \frac{g'(z)}{g(z)}\,dz \\
&= \frac{1}{2\pi i}\int_{\beta_1}^{\beta_2} \left(\frac{-\upsilon_p(f)}{re^{i\theta}} + \frac{g'(p+re^{i\theta})}{g(p+re^{i\theta})}\right) re^{i\theta} i\,d\theta \\
&= \frac{1}{2\pi}\int_{\beta_1}^{\beta_2} -\upsilon_p(f)\,d\theta + \frac{r}{2\pi}\int_{\beta_1}^{\beta_2}\left(\frac{g'(p+re^{i\theta})}{g(p+re^{i\theta})}\right)e^{i\theta}\,d\theta \\
&= \frac{-(\beta_2-\beta_1)\upsilon_p(f)}{2\pi} + \frac{r}{2\pi}\int_{\beta_1}^{\beta_2}\left(\frac{g'(p+re^{i\theta})}{g(p+re^{i\theta})}\right)e^{i\theta}\,d\theta \qquad (1.34)
\end{aligned}$$

Recordemos que estamos integrando recorriendo a γ en sentido negativo y por lo tanto $\dfrac{-(\beta_2-\beta_1)}{2\pi}$ es igual al ángulo positivo que subtiende el arco γ en la circunferencia centrada en p de radio r. Por otro lado como g es tal que $g(z)$ es holomorfa y no cero cerca de p (lo cual incluye que es holomorfa y no cero en p), se tiene que $\dfrac{g'(z)}{g(z)}$ es holomorfa cerca de p pues es el cociente de dos funciones holomorfas (en esta región) y $g(z)$ nunca es cero aquí por lo que el cociente no tiene polos. Como γ es compacto y $\dfrac{g'(z)}{g(z)}$ es holomorfa en una región que contiene a γ entonces, $\dfrac{g'(z)}{g(z)}$ es acotada en γ y por lo tanto:

$$
\begin{aligned}
0 &\leq \lim_{r\to 0} \frac{r}{2\pi}\left|\int_{\beta_1}^{\beta_2}\left(\frac{g'(p+re^{i\theta})}{g(p+re^{i\theta})}\right)e^{i\theta}\,d\theta\right| \\
&\leq \lim_{r\to 0} \frac{r}{2\pi}\int_{\beta_1}^{\beta_2}\left|\left(\frac{g'(p+re^{i\theta})}{g(p+re^{i\theta})}\right)e^{i\theta}\right|d\theta \\
&\leq \lim_{r\to 0} \frac{r}{2\pi}\int_{\beta_1}^{\beta_2} C\,d\theta = \lim_{r\to 0} \frac{r}{2\pi}(\beta_2-\beta_1)C = 0
\end{aligned}
$$

retomando (1.34) y tomando el limite cuando r tiende a cero tenemos:

$$
\begin{aligned}
\lim_{r\to 0}\frac{1}{2\pi i}\int_\gamma \frac{f'(z)}{f(z)}\,dz &= \lim_{r\to 0}\frac{-(\beta_2-\beta_1)\upsilon_p(f)}{2\pi} + \frac{r}{2\pi}\int_{\beta_1}^{\beta_2}\left(\frac{g'(p+re^{i\theta})}{g(p+re^{i\theta})}\right)e^{i\theta}\,d\theta \\
&= \alpha\,\upsilon_p(f) + 0 = \alpha\,\upsilon_p(f) \qquad (1.35)
\end{aligned}
$$

■

c) Por el lema (1.3.4) tenemos que cuando hacemos los radios de los arcos BB', CC' y DD' tender a cero obtenemos:

$$\frac{1}{2\pi i}\int_B^{B'}\frac{df}{f} \to -\frac{1}{6}\upsilon_\rho(f) \qquad (1.36)$$

$$\frac{1}{2\pi i}\int_C^{C'}\frac{df}{f} \to -\frac{1}{2}\upsilon_i(f) \qquad (1.37)$$

$$\frac{1}{2\pi i}\int_D^{D'}\frac{df}{f} \to -\frac{1}{6}\upsilon_\rho(f) \quad (\upsilon_{-\bar{\rho}}(f) = \upsilon_\rho(f)) \qquad (1.38)$$

d) El elemento S de G transforma el arco $B'C$ en el arco DC'; dado que $f(Sz) = z^{2k}f(z)$, tenemos:

$$\frac{df(Sz)}{f(Sz)} = 2k\frac{dz}{z} + \frac{df(z)}{f(z)} \qquad (1.39)$$

y por lo tanto:

$$\begin{aligned}\frac{1}{2i\pi}\int_{B'}^{C}\frac{df}{f}+\frac{1}{2i\pi}\int_{C'}^{D}\frac{df}{f} &= \frac{1}{2i\pi}\int_{B'}^{C}\left(\frac{df(z)}{f(z)}-\frac{df(Sz)}{f(Sz)}\right)\\ &= \frac{1}{2i\pi}\int_{B'}^{C}-2k\frac{dz}{z}\\ &\to -2k(-\frac{1}{12})=\frac{k}{6} \qquad (1.40)\end{aligned}$$

Cuando el radio de los arcos BB', CC' y DD' tiende a cero.

Hemos entonces calculado la integral en (1.29) de una segunda forma dividiendo el contorno R y hemos obtenido que dicha integral es la suma de las integrales calculadas en las ecuaciones (1.30), (1.31), (1.36), (1.37), (1.38) y (1.40), por lo que tenemos la siguiente identidad:

$$\sum_{p\in H/G}^{*}\upsilon_p(f)=\frac{1}{2i\pi}\int_R\frac{df}{f}=\frac{k}{6}-\frac{1}{6}\upsilon_\rho(f)-\frac{1}{2}\upsilon_i(f)-\frac{1}{6}\upsilon_\rho(f)-\upsilon_\infty(f)$$

de donde se sigue

$$\upsilon_\infty(f)+\frac{1}{2}\upsilon_i(f)+\frac{1}{3}\upsilon_\rho(f)+\sum_{p\in H/G}^{*}\upsilon_p(f)=\frac{k}{6}.$$

Hemos probado nuestro resultado bajo el supuesto de que f no tiene ceros ni polos en la frontera de $D_{R'}$ excepto tal vez en ρ o i, sin embargo dado que el numero de ceros y polos de f son finitos podemos resolver el caso general haciendo ligeras (finitas) modificaciones al contorno R de la siguiente forma:

1. Si f tiene un cero o un polo en un punto λ sobre AB rodeamos a λ por una semicircunferencia de radio suficientemente pequeño y rodeamos también a $T\lambda$ en $D'E$ por una semicircunferencia de igual radio y de tal manera que exactamente un de las dos semicircunferencias está dentro de $D_{R'}$. De esta forma, exactamente un representante de λ (que es un cero o un polo) queda dentro de la región delimitada por el contorno sobre el que vamos a integrar y además T sigue transformando AD en $D'E$ por lo que las integrales sobre estas curvas se calculan de manera análoga (se siguen anulando una a la otra). Hacemos esto por cada cero o polo que haya en AB (que son finitos).

2. Si f tiene un cero o un polo en un punto w sobre el arco $B'C$, rodeamos w con un arco de circunferencia de radio suficientemente pequeño contenido en $D_{R'}$ y aplicamos S a la nueva trayectoria de B' a C, esta transformación nos da una nueva trayectoria de C' a D que no pasa por Sw y más aun,

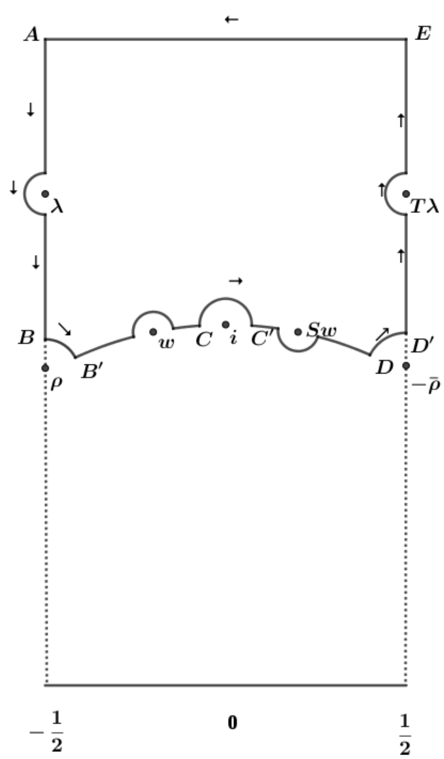

Figura 1.4: Contorno R con modificaciones

como $Sz = -\dfrac{1}{z}$, el arco pequeño alrededor de w es transformado en un arco pequeño alrededor de Sw que está contenido en el disco unitario y por lo tanto tenemos que hay exactamente un representante de w contenido en la nueva región acotada por el contorno en el que integraremos. Podemos hacer esto por cada cero y polo de f que esté sobre el arco $B'C$ (que son finitos).

Con esas modificaciones obtenemos un contorno como el de la figura 1.4.

Como la manera en la que obtuvimos las integrales de $\dfrac{f'(z)}{f(z)}$ a lo largo de $B'C$ y $C'D$ dependían de que $B'C$ era transformado en $C'D$ por S y esto sigue siendo cierto, el resultado obtenido será el mismo y se obtiene de manera análoga pues al hacer tender los radios de las circunferencias que rodean a los ceros, polos, ρ, i y $-\bar{\rho}$ a cero, la trayectoria $B'C$ tiende nuevamente a ser el arco ρi.

$\blacksquare$

Si k es un entero, denotamos por M_k y M_k^0 los $\mathbb{C}$-espacios vectoriales de las formas modulares de peso $2k$ y las formas cuspidales de peso $2k$, respectivamente. Por definición, M_k^0 es el kernel de la forma lineal $f \to f(\infty)$ sobre M_k. Por lo anterior tenemos que $M_k/M_k^0 \leq 1$ ya que M_k/M_k^0 es isomorfo a la imagen de $f \to f(\infty)$ sobre M_k, que como $\mathbb{C}$-espacio vectorial tiene dimensión menor o igual a 1. Más aun, para $k \geq 2$, la serie de Eisenstein G_k es un elemento de M_k tal que $G_k(\infty) \neq 0$ y por lo tanto tenemos

$$M_k = M_k^0 \oplus \mathbb{C} \cdot G_k.$$

Finalmente recordamos que se denota por Δ el elemento $g_2^3 - 27g_3^2$ de M_6^0 donde $g_2 = 60G_2$ y $g_3 = 140G_3$.

Teorema 1.3.5. *(i) Se tiene que $M_k = 0$ para $k < 0$ y $k = 1$.*
(ii) Para $k = 0, 2, 3, 4, 5$, M_k es un espacio vectorial de dimensión 1 con bases $1, G_2, G_3, G_4, G_5$ y se tiene $M_k^0 = 0$.
(iii) Multiplicar por Δ define un isomorfismo de M_{k-6} en M_k^0.

Demostración. Sea f un elemento no cero de M_k, todos los términos del lado izquierdo de la formula

$$\upsilon_\infty(f) + \frac{1}{2}\upsilon_i(f) + \frac{1}{3}\upsilon_\rho(f) + \sum_{p \in H/G}^{*} \upsilon_p(f) = \frac{k}{6} \tag{1.41}$$

son mayores o iguales a cero, por lo que debemos tener que $k \geq 0$ y también $k \neq 1$, ya que $\frac{1}{6}$ no puede ser escrito en la forma $n + n'/2 + n''/3$ con $n, n', n'' \geq 0$. Lo anterior demuestra (i).
Para $k = 0$ claramente M_0 es un espacio vectorial de dimensión 1 con base 1. Por otro lado, por la formula (1.41) se tiene que para $k = 2, 3, 4, 5$ debe suceder que $\upsilon_p(f) = 0$, excepto para $p = i$ o $p = \rho$, pues el lado derecho de (1.41) es menor a 1, en particular $\upsilon_\infty(f) \neq 0$ para todo $f \in M_k$ con $2 \leq k \leq 5$, lo cual implica que $M_k^0 = 0$ para $k = 2, 3, 4, 5$, es decir, M_k^0 tiene dimensión 0 para $k = 2, 3, 4, 5$. Además como M_k/M_k^0 tiene dimensión menor o igual a 1 y G_2, G_3, G_4 y G_5 son elementos no idénticamente cero (pues $G_k(\infty) = 2\zeta(2k)$) de M_2, M_3, M_4 y M_5, respectivamente, se sigue que M_k tiene dimensión 1 para $k = 2, 3, 4, 5$ con bases G_2, G_3, G_4, G_5 por lo tanto hemos probado (ii).
Ahora aplicamos (1.41) a $f = G_2$. Queremos escribir $\frac{2}{6}$ en la forma $n + n'/2 + n''/3$ con $n, n', n'' \geq 0$ lo que implica que $n = 0$ y $\frac{3n'+2n''}{6} = \frac{2}{6}$, de donde se debe tener que $n' = 0$ y $n'' = 1$. Esto muestra que $\upsilon_\rho(G_2) = 1$ y que $\upsilon_p(G_2) = 0$ para todo $p \neq \rho$ (modulo G). Aplicando 1.41 a G_3 queremos escribir $\frac{3}{6}$ en la forma $n + n'/2 + n''/3$ con $n, n', n'' \geq 0$ lo que implica que $n = 0$ y $\frac{3n'+2n''}{6} = \frac{3}{6}$, de donde se debe tener $n' = 1$ y $n'' = 0$. Esto muestra que $\upsilon_i(G_3) = 1$ y que $\upsilon_p(G_3) = 0$ para todo $p \neq i$ (modulo G). Con lo anterior, y recordando que $\Delta = g_2^3 - 27g_3^2$ donde $g_2 = 60G_2$ y $g_3 = 140G_3$, tenemos que Δ no es cero en i, pues G_3 tiene un cero en i pero G_2 no, de donde se sigue que Δ no es

idénticamente cero.
Dado que el peso de Δ es 12 y $\upsilon_\infty(\Delta) \geq 1$, la formula (1.41) implica que $\upsilon_p(\Delta) = 0$ para $p \neq \infty$ y $\upsilon_\infty(\Delta) = 1$. En otras palabras, Δ no se hace cero en H y tiene un cero simple en infinito. Si f es un elemento de M_k^0 y si hacemos $g = f/\Delta$, es claro que g es de peso $2k - 12$. Más aun, la formula

$$\upsilon_p(g) = \upsilon_p(f) - \upsilon_p(\Delta)$$

nos dice que $\upsilon_p(g) = \upsilon_p(f)$ si $p \neq \infty$ y $\upsilon_p(g) = \upsilon_p(f) - 1$ si $p = \infty$, lo que prueba que $\upsilon_p(g) \geq 0$ para todo p, por lo que g pertenece a M_{k-6}, lo cual demuestra (iii). ∎

Corolario 1.3.5.1. *Se tiene que:*

$$\dim M_k = \begin{cases} \lfloor k/6 \rfloor & si \quad k \equiv 1 \pmod 6,\ k \geq 0 \\ \lfloor k/6 \rfloor + 1 & si \quad k \not\equiv 1 \pmod 6,\ k \geq 0 \end{cases} \tag{1.42}$$

Demostración. La formula (1.42) es valida para $0 \leq k < 6$ por las partes (i) y (ii) del teorema (1.3.5). Además las dos expresiones se aumentan en 1 cuando reemplazamos k por $k+6$ por la parte (iii) del mismo teorema. Por lo tanto la formula es valida para todo $k \geq 0$ ∎

Corolario 1.3.5.2. *El espacio M_k tiene como base la familia de monomios $G_2^\alpha G_3^\beta$ con α y β enteros no negativos tales que $2\alpha + 3\beta = k$.*

Demostración. Omitimos los k tales que M_k tiene dimensión 0, es decir cuando $k < 0$, $k = 1$. Primero mostraremos que esos monomios generan M_k. Esto es claro para $k \leq 3$ por el inciso (ii) del teorema (1.3.5). Para $k \geq 4$ argumentaremos por inducción en k. Elegimos un par (γ, δ) de enteros mayores o iguales a 0 tales que $2\delta + 3\gamma = k$ (esto es posible para todo $k \geq 2$). La forma modular $g = G_2^\gamma G_2^\delta$ es no cero en infinito. Si f pertenece a M_k, entonces existe $\lambda \in \mathbb{C}$ tal que $f - \lambda g$ es una forma cuspidal, que, por (iii) es igual a Δh con $h \in M_{k-6}$. Aplicando la hipótesis de inducción a h tenemos el resultado.
Ahora que sabemos que los monomios $G_2^\alpha G_3^\beta$ con α, $\beta \geq 0$ tales que $2\alpha + 3\beta = k$ generan M_k, bastará ver que estos monomios son linealmente independientes. Para probar lo anterior bastará ver que la cantidad de monomios de este tipo es igual a la dimensión de M_k, pues si probamos esto y los monomios fueran linealmente dependientes, entonces M_k tendría un conjunto de generadores con cardinal menor a la dimensión, lo cual sería una contradicción. Veamos entonces que lo que queremos contar es la cantidad de parejas:

$$n = |\{(i,j) \,|\, i,j \geq 0 \quad \text{y} \quad 2i + 3j = k\}|$$

Primero notamos que el resultado es claro para $0 \leq k \leq 5$ por las partes (i) y (ii) del teorema (1.3.5) ya que en esos caso M_k es de dimensión 1 si $k \neq 1$ y a 0 si $k = 1$ y las únicas parejas $(i, \jmath)$ con i, $j \geq 0$ tales que $2i + 3j = k$

para $k = 0, 2, 3, 4, 5$ son $(0, 0)$, $(1, 0)$, $(0, 1)$, $(2, 0)$, $(1, 1)$, respectivamente, y para $k = 1$ hay 0 soluciones. Sea l el residuo de k al dividirlo entre 6 tenemos:

$$\left\lfloor \frac{k}{6} \right\rfloor = \frac{k-l}{6} = m$$

por otro lado $k = 6m + l$, por lo que estamos buscando la cantidad de parejas $i, j \geq 0$ que cumplen $2i = 6m + l - 3j$. Observamos que $l \equiv j \pmod 2$ y que como $2i \geq 0$, entonces $2i = 6m + l - 3j \geq 0$, de donde se sigue que $0 \leq j \leq 2m + \frac{l}{3}$. Además cada j que cumple $l \equiv j \pmod 2$ y $0 \leq j \leq 2m + \frac{l}{3}$ determina exactamente una pareja (i, j) que es solución a $2i = 6m + l - 3j$. Basta entonces contar las j tales que $l \equiv j \pmod 2$ y $0 \leq j \leq 2m + \frac{l}{3}$. Tenemos los siguientes casos:

$$n = |\{j \mid l \equiv j \pmod 2 \quad \text{y} \quad 0 \leq j \leq 2m{+}l/3\}| = \begin{cases} m+1 & \text{si } l = 0 \\ m & \text{si } l = 1 \\ m+1 & \text{si } l = 2 \\ m+1 & \text{si } l = 3 \\ m+1 & \text{si } l = 4 \\ m+1 & \text{si } l = 5 \end{cases} \tag{1.43}$$

y como $\left\lfloor \frac{k}{6} \right\rfloor = m$, se sigue del corolario (1.42) que la cantidad de monomios $G_2^{\alpha} G_3^{\beta}$ con α, $\beta \geq 0$ tales que $2\alpha + 3\beta = k$ es igual a la dimensión de M_k y como estos generan M_k concluimos que dichos monomios forman una base para M_k. ■

1.3.1. El *Invariante modular*

Hacemos

$$j = 1728\, g_2^3/\Delta = 12^3 g_2^3/\Delta$$

Llamaremos a j el invariante modular. Dicho nombre se justifica pues, como veremos a continuación j es una función modular de peso 0 y por lo tanto es invariante bajo el grupo modular.

Proposición 1.3.1. *(a) La función j es una función modular de peso* 0.
(b) j es holomorfa en H y tiene un polo simple en ∞
(c) j define una biyección entre el cociente H/G y $\mathbb{C}$

Demostración. La afirmación (a) se sigue del hecho de que g_2^3 y Δ son funciones modulares de peso 12; (b) se sigue del hecho de que $\Delta \neq 0$ en H y tiene un cero simple en infinito, mientras que g_2 no es cero en infinito. Para probar (c) veamos que si $\lambda \in \mathbb{C}$, entonces la forma modular $f_\lambda = 1728 g_2^3 - \lambda\Delta$ tiene un único cero modulo G. Para ver lo anterior notamos que claramente f_λ es una forma modular de peso 12 pues es combinación lineal de dos formas modulares de peso 12, entonces f_λ no tiene polos en H y, si aplicamos la formula (1.28) con

$f = f_\lambda$ y $k = 6$ se debe obtener una identidad de la forma $n + n'/2 + n''/3 = 1$ donde n, n', n'' son enteros no negativos pero, las únicas soluciones a esto son $(1, 0, 0)$, $(0, 2, 0)$, $(0, 0, 3)$, por lo tanto $f_\lambda(z) = 0$ para un único $z \in H$, y por lo tanto

$$f_\lambda = 1728\, g_2^3/\Delta - \lambda$$

es igual a cero para exactamente un $z_\lambda \in H$, por lo que asociando z_λ con $\lambda \in \mathbb{C}$, tenemos que j define una biyección entre H/G y $\mathbb{C}$. ■

Hemos caracterizado los espacios de las formas modulares de peso $2k$ para todo entero k he incluso hemos dado una base para dichos espacios, sin embargo poco hemos podido decir de las funciones modulares en general. En este sentido j, el invariante modular, nos da una caracterización de las funciones modulares de peso 0. Más precisamente, tenemos la siguiente proposición:

Proposición 1.3.2. *Sea f una función meromorfa en H. f es una función modular de peso 0 si y solo si f es una función racional de j.*

Demostración. Es claro que si f es una función racional de j entonces, como tanto numerador y denominador son polinomios de j y cada uno de ellos es una función modular de peso 0, entonces j es una función modular de peso 0.
Ahora supongamos que f es una función modular de peso 0, sabemos por (1.3.2) que f tiene un número finito de ceros y polos en la región fundamental D. Si $z_1, ...z_n$ y $p_1, ..., p_m$ son los ceros y los polos de f en D, respectivamente, contados con multiplicidad. Hacemos

$$g(z) = \frac{\prod_{k=1}^{n} j(z) - j(z_k)}{\prod_{k=1}^{m} j(z) - j(p_k)}$$

donde insertamos un 1 si alguno de z_k o p_k es ∞. Entonces f y g tienen los mismos ceros y los mismos polos en D y con la misma multiplicidad, además f y g son funciones modulares de peso 0 y por lo tanto f/g es una función modular de peso 0 sin ceros ni polos en D, luego por la identidad (1.28) aplicada a f/g (con $k = 0$), se debe tener $v_\infty(f/g) = 0$ y entonces f/g no tiene un cero ni un polo en infinito y por lo tanto f/g debe ser una forma modular de peso 0, pero sabemos por (1.3.5) que las formas modulares de peso 0 son las constantes y por lo tanto $f/g = c$, de donde se sigue que $f = gc$, es decir f es una función racional de j. ■

1.4. Expansión en Infinito

1.4.1. Los números de Bernoulli $\mathbf{B_k}$

Definición 1.4.1. *Los números de Bernoulli B_k se pueden definir por la expansión en serie de potencias:*

$$\frac{x}{e^x - 1} = \frac{x}{2}\Big(\coth\frac{x}{2} - 1\Big) = \frac{x}{2}\sum_{k=-1}^{\infty} c_k x^k = 1 - \frac{x}{2} + \sum_{k=1}^{\infty}(-1)^{k+1} B_k \frac{x^{2k}}{(2k)!} \quad (1.44)$$

Para la definición anterior se ha usado que la serie de Laurent de $\coth z$ es de la forma $\sum_{k=-1}^{\infty} c_k x^k$ con $c_{-1} = 1$ y $c_{2k} = 0$.
Enlistamos a continuación los primeros 7 valores para los números de Bernoulli[6]:

$$B_1 = \frac{1}{6}, \quad B_2 = \frac{1}{30}, \quad B_3 = \frac{1}{42} \quad B_4 = \frac{1}{30}, \quad B_5 = \frac{5}{66}, \quad B_6 = \frac{691}{2730}, \quad B_7 = \frac{7}{6}$$

Los B_k dan los valores de la función zeta de Riemann para los enteros positivos pares (y también para los enteros impares negativos):

Teorema 1.4.1. *Si k es un entero mayor o igual a 1, entonces:*

$$\zeta(2k) = \frac{2^{2k-1}}{(2k)!} B_k \pi^{2k} \tag{1.45}$$

Demostración. Tenemos que

$$z \cot z = z\frac{e^{iz} + e^{-iz}}{2} \cdot \frac{2i}{e^{iz} - e^{-iz}} = iz\frac{e^{iz} + e^{-iz}}{e^{iz} - e^{-iz}} = iz\frac{e^{2iz} + 1}{e^{2iz} - 1} \tag{1.46}$$

y por otro lado al poner $x = 2iz$ en (1.44), tenemos

$$\frac{2iz}{e^{2iz} - 1} = 1 - \frac{2iz}{2} + \sum_{k=1}^{\infty} (-1)^{k+1} B_k \frac{(2iz)^{2k}}{(2k)!} \tag{1.47}$$

y al sumar $\frac{2iz}{2}$ a (1.47) nos da la identidad

$$iz\frac{e^{2iz} + 1}{e^{2iz} - 1} = \frac{2iz}{e^{2iz} - 1} + iz = 1 + \sum_{k=1}^{\infty} (-1)^{k+1} B_k \frac{(2iz)^{2k}}{(2k)!} \tag{1.48}$$

y así, juntando (1.47) y (1.48) nos queda la identidad

$$\begin{aligned} z \cot z &= 1 + \sum_{k=1}^{\infty} (-1)^{k+1} B_k \frac{(2iz)^{2k}}{(2k)!} = 1 + \sum_{k=1}^{\infty} (-1)^{2k+1} B_k \frac{(2)^{2k} z^{2k}}{(2k)!} \\ &= 1 - \sum_{k=1}^{\infty} B_k \frac{(2)^{2k} z^{2k}}{(2k)!} \end{aligned} \tag{1.49}$$

Ahora usando la identidad[7]

$$\pi \cot \pi w = \frac{1}{w} + 2\sum_{n=1}^{\infty} \frac{w}{w^2 - n^2}$$

[6]Esta lista ha sido tomada de [13]
[7]Está identidad puede consultarse en el apéndice “B. Identidad de Euler para cotangente.”

y haciendo $z = \pi w$ tenemos

$$\pi \cot z = \frac{\pi}{z} + 2\sum_{n=1}^{\infty} \frac{\frac{z}{\pi}}{(\frac{z}{\pi})^2 - n^2} = \frac{\pi}{z} + 2\sum_{n=1}^{\infty} \frac{\pi z}{z^2 - n^2\pi^2} \tag{1.50}$$

Usando la ecuación (1.50) tenemos

$$\begin{aligned} z\,\cot z &= z\left(\frac{1}{z} + 2\sum_{n=1}^{\infty} \frac{z}{z^2 - n^2\pi^2}\right) \\ &= 1 + 2\sum_{n=1}^{\infty} \frac{z^2}{z^2 - n^2\pi^2} = 1 - 2\sum_{n=1}^{\infty}\left(\frac{1}{1 - (\frac{z}{n\pi})^2} - 1\right) \\ &= 1 - 2\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}\left(\frac{z}{n\pi}\right)^{2k} = 1 - 2\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}\frac{z^{2k}}{n^{2k}\pi^{2k}} \\ &= 1 - 2\sum_{k=1}^{\infty}\sum_{n=1}^{\infty}\frac{z^{2k}}{n^{2k}\pi^{2k}} = 1 - 2\sum_{k=1}^{\infty}\frac{\zeta(2k)z^{2k}}{\pi^{2k}} \end{aligned} \tag{1.51}$$

comparando ambas expresiones para $z\,\cot z$ obtenemos el resultado.

■

Corolario 1.4.1.1. *Sea ζ la función zeta de Riemann se tiene:*

$$\zeta(2) = \frac{\pi^2}{2\cdot 3}, \quad \zeta(4) = \frac{\pi^4}{2\cdot 3^2\cdot 5}, \quad \zeta(6) = \frac{\pi^6}{3^3\cdot 5\cdot 7}$$
$$\zeta(8) = \frac{\pi^8}{2\cdot 3^3\cdot 5^2\cdot 7}, \quad \zeta(10) = \frac{\pi^{10}}{3^5\cdot 5\cdot 7\cdot 11}, \quad \zeta(12) = \frac{691\pi^{12}}{3^6\cdot 5^3\cdot 7^2\cdot 11\cdot 13}$$

Demostración. Sustituyendo los valores conocidos:

$$B_1 = \frac{1}{6}, \quad B_2 = \frac{1}{30}, \quad B_3 = \frac{1}{42} \quad B_4 = \frac{1}{30}, \quad B_5 = \frac{5}{66}, \quad B_6 = \frac{691}{2730},$$

en la ecuación (1.45) del teorema (1.4.1) tenemos

$$
\begin{aligned}
\zeta(2) &= \frac{2^1}{2!}B_1\pi^2 = \frac{2^1}{2!}\frac{1}{6}\pi^2 = \frac{\pi^2}{2\cdot 3}\\
\zeta(4) &= \frac{2^3}{4!}B_2\pi^4 = \frac{2^3}{4!}\frac{1}{30}\pi^4 = \frac{\pi^4}{2\cdot 3^2\cdot 5}\\
\zeta(6) &= \frac{2^5}{6!}B_3\pi^6 = \frac{2^5}{6!}\frac{1}{42}\pi^6 = \frac{\pi^6}{3^3\cdot 5\cdot 7}\\
\zeta(8) &= \frac{2^7}{8!}B_4\pi^8 = \frac{2^7}{8!}\frac{1}{30}\pi^8 = \frac{\pi^8}{2\cdot 3^3\cdot 5^2\cdot 7}\\
\zeta(10) &= \frac{2^9}{10!}B_5\pi^{10} = \frac{2^9}{10!}\frac{5}{66}\pi^{10} = \frac{\pi^{10}}{3^5\cdot 5\cdot 7\cdot 11}\\
\zeta(12) &= \frac{2^{11}}{12!}B_6\pi^{12} = \frac{2^{11}}{12!}\frac{691}{2730}\pi^{12} = \frac{691\pi^{12}}{3^6\cdot 5^3\cdot 7^2\cdot 11\cdot 13}
\end{aligned}
$$

■

Daremos ahora la expansión como serie de Taylor de la serie de Eisenstein $G_k(z)$ con respecto a $q = e^{2\pi iz}$.

Empecemos con la siguiente formula:

$$\pi\cot\pi z = \frac{1}{z} + \sum_{m=1}^{\infty}\frac{1}{z+m} + \frac{1}{z-m} \tag{1.52}$$

Tenemos por otro lado:

$$\pi\cot\pi z = \pi\frac{\cos\pi z}{\sin\pi z} = \pi i\,\frac{e^{\pi iz}+e^{-\pi iz}}{e^{\pi iz}-e^{-\pi iz}} = \pi i\,\frac{e^{2\pi iz}+1}{e^{2\pi iz}-1} \tag{1.53}$$

reemplazando ahora $e^{2\pi iz}$ por q en (1.53) obtenemos:

$$\pi i\,\frac{q+1}{q-1} = \frac{(1-q)\pi i - 2\pi i}{1-q} = \pi i - \frac{2\pi i}{1-q} = \pi i - 2\pi i\sum_{n=0}^{\infty} q^n \tag{1.54}$$

comparando (1.52) con (1.54) tenemos

$$\frac{1}{z} + \sum_{m=1}^{\infty}\frac{1}{z+m} + \frac{1}{z-m} = \pi i - 2\pi i\sum_{n=0}^{\infty} q^n \tag{1.55}$$

Ahora usaremos (1.55) para probar el siguiente lema.

Lema 1.4.2. *Para todo entero $k \geq 2$ se tiene:*

$$\sum_{m\in\mathbb{Z}}\frac{(-1)^{k-1}(k-1)!}{(m+z)^k} = -(2\pi i)^k\sum_{n=1}^{\infty} n^{k-1}q^n \tag{1.56}$$

Demostración. Haremos la prueba por inducción. Derivando ambos lados de (1.55) respecto a z obtenemos:

$$\sum_{m\in\mathbb{Z}} \frac{-1}{(m+z)^2} = \sum_{m\in\mathbb{Z}} \frac{(-1)^{(2-1)}(2-1)!}{(m+z)^2} = -(2\pi i)^1 \sum_{n=1}^{\infty} n^{2-1} q^n \tag{1.57}$$

ya que podemos derivar ambos lados término por término, pues ambas series representan funciones meromorfas, y ya que

$$\frac{d}{dz}\frac{1}{(m+z)} = \frac{-1}{(m+z)^2}$$

y dado que $q = e^{2\pi i z}$, se tiene que

$$\begin{aligned}\frac{d}{dz} q^n &= \frac{d}{dz}(e^{2\pi i z})^n = n(e^{2\pi i z})^{n-1}(e^{2\pi i z})(2\pi i)\\ &= n(2\pi i) q^n \quad \text{si} \quad n \neq 0 \quad \text{y cero si} \quad n = 0 \end{aligned}\tag{1.58}$$

Hacemos entonces (1.57) nuestra base de inducción. Nuestra hipótesis de inducción es que se satisface (1.56) para todo $2 \leq j < k$
Queremos probar que se satisface (1.56) para k pero, usando nuestra hipótesis para $j = k-1$ tenemos la identidad:

$$\sum_{m\in\mathbb{Z}} \frac{(-1)^{k-2}(k-2)!}{(m+z)^{k-1}} = -(2\pi i)^{k-1} \sum_{n=1}^{\infty} n^{k-2} q^n \tag{1.59}$$

y derivándola de ambos lados respecto a z concluimos el paso inductivo, pues

$$\frac{d}{dz}\frac{1}{(m+z)^{k-1}} = \frac{-(k-1)(m+z)^{k-2}}{(m+z)^{2k-2}} = \frac{(-1)(k-1)}{(m+z)^k}$$

y

$$\frac{d}{dz} n^{k-2} q^n = (2\pi i) n^{k-1} q^n$$

y al multiplicar estas derivadas por las constantes que tenemos por la hipótesis de inducción y tomar la suma obtenemos justamente la igualdad (1.56).

■

Corolario 1.4.2.1. *Para todo entero $k \geq 2$ se tiene:*

$$\sum_{m\in\mathbb{Z}} \frac{1}{(m+z)^k} = \frac{1}{(k-1)!}(-2\pi i)^k \sum_{n=1}^{\infty} n^{k-1} q^n \tag{1.60}$$

Denotamos por $\sigma_k(n)$ a la suma $\sum_{d|n} d^k$ de las k-esimas potencias de los divisores positivo de n. Utilizaremos ahora el corolario (1.4.2.1) para probar el siguiente teorema.

Teorema 1.4.3. *Para todo entero $k \geq 2$ se tiene:*

$$G_k(z) = 2\zeta(2k) + 2\,\frac{(2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n \tag{1.61}$$

Demostración. Expandimos:

$$G_k(z) = \sum_{(n,m)\neq(0,0)} \frac{1}{(nz+m)^{2k}} = 2\zeta(2k) + 2\sum_{n=1}^{\infty}\sum_{m\in\mathbb{Z}}\frac{1}{(nz+m)^{2k}} \tag{1.62}$$

Donde, como se ha visto anteriormente, el término $2\zeta(2k)$ se obtiene al tomar la suma cuando $n = 0$. Aplicamos el corolario (1.4.2.1) reemplazando z por nz y cambiamos por claridad de la demostración el indice n usado en el corolario (1.4.2.1)por el indice d:

$$\begin{aligned} G_k(z) &= 2\zeta(2k) + 2\sum_{n=1}^{\infty}\frac{(-2\pi i)^{2k}}{(2k-1)!}\sum_{d=1}^{\infty} d^{2k-1}q^{nd} \\ &= 2\zeta(2k) + \frac{2(-2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sum_{d=1}^{\infty} d^{2k-1}q^{nd} \end{aligned} \tag{1.63}$$

Cambiemos el indice n por el indice a, con la intención de calcular la suma (doble) buscada pero ahora agrupando los términos en los que el exponente de q son iguales. Retomando (1.63) con estos cambios tenemos entonces:

$$\begin{aligned} G_k(z) &= 2\zeta(2k) + \frac{2(-2\pi i)^{2k}}{(2k-1)!}\sum_{a=1}^{\infty}\sum_{d=1}^{\infty} d^{2k-1}q^{ad} \\ &= 2\zeta(2k) + \frac{2(-2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sum_{d\mid n} d^{2k-1}q^{n} \\ &= 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n \end{aligned} \tag{1.64}$$

donde hemos usado que ad es igual a un entero fijo n justamente cuando d (y a) es un divisor de n.

■

Corolario 1.4.3.1. $G_k(z) = 2\zeta(2k)E_k(z)$ *con*

$$E_k(z) = 1 + \gamma_k\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n \tag{1.65}$$

y

$$\gamma_k = (-1)^k\frac{4k}{B_k} \tag{1.66}$$

Demostración. Definimos E_k como el cociente de $G_k(z)$ por $2\zeta(2k)$. Por la ecuación (1.61) establecida en el teorema anterior concluimos que E_k tiene la forma buscada con $\gamma_k = \frac{(2\pi i)^{2k}}{\zeta(2k)(2k-1)!}$. Por otro lado según el teorema (1.4.1) tenemos

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

de donde se sigue que

$$\gamma_k = \frac{(2\pi i)^{2k}}{\zeta(2k)(2k-1)!} = \frac{(2k)!}{2^{2k-1}B_k\pi^{2k}} \frac{(2\pi i)^{2k}}{(2k-1)!} = (-1)^k \frac{4k}{B_k} \tag{1.67}$$

■

Corolario 1.4.3.2.

$$\Delta(z) = (12\pi)^{12} \sum_{n=1}^{\infty} \tau(n) q^n$$

donde $\tau(n)$ es un entero para toda n y $\tau(1) = 1$, $\tau(2) = -24$.

Demostración. Tenemos que $g_2(z) = 60G_2(z)$ por lo que usando el corolario (1.4.3.1) tenemos

$$g_2(z) = 60G_2(z) = 120\zeta(4)E_2(z) = \frac{4\pi^4}{3} E_2(z) \tag{1.68}$$

Por otro lado $g_3(z) = 140G_3(z)$ por lo que usando el corolario (1.4.3.1) tenemos

$$g_3(z) = 140G_3(z) = 280\zeta(6)E_3(z) = \frac{8\pi^6}{27} E_2 \tag{1.69}$$

Recordando que $\Delta(z) = g_2^3 - 27g_3^2$ tenemos

$$\Delta(z) = g_2^3 - 27g_3^2 = \frac{64\pi^{12}}{27} E_2^3 - 27\frac{64\pi^{12}}{27^2} E_3^2 = \frac{64\pi^{12}}{27}(E_2^3 - E_3^2) \tag{1.70}$$

si hacemos

$$A = \sum_{n=1}^{\infty} \sigma_3(n) q^n, \quad B = \sum_{n=1}^{\infty} \sigma_5(n) q^n \tag{1.71}$$

y usamos la identidad (1.65) del corolario (1.4.3.1) en (1.70) , tenemos

$$\Delta(z) = \frac{64\pi^{12}}{27}(E_2^3 - E_3^2) = \frac{64\pi^{12}}{27}((1+240A)^3 - (1-504B)^2) \tag{1.72}$$

Ahora, A y B tienen coeficientes enteros y

$$\begin{aligned} (1+240A)^3 - (1-504B)^2 = \\ &= 1 + 720A + 3(240)^2A^2 + (240)^3A^3 - 1 + 1008B - (504)^2B^2 \\ &= 12^2(5A+7B) + 12^3(100A^2 - 147B^2 + 8000A^3) \end{aligned} \tag{1.73}$$

pero

$$5A + 7B = \sum_{n=1}^{\infty} 5\sigma_3(n)q^n + \sum_{n=1}^{\infty} 7\sigma_5(n)q^n \tag{1.74}$$

y

$$5d^3 + 7d^5 = d^3(5 + 7d^2) \equiv \begin{cases} d^3(d^2 - 1) \equiv 0 \pmod{3} \\ d^3(1 - d^2) \equiv 0 \pmod{4}. \end{cases} \tag{1.75}$$

Por lo tanto

$$5d^3 + 7d^5 \equiv 0 \pmod{12}$$

Entonces 12^3 es un factor de cada coeficiente en la expansión en serie de potencias de $((1 + 240A)^3 - (1 - 504B)^2)$ de donde se sigue que

$$\Delta(z) = \frac{64\pi^{12}}{27}\left(12^3 \sum_{n=1}^{\infty} \tau(n)q^n\right) = (2\pi)^{12} \sum_{n=1}^{\infty} \tau(n)q^n$$

y cada uno de los $\tau(n)$ es un entero. Además, observando la expansión de la ecuación (1.73), tenemos que el coeficiente de q es $12^2(5+7)$ y el coeficiente de q^2 es $12^2(5 \cdot 9 + 7 \cdot 33) + 12^3(100 - 147) = 12^3(-24)$ y al juntar esto con (1.72) tenemos $\tau(1) = 1$ y $\tau(2) = -24$. ■

Corolario 1.4.3.3.

$$j(z) = \frac{12^3 g_2^3(z)}{\Delta(z)} = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c_n q^n$$

donde los c_n son enteros.

Demostración. A lo largo de esta demostración escribiremos I para denotar cualquier serie de potencias con coeficientes enteros y tal que los coeficientes a_0 y a_1 de I son iguales a 0. Por lo visto en la demostración del corolario (1.4.3.2) tenemos

$$g_2^3(z) = \frac{64\pi^{12}}{27}(1 + 240q + I)^3 = \frac{64\pi^{12}}{27}(1 + 720q + I) \tag{1.76}$$

y

$$\Delta(z) = \frac{64\pi^{12}}{27}(12^3 q(1 - 24q + I)) \tag{1.77}$$

Dado que Δ tiene un cero simple en infinito, entonces la función $f(q) = 1 - 24q + I$ es holomorfa y no cero $q = 0$, por lo tanto tiene una serie de Taylor alrededor de $q = 0$. Ahora, sea

$$f(q) = 1 - 24q + I = \sum_{n=0}^{\infty} a_n q^n$$

Por la forma de la serie de Taylor de f alrededor de $q = 0$ tenemos que $f(0) = 1$. Como f es holomorfa y no cero en $q = 0$ se tiene, al considerar $1/f(q)$ que

$h(q) = 1/f(q)$ es holomorfa en $q = 0$ y además $h(0) = 1$. Veremos que la serie de Taylor de $h(q)$ alrededor de $q = 0$ es de la forma

$$h(q) = 1 - 24q + I$$

para ver esto notamos que

$$1 = f(q) \cdot 1/f(q) = f(q)h(q) = (1 - 24q + I)\left(\sum_{n=0}^{\infty} b_n q^n\right) \tag{1.78}$$

Ya vimos que $b_0 = 1$ y tenemos que $a_0 = 1$ y $a_1 = -24$ y dado que el producto de las series en la ecuación (1.78) es igual a 1, se debe tener para todo n que

$$0 = c_n = \sum_{k=0}^{n} a_{n-k} b_k \tag{1.79}$$

esto implica en particular que

$$b_1 = -a_1 b_0 = -1 \cdot 24 \tag{1.80}$$

y en general

$$b_n = b_n a_0 = -\sum_{k=0}^{n-1} a_{n-k} b_k \tag{1.81}$$

como $a_0 = b_0 = 1$ y los a_n son enteros, es fácil ver inductivamente de la ecuación (1.81) que los b_n son enteros y por lo tanto

$$h(q) = 1 - 24q + I.$$

Finalmente utilizando las ecuaciones (1.76) y (1.77) tenemos

$$\frac{j(z)}{12^3} = \frac{g_2^3(z)}{\Delta(z)} = \frac{1 + 720q + I}{12^3 q(1 - 24q + I)} = \frac{1}{12^3 q}(1 + 720q + I)(1 + 24q + I) \tag{1.82}$$

de donde concluimos

$$j(z) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c_n q^n$$

donde los c_n son enteros. ■

Notemos que E_k es una forma modular de peso $2k$ tal que $E_k(\infty) = 1$ para todo $k > 2$. Lo anterior es cierto pues por (1.2.3) tenemos que $G_k(\infty) = 2\zeta(2k)$ y por el corolario (1.4.3.1) tenemos:

$$2\zeta(2k) = G_k(\infty) = 2\zeta(2k)E_k(\infty)$$

Recordamos que las dimensiones de M_4 y M_5 son ambas 1, y por lo tanto las formas modulares de pesos 8 y 10 que valen 1 en infinito son únicas. Se debe tener entonces

$$E_2\, E_2 = E_4 \tag{1.83}$$

$$E_2\, E_3 = E_5 \tag{1.84}$$

Usando (1.4.3.1) y los valores $B_2 = \frac{1}{30}$, $B_3 = \frac{1}{42}$ $B_4 = \frac{1}{30}$, $B_5 = \frac{5}{66}$, tenemos:

$$E_2 = 1 + \gamma_2 \sum_{n=1}^{\infty} \sigma_3(n) q^n = 1 + (-1)^2 \frac{8}{B_2} \sum_{n=1}^{\infty} \sigma_3(n) q^n = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n \tag{1.85}$$

$$E_3 = 1 + \gamma_3 \sum_{n=1}^{\infty} \sigma_5(n) q^n = 1 + (-1)^3 \frac{12}{B_3} \sum_{n=1}^{\infty} \sigma_5(n) q^n = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n \tag{1.86}$$

$$E_4 = 1 + \gamma_4 \sum_{n=1}^{\infty} \sigma_7(n) q^n = 1 + (-1)^4 \frac{16}{B_4} \sum_{n=1}^{\infty} \sigma_7(n) q^n = 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n) q^n \tag{1.87}$$

$$E_5 = 1 + \gamma_5 \sum_{n=1}^{\infty} \sigma_9(n) q^n = 1 + (-1)^5 \frac{20}{B_5} \sum_{n=1}^{\infty} \sigma_9(n) q^n = 1 - 264 \sum_{n=1}^{\infty} \sigma_5(n) q^n \tag{1.88}$$

y substituyendo estos valores en (1.83) y (1.84) y fijándonos en el coeficiente de q^n de ambos lados, tenemos:

$$\sigma_7(n) = \sigma_3 + 120 \sum_{m=1}^{n-1} \sigma_3(m)\, \sigma_3(n-m) \tag{1.89}$$

$$11\sigma_9(n) = 21\sigma_5 - 10\sigma_3 + 5040 \sum_{m=1}^{n-1} \sigma_3(m)\, \sigma_5(n-m) \tag{1.90}$$

Más generalmente, cada E_k se puede expresar en términos de E_2 y E_3.

1.4.2. Estimaciones para los coeficientes de las formas modulares

Sea

$$f(z) = \sum_{n=0}^{\infty} a_n q^n \quad (q = e^{2\pi i z}) \tag{1.91}$$

una forma modular de peso $2k$, $k \geq 2$. Estamos interesados en el crecimiento de a_n. Tenemos los siguientes teoremas.

Teorema 1.4.4. *Si $f = G_k$, el orden de magnitud de a_n es n^{2k-1}. Más precisamente, existen dos constantes $A, B > 0$ que dependen solamente de k, tales que*

$$An^{2k-1} \leq |a_n| \leq Bn^{2k-1} \tag{1.92}$$

Demostración. El teorema (1.4.3) muestra que existe una constante $A > 0$ tal que

$$a_n = (-1)^k A\sigma_{2k-1}(n), \quad \text{por lo tanto} \quad |a_n| = A\sigma_{2k-1}(n) \geq An^{2k-1} \tag{1.93}$$

por otro lado:

$$\frac{|a_n|}{n^{2k-1}} = A\sum_{d|n} \frac{1}{d^{2k-1}} \leq A\sum_{d=1}^{\infty} \frac{1}{d^{2k-1}} = A\zeta(2k-1) < +\infty \tag{1.94}$$

y entonces A y $B = A\zeta(2k-1)$ cumplen las condiciones.

■

Teorema 1.4.5 (Hecke). *Si f es una forma cuspidal de peso $2k$, entonces*

$$a_n = O(n^k) \tag{1.95}$$

(en otras palabras, el cociente $\frac{|a_n|}{n^k}$ permanece acotado cuando n tiende a infinito).

Demostración. Dado que $f(z) = \sum_{n=0}^{\infty} a_n q^n$ es una forma cuspidal, se tiene que $a_0 = 0$ y por lo tanto podemos factorizar q de la expansión de f y tenemos

$$f(z) = q\sum_{n=1}^{\infty} a_n q^{n-1} \tag{1.96}$$

además, dado que la series $\sum_{n=1}^{\infty} a_n q^n$ define una función holomorfa en el interior del disco unitario, se tiene que el radio de convergencia de la serie $\sum_{n=1}^{\infty} a_n q^n$ es mayor o igual a 1, y por lo tanto su derivada $\sum_{n=1}^{\infty} n a_n q^{n-1}$ converge absolutamente en el disco unitario y como $|a_n q^{n-1}| \leq |n a_n q^{n-1}|$, se tiene que para todo $\epsilon > 0$ existe N tal que si $m > N$, entonces se satisface la siguiente desigualdad

$$\left|\sum_{n=m}^{\infty} a_n q^{n-1}\right| \leq \sum_{n=m}^{\infty} |a_n q^{n-1}| \leq \sum_{n=m}^{\infty} |n a_n q^{n-1}| < \epsilon \tag{1.97}$$

la cual implica que la sucesión $\{f_r\}$, con $f_r = \sum_{n=1}^{r} a_n q^{n-1}$ converge uniformemente a $g(q) = \sum_{n=1}^{\infty} a_n q^{n-1}$ y ya que las f_r son continuas, entonces también lo es g.

Utilizando la ecuación (1.96), tenemos:

$$|f(z)| = |q|\left|\sum_{n=1}^{\infty} a_n q^{n-1}\right| = |q||g(z)| = O(q) = O(e^{-2\pi y}) \tag{1.98}$$

cuando q tiende a 0, donde $y = \Im(z)$, pues como g es una función continua en el disco unitario, entonces g tiene un máximo en los discos cerrados centrados en el origen y contenidos en el disco unitario. Ahora hacemos $\phi(z) = |f(z)|y^k$. Observamos que, dado que f es una forma modular se tiene:

$$\phi(z+1) = |f(z+1)|\, y^k = |f(z)|\, y^k$$
$$\phi\left(-\frac{1}{z}\right) = \left|f\left(-\frac{1}{z}\right)\right|\left(\frac{y}{|z|^2}\right)^k = \left|z^k f(z)\right|\left(\frac{y}{|z|^2}\right)^k = |f(z)|\, y^k$$

es decir, ϕ es invariante bajo los elementos T y S de G y por lo tanto ϕ es invariante bajo el grupo modular. Adicionalmente, ϕ es continua en el dominio fundamental D y la ecuación (1.98) implica que ϕ tiende a 0 cuando $y = \Im(z)$ tiende a infinito. Por lo anterior, podemos concluir que ϕ es acotada en H, es decir existe M tal que

$$|f(z)| \leq My^k \quad \text{para todo } z \in H. \tag{1.99}$$

Fijando y y variando x de 0 a 1 se tiene que el punto $q = e^{2\pi i(x+iy)}$ recorre una circunferencia C_y centrada en 0 . Por la formula del residuo se tiene:

$$a_n = \frac{1}{2\pi i}\int_{C_y} f(z)q^{-n-1}dq = \int_0^1 f(x+iy)q^{-n}dx. \tag{1.100}$$

Usando (1.99) obtenemos:

$$|a_n| = \left|\int_0^1 f(x+iy)q^{-n}dx\right| \leq \int_0^1 \left|f(x+iy)q^{-n}\right| dx \leq My^k e^{2\pi ny} \tag{1.101}$$

Esta desigualdad es valida para todo $y > 0$. Para $y = 1/n$ la desigualdad se convierte en $|a_n| \leq e^{2\pi} Mn^k$ de donde se sigue el resultado.

■

1.5. Expresión de Δ como producto infinito

Estamos ahora en posición de probar una expresión del discriminante modular Δ como producto infinito.
Antes que nada consideremos el producto infinito:

$$\prod_{n=1}^{\infty}(1-q^n) \tag{1.102}$$

donde como siempre $q = e^{2\pi i n z}$, por lo que $|q| < 1$ y entonces $\sum_{n=1}^{\infty} q^n$ converge absolutamente y por la proposición 2.4.3 del apéndice A, también $\sum_{n=1}^{\infty} \log(1-q^n)$ converge absolutamente, lo cual a su vez implica, por la proposición 2.4.2 del apéndice A, la convergencia del producto (1.102)[8].

El objetivo ahora es demostrar una expresión de Δ, la forma cuspidal de peso 12 como un producto infinito. Para ellos seguiremos el camino esbozado por Serre en [13], para lo cual primero necesitamos definir las siguientes series dobles y demostrar un par de lemas sobre ellas.

Definimos G_1, G_2, H_1 y H_2 de forma explícita como:

$$G_1(z) = \sum_n \sum_m{}' \frac{1}{(m+nz)^2} \qquad G_2(z) = \sum_m \sum_n{}' \frac{1}{(m+nz)^2} \tag{1.103}$$

$$H_1(z) = \sum_n \sum_m{}' \frac{1}{(m-1+nz)(m+nz)} \quad H_2(z) = \sum_m \sum_n{}' \frac{1}{(m-1+nz)(m+nz)} \tag{1.104}$$

donde el signo $\sum'$ indica que (m,n) recorre todas las parejas $m \in \mathbb{Z}$, $n \in \mathbb{Z}$, con $(m,n) \neq (0,0)$ para G_2 y G_1 y $(m,n) \neq (0,0), (1,0)$ para H_2 y H_1 (obsérvese bien el orden de las sumas).

Lema 1.5.1. *H_1 y H_2 convergen a 2 y $2 - 2\pi i/z$, respectivamente.*

Demostración. Para esto observemos primero la identidad:

$$\frac{1}{(m-1+nz)(m+nz)} = \frac{1}{m-1+nz} - \frac{1}{m+zn} \tag{1.105}$$

estudiemos primero la siguiente suma suponiendo $n \neq 0$

$$\sum_m{}' \left(\frac{1}{m-1+nz} - \frac{1}{m+zn} \right) = \lim_{k\to\infty} \sum_{m=-k}^{k} \left(\frac{1}{m-1+nz} - \frac{1}{m+zn} \right) \tag{1.106}$$

y dado que

$$\left(\frac{1}{m-1+nz} - \frac{1}{m+zn} \right) + \left(\frac{1}{m+nz} - \frac{1}{(m+1)+zn} \right) = \frac{1}{m-1+nz} - \frac{1}{(m+1)+zn}$$

[8] La convergencia del producto (1.102) también se sigue del Teorema 1 en [5] pág. 27.

tenemos que el lado derecho de (1.106) es simplemente:

$$\lim_{k\to\infty}\left(\frac{1}{k-1+nz}-\frac{1}{-k+zn}\right)=\lim_{k\to\infty}\frac{1}{k-1+nz}-\lim_{k\to\infty}\frac{1}{-k+nz}=0 \tag{1.107}$$

Por otro lado si $n=0$, se deben excluir los términos cuando $m=0,1$, por lo que se tiene que:

$$\sum_m{}'\left(\frac{1}{m-1}-\frac{1}{m}\right)=\left(\sum_{m=2}^{\infty}\frac{1}{m-1}-\frac{1}{m}+\sum_{-\infty}^{m=-1}\frac{1}{m-1}-\frac{1}{m}\right) \tag{1.108}$$

y en este caso la suma desde $m=2$ hasta infinito, como la suma en los negativos, son ambas telescópicas y por lo tanto

$$\sum_m{}'\left(\frac{1}{m-1}-\frac{1}{m}\right)=\lim_{k\to\infty}1+\frac{1}{k-1}-\lim_{k\to\infty}1+\frac{1}{-k}=2 \tag{1.109}$$

Las ecuaciones (1.107) y (1.109) implican que H_1 converge en H y $H_1(z)=2$ para todo z en el semiplano superior.

Ahora, recordemos la identidad:

$$\pi\cot\pi z=\frac{1}{z}+\sum_{n=1}^{\infty}\frac{1}{z+n}+\frac{1}{z-n}=\frac{1}{z}+2z\sum_{n=1}^{\infty}\frac{1}{z^2-n^2}$$

la cual es equivalente a:

$$\frac{z\pi\cot\pi z-1}{2z^2}=\sum_{n=1}^{\infty}\frac{1}{z^2-n^2} \tag{1.110}$$

y al remplazar z por $\frac{m}{z}$ en la ecuación anterior nos queda la identidad:

$$z^2\frac{m\pi\cot\left(\frac{\pi m}{z}\right)-z}{2zm^2}=\sum_{n=1}^{\infty}\frac{1}{\left(\frac{m}{z}\right)^2-n^2} \tag{1.111}$$

dividamos ambos lados de (1.111) por $\frac{z^2}{2m}$ y llamemos al resultado $P(z)$, es decir:

$$P_m(z)=\frac{m\pi\cot\left(\frac{\pi m}{z}\right)-z}{zm}=\sum_{n=1}^{\infty}\frac{2m}{m^2-(zn)^2} \tag{1.112}$$

pero, el lado derecho de (1.112) se puede ver de la siguiente forma:

$$P_m(z)=\sum_{n=1}^{\infty}\frac{2m}{m^2-(zn)^2}=\sum_{n=1}^{\infty}\frac{1}{m+nz}+\sum_{n=1}^{\infty}\frac{1}{m-nz}=\sum_{n=1}^{\infty}\frac{1}{m+nz}+\frac{1}{m-nz} \tag{1.113}$$

de donde se sigue que

$$P_m(z) + \frac{1}{m} = \sum_{n\in\mathbb{Z}} \frac{1}{m+nz} \quad \text{si } m \neq 0 \tag{1.114}$$

hagamos $Q_m(z) = P_m(z) + \dfrac{1}{m}$.

Por otro lado si $m = 0$ la suma $\sum'_{n\in\mathbb{Z}} \frac{1}{nz}$ es claramente 0.

Además tenemos que:

$$Q_{-m}(z) = P_{-m}(z) - \frac{1}{m} = -\frac{-m\pi\cot\left(-\frac{\pi m}{z}\right) - z}{zm} - \frac{1}{m} \tag{1.115}$$

y como cot es una función impar, la ecuación anterior es igual a:

$$Q_{-m}(z) = -\frac{m\pi\cot\left(\frac{\pi m}{z}\right) - z}{zm} - \frac{1}{m} = -Q_m(z) \tag{1.116}$$

y de hecho también probamos que $P_{-m}(z) = -P_m(z)$.

Con lo anterior podemos ahora calcular $H_2(z)$ (y ver que $H_2(z)$ converge):

$$\begin{aligned} H_2(z) &= \sum_m \sum_n{}' \frac{1}{(m-1+nz)(m+nz)} \\ &= -\left(\sum_{n=1}^{\infty} \frac{1}{1+zn} + \frac{1}{1-zn}\right) + \left(\sum_{m=2}^{\infty}\sum_n \frac{1}{m-1+nz} - \frac{1}{m+zn}\right) \\ &+ \left(\sum_{n=1}^{\infty} \frac{1}{-1+zn} + \frac{1}{-1-zn}\right) + \left(\sum_{m=1}^{\infty}\sum_n \frac{1}{-m-1+nz} - \frac{1}{-m+zn}\right) \\ &= -(Q_1(z)-1) + \left(\sum_{m=2}^{\infty} Q_{m-1}(z) - Q_m(z)\right) \\ &+ (Q_{-1}(z)+1) + \left(\sum_{m=1}^{\infty} Q_{-m-1}(z) - Q_{-m}(z)\right) \end{aligned} \tag{1.117}$$

La suma en la última igualdad de (1.117) es telescópica, por lo que el valor de $H_2(z)$ es igual a lo siguiente:

$$H_2(z) = 2 - \lim_{m\to\infty} Q_m(z) + \lim_{m\to\infty} Q_{-m-1}(z) = 2 - 2\lim_{m\to\infty} Q_m(z) \tag{1.118}$$

ya que $\quad Q_{-m}(z) = -Q_m(z)$

por lo que basta ahora calcular el limite de $Q_m(z)$ cuando m tiende a infinito, es decir

$$\begin{aligned}
\lim_{m\to\infty} Q_m(z) &= \lim_{m\to\infty} \frac{m\pi\cot\left(\frac{\pi m}{z}\right) - z}{zm} + \frac{1}{m} = \lim_{m\to\infty} \frac{\pi\cot\left(\frac{\pi m}{z}\right)}{z} - \frac{1}{m} + \frac{1}{m} \\
&= \frac{\pi}{z}\lim_{m\to\infty} \cot\left(\frac{\pi m}{z}\right) = \frac{\pi}{z}\lim_{m\to\infty} -i\frac{e^{\frac{\pi i n}{z}} + e^{-\frac{\pi i n}{z}}}{-e^{\frac{\pi i n}{z}} + e^{-\frac{\pi i n}{z}}} \\
&= -i\frac{\pi}{z}\lim_{m\to\infty}\left(-1 + \frac{-1}{-e^{\frac{2\pi i n}{z}} + 1}\right) = -\frac{\pi i}{z}(-1) \qquad (1.119)
\end{aligned}$$

y finalmente sustituyendo este valor en (1.118) tenemos $H_2(z) = 2 - 2\pi i/z$. ■

Lema 1.5.2. *La suma*

$$\sum_{n,m}\left(\frac{1}{(m-1+nz)(m+nz)} - \frac{1}{(m+nz)^2}\right) = \sum_{n,m}\left(\frac{1}{(m-1+nz)(m+nz)^2}\right) \qquad (1.120)$$

es absolutamente sumable.

Demostración. Como se probo en (1.1.2), se tiene que $|m-1+nz| \leq 1$ se cumple solo para un número finito de parejas (n,m). Por lo anterior para todas las parejas (n,m) de enteros, salvo un número finito de ellas se tiene que:

$$\begin{aligned}
2 > 1 + \frac{1}{|m-1+nz|} &= \frac{|m-1+nz| + |1|}{|m-1+nz|} \geq \frac{|m+nz|}{|m-1+nz|} \\
&= \frac{|m+nz|^3}{|m-1+nz||m+nz|^2}
\end{aligned}$$

$$\text{por lo tanto} \quad \frac{2}{|m+nz|^3} > \frac{1}{|m-1+nz||m+nz|^2} \qquad (1.121)$$

y como la suma

$$\sum_{n,m}\frac{1}{|m+nz|^r} \qquad (1.122)$$

converge absolutamente para $r > \frac{5}{2}$ por lo visto en la demostración del teorema (1.2.3), tenemos que (1.121) y el hecho de que hay solo un número finito de parejas (n,m) tales que $|m-1+nz| \leq 1$, implican que la suma (1.120) es absolutamente sumable.

■

Podemos ahora demostrar el teorema siguiente.

Teorema 1.5.3 (Jacobi)**.** $\Delta = (2\pi)^{12} q \prod_{n=1}^{\infty}(1-q^n)^{24}$

Demostración. La convergencia de $(2\pi)^{12}q\prod_{n=1}^{\infty}(1-q^n)^{24}$ se sigue de la convergencia de (1.102). Por otro lado hagamos:

$$F(z)=q\prod_{n=1}^{\infty}(1-q^n)^{24} \tag{1.123}$$

Para demostrar que Δ y F son proporcionales, es suficiente mostrar que F es una forma modular de peso 12, ya que de serlo, el hecho de que la expansión de F tiene termino constante cero, implicaría que F tendría que ser una forma cuspidal y sabemos por el teorema (1.3.5) que el espacio M_6^0 de las formas cuspidales de peso 12 es de dimensión 1. Por la ecuación (1.5) todo lo que tenemos que hacer es mostrar que:

$$F(-1/z)=z^{12}F(z) \tag{1.124}$$

Por otro lado ya que la suma:

$$\sum_{n,m}\left(\frac{1}{(m-1+nz)(m+nz)}-\frac{1}{(m+nz)^2}\right) \tag{1.125}$$

es absolutamente sumable, podemos entonces cambiar el orden de los sumandos sin alterar el valor de la suma y en particular

$$\begin{aligned}H_1(z)-G_1(z)&=\sum_n\sum_m\left(\frac{1}{(m-1+nz)(m+nz)}-\frac{1}{(m+nz)^2}\right)\\&=\sum_{n,m}\left(\frac{1}{(m-1+nz)(m+nz)}-\frac{1}{(m+nz)^2}\right)\\&=\sum_m\sum_n\left(\frac{1}{(m-1+nz)(m+nz)}-\frac{1}{(m+nz)^2}\right)\\&=H_2(z)-G_2(z)\end{aligned} \tag{1.126}$$

Lo anterior muestra que $H_1(z)-G_1(z)$ y $H_2(z)-G_2(z)$ convergen y son iguales (con el orden de adición indicado), y como además por el lema (1.5.1) $H_1(z)$ y $H_2(z)$ convergen, se sigue que $G_1(z)$ y $G_2(z)$ convergen y

$$G_1(z)-G_2(z)=H_1(z)-H_2(z)=2-(2-2\pi i/z)=2\pi i/z \tag{1.127}$$

Observemos que:

$$G_1(-1/z)=\sum_n\sum_m\frac{1}{(m-\frac{n}{z})^2}=\sum_n\sum_m\frac{z^2}{(zm-n)^2}=z^2G_2(z) \tag{1.128}$$

Juntando (1.127) y 1.128 obtenemos:

$$G_1(-1/z) = z^2 G_1(z) - 2\pi i z \tag{1.129}$$

Ahora, ya que $G_1(z)$ converge, podemos usar el teorema (1.4.3) y el hecho de que $\zeta(2) = \pi^2/6$, lo que nos da la identidad:

$$G_1(z) = \frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{\infty} \sigma_1(n) q^n \tag{1.130}$$

Volvamos a la función F definida en (1.123). Su derivada logarítmica es

$$\begin{aligned}
\frac{dF}{F} &= \frac{2\pi i q}{q} - 24 \sum_{n=1}^{\infty} \frac{(1-q^n)^{23} n q^n 2\pi i}{(1-q^n)^{24}} = \frac{2\pi i q}{q} - 24 \sum_{n=1}^{\infty} \frac{n q^n 2\pi i}{1-q^n} \\
&= 2\pi i \left(1 - 24 \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} n q^{nm} \right) = 2\pi i \left(1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) q^n \right) \\
&= 2\pi i - 48\pi i \sum_{n=1}^{\infty} \sigma_1(n) q^n \qquad (1.131)
\end{aligned}$$

Comparando (1.130) con (1.131) obtenemos:

$$\frac{dF(z)}{F(z)} = \frac{6i}{\pi} G_1(z) dz \tag{1.132}$$

Combinando (1.129) y (1.132) tenemos:

$$\begin{aligned}
\frac{dF(-1/z)}{F(-1/z)} &= \frac{6i}{\pi} G_1(-1/z) \frac{dz}{z^2} = \frac{6i}{\pi} \frac{dz}{z^2} (z^2 G_1(z) - 2\pi i z) \qquad (1.133) \\
&= \frac{dF(z)}{F(z)} + 12 \frac{dz}{z} \qquad (1.134)
\end{aligned}$$

así, las funciones $F(-1/z)$ y $z^{12}F(z)$ tienen la misma derivada logarítmica. Por lo tanto existe una constante k tal que $F(-1/z) = kz^{12}F(z)$ para todo $z \in H$. Para $z = i$ tenemos $z^{12} = 1$, $-1/z = z$ y $F(z) \neq 0$ lo que implica que $F(i) = kF(i)$ y por lo tanto $k = 1$, lo que implica (1.124), lo que prueba que F y Δ son proporcionales y al observar los coeficientes asociados al termino q de F y Δ vistos como series concluimos que se tiene la igualdad $\Delta = (2\pi)^{12} q \prod_{n=1}^{\infty} (1-q^n)^{24}$. ■

Capítulo 2

La función Tau de Ramanujan

2.1. Subgrupos de G

Recordemos que hemos definido el invariante modular

$$j = 1728\, g_2^3/\Delta = \frac{12^3 g_2^3}{\Delta}$$

y que según la proposición (1.3.1) j es una función modular de peso 0 (con un polo simple en ∞) y por lo tanto es invariante bajo el grupo modular. Además según la proposición (1.3.2), toda función modular de peso 0 es una función racional de j. En este sentido el encontrar una función modular de peso 0 que sea invariante bajo el grupo modular nos permite expresar todas las funciones modulares de peso 0 como funciones racionales de j, de las cuales algunos son polinomios en j con coeficientes enteros y, como se vio en el corolario 1.4.3.3, la expresión de j como serie de Laurent es

$$j(z) = \frac{12^3 g_2^3(z)}{\Delta(z)} = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c_n q^n$$

donde los coeficientes son enteros y esto nos permitirá por un lado encontrar funciones modulares de peso 0 que tienen coeficientes enteros en su expansión como serie de Laurent y, por otro lado, nos permitirá deducir propiedades aritméticas sobre dichas funciones modulares.

Ramanujan conjeturo propiedades aritméticas sobre su función Tau que, como sabemos ahora, son los coeficientes de una forma cuspidal de peso 12. En este capítulo completaremos las pruebas de Mordell de dichas propiedades, las cuales son esbozadas por Apostol en su libro [2].

Recordemos que, según la definición 1.1.1, el grupo modular puede verse como $G = SL_2(\mathbb{Z})/\{\pm I_2\}$. Si consideráramos algún subgrupo G' del grupo modular podríamos encontrar funciones modulares invariantes bajo G' (de peso 0 respecto a G') tales que no son invariantes bajo G, el grupo modular completo y podríamos encontrar una función invariante bajo G' que juegue el papel de j, es decir que todas las funciones modulares invariantes bajo G' sean funciones racionales de dicha función, esto podría ayudarnos a encontrar otras propiedades aritméticas. Dado que estamos buscando propiedades aritméticas, resulta natural que restrinjamos nuestra atención a subgrupos de G asociados a los primos, sin embargo, resulta mejor definir subgrupos asociados a N para todo $N \in \mathbb{N}$. Con lo anterior en mente tenemos la siguiente definición.

Definición 2.1.1. *Si N es cualquier entero positivo, definimos $\Gamma_0(N)$ como el conjunto de todas las matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ con $c \equiv 0 \pmod{N}$.*

Es fácil verificar que $\Gamma_0(N)$ es un subgrupo de G pues sean $h_1, h_2 \in \Gamma_0(m)$, entonces

$$\text{si} \quad h_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{y} \quad h_2 = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}, \quad \text{con} \quad c \equiv c' \equiv 0 \pmod{N} \tag{2.1}$$

entonces

$$h_3 = h_2 \cdot h_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} A & B \\ ca' + dc' & D \end{pmatrix} \tag{2.2}$$

donde A, B y D son enteros, y entonces $N \mid ca' + dc'$, pues $N \mid c, c'$ y además como h_1 y h_2 tienen determinante 1, también h_3 tiene determinante 1 y por lo tanto h_3 pertenece a $\Gamma_0(N)$.

2.2. Pruebas de Mordell

Sea p un primo fijo, definimos T_μ como la acción de $\begin{pmatrix} 1 & \mu \\ 0 & p \end{pmatrix}$ en H donde μ es un entero, es decir $T_\mu z = \dfrac{z+\mu}{p}$. Sea $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ uno de los dos generadores del grupo modular. Recordemos que S actúa en H de tal manera que $Sz = -\dfrac{1}{z}$. Tenemos entonces el siguiente lema.

Lema 2.2.1. *Lema. Sea p un primo fijo y sea $1 \leq k \leq p-1$, con k entero, se tiene entonces que existe $V = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ perteneciente al grupo modular con $p|c$ tal que $T_k S = V T_h$ con h en el mismo intervalo que k y además cuando k recorre un sistema reducido de residuos $\pmod{p}$ también h recorre un sistema reducido de residuos $\pmod{p}$.*

Demostración. Queremos encontrar $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ con $p|c$ tal que

$$\begin{pmatrix} 1 & k \\ 0 & p \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & h \\ 0 & p \end{pmatrix}$$

es decir tal que

$$\begin{pmatrix} k & -1 \\ p & 0 \end{pmatrix} = \begin{pmatrix} a & ah+bp \\ c & ch+dp \end{pmatrix}$$

tomamos $a = k$ y $c = p$ y tomamos h tal que se tiene la congruencia $kh \equiv -1 \pmod p$ con h en el intervalo $1 \leq h \leq p-1$, esta solución es única y recorre un sistema reducido de residuos a la vez que lo hace k. Elegimos b como el entero tal que $ah + bp = -1$ y tomamos $d = -h$, entonces $ch + dp = 0$ y esto termina la prueba. ■

Lema 2.2.2. *Sea p un primo y k un entero con $1 \leq k \leq p-1$ entonces, existe un entero h tal que*

$$z^{12}\Delta\left(\frac{z+h}{p}\right) = \Delta\left(\frac{kz-1}{pz}\right) \tag{2.3}$$

y h recorre un sistema reducido de residuos $\pmod p$ junto con k.

Demostración. Por el lema (2.2.1) tenemos que existe $V \in \Gamma_0(p)$ tal que $\Delta(T_k S z) = \Delta(V T_h z)$ y más aun, por lo visto en la demostración de dicho lema tenemos que

$$V = \begin{pmatrix} k & -\frac{hk+1}{p} \\ p & -h \end{pmatrix}$$

y como Δ es una forma modular de peso 12 y $V \in G$ tenemos que

$$\Delta(VT_h z) = \left(p\left(\frac{z+h}{p}\right) + -h\right)^{12}\Delta(T_h z) = z^{12}\Delta(T_h z) \tag{2.4}$$

Es decir tenemos, igualando los extremos

$$\Delta\left(\frac{kz-1}{pz}\right) = \Delta(T_k S z) = z^{12}\Delta(T_h z) = z^{12}\Delta\left(\frac{z+h}{p}\right) \tag{2.5}$$

y además, por el lema (2.2.1), h recorre un sistema reducido de residuos junto con k. ■

Lema 2.2.3. *Si f es una función modular y p es un primo, hacemos*

$$f_p(w) = \frac{1}{p}\sum_{\lambda=0}^{p-1} f\left(\frac{w+\lambda}{p}\right) \tag{2.6}$$

si f tiene la expansión de Fourier

$$f(w) = \sum_{n=-m}^{\infty} a(n)e^{2\pi inw} \tag{2.7}$$

Entonces f_p tiene la expansión de Fourier

$$f_p(w) = \sum_{n=-\lfloor m/p \rfloor}^{\infty} a(np)e^{2\pi inw} \tag{2.8}$$

Demostración. Tenemos

$$f_p(w) = \frac{1}{p}\sum_{\lambda=0}^{p-1} f\Big(\frac{w+\lambda}{p}\Big) = \frac{1}{p}\sum_{\lambda=0}^{p-1}\sum_{n=-m}^{\infty} a(n)e^{2\pi in(w+\lambda)/p} \tag{2.9}$$

$$= \frac{1}{p}\sum_{n=-m}^{\infty} a(n)e^{2\pi inw/p}\sum_{\lambda=0}^{p-1} e^{2\pi in\lambda/p} \tag{2.10}$$

pero, si $p|n$, entonces $e^{2\pi in\lambda/p}$ es igual a 1, pues será de la forma $e^{2\pi iN\lambda}$, con N entero y si p no divide a n entonces $e^{2\pi in\lambda/p}$ será una raíz de la unidad distinta de 1 y por lo tanto, tenemos los siguientes dos casos

$$\sum_{\lambda=0}^{p-1} e^{2\pi in\lambda/p} = \begin{cases} 0 & \text{if} \quad p \nmid n \\ p & \text{if} \quad p \mid n \end{cases} \tag{2.11}$$

de donde se sigue

$$f_p(w) = \sum_{\substack{n=-m \\ p|n}}^{\infty} a(n)e^{2\pi inw/p} = \sum_{n=-\lfloor m/p \rfloor}^{\infty} a(np)e^{2\pi inw} \tag{2.12}$$

■

Ahora definamos la siguiente función

Definición 2.2.1. *Definimos la función $F_p(w)$ para todo $w \in H$ de manera explicita como:*

$$F_p(w) = p^{11}\Delta(pw) + \frac{1}{p}\sum_{\lambda=0}^{p-1}\Delta\Big(\frac{w+\lambda}{p}\Big) \tag{2.13}$$

Lema 2.2.4. *Se tiene que*

$$F_p(w) = F_p(w+1) \quad y \quad F_p\left(-\frac{1}{w}\right) = w^{12}F_p(w) \tag{2.14}$$

Demostración. Usando que $\Delta(z+m) = \Delta(z)$ para todo $z \in H$ y todo $m \in \mathbb{Z}$ tenemos que:

$$\begin{aligned}
F_p(w+1) &= p^{11}\Delta(p(w+1)) + \frac{1}{p}\sum_{\lambda=0}^{p-1}\Delta\left(\frac{(w+1)+\lambda}{p}\right)\\
&= p^{11}\Delta(pw+p) + \frac{1}{p}\sum_{\lambda=0}^{p-1}\Delta\left(\frac{w+(\lambda+1)}{p}\right)\\
&= p^{11}\Delta(pw) + \frac{1}{p}\sum_{\lambda=1}^{p}\Delta\left(\frac{w+\lambda}{p}\right)\\
&= p^{11}\Delta(pw) + \frac{1}{p}\sum_{\lambda=0}^{p-1}\Delta\left(\frac{w+\lambda}{p}\right) + \left(\Delta\left(\frac{w+p}{p}\right) - \Delta\left(\frac{w}{p}\right)\right)\\
&= p^{11}\Delta(pw) + \frac{1}{p}\sum_{\lambda=0}^{p-1}\Delta\left(\frac{w+\lambda}{p}\right) + \left(\Delta\left(\frac{w}{p}+1\right) - \Delta\left(\frac{w}{p}\right)\right)\\
&= p^{11}\Delta(pw) + \frac{1}{p}\sum_{\lambda=0}^{p-1}\Delta\left(\frac{w+\lambda}{p}\right) = F_p(w) \qquad (2.15)
\end{aligned}$$

Por otro lado, usando que $\Delta\left(\frac{-1}{z}\right) = z^{12}\Delta(z)$, tenemos:

$$\begin{aligned}
F_p\left(-\frac{1}{w}\right) &= p^{11}\Delta\left(-\frac{p}{w}\right) + \frac{1}{p}\sum_{k=0}^{p-1}\Delta\left(\frac{-\frac{1}{w}+k}{p}\right)\\
&= p^{11}\Delta\left(-\frac{p}{w}\right) + \frac{1}{p}\sum_{k=0}^{p-1}\Delta\left(\frac{kw-1}{pw}\right) \qquad (2.16)
\end{aligned}$$

usando el lema (2.2) en la ecuación (2.16) y que $\Delta\left(\frac{-1}{z}\right) = z^{12}\Delta(z)$, tenemos:

$$\begin{aligned}
F_p\left(-\frac{1}{w}\right) &= p^{11}\Delta\left(-\frac{p}{w}\right) + \frac{w^{12}}{p}\sum_{h=1}^{p-1}\Delta\left(\frac{w+h}{p}\right) + \frac{1}{p}\Delta\left(-\frac{1}{wp}\right)\\
&= p^{11}\left(\frac{w}{p}\right)^{12}\Delta\left(\frac{w}{p}\right) + \frac{w^{12}}{p}\sum_{h=1}^{p-1}\Delta\left(\frac{w+h}{p}\right) + \frac{(wp)^{12}}{p}\Delta(wp)\\
&= \frac{w^{12}}{p}\Delta\left(\frac{w}{p}\right) + \frac{w^{12}}{p}\sum_{h=1}^{p-1}\Delta\left(\frac{w+h}{p}\right) + w^{12}p^{11}\Delta(wp)\\
&= w^{12}\left(p^{11}\Delta(wp) + \frac{1}{p}\sum_{h=0}^{p-1}\Delta\left(\frac{w+h}{p}\right)\right)\\
&= w^{12}F_p(w) \qquad (2.17)
\end{aligned}$$

■

Lema 2.2.5. *$F_p(w)$ es una forma cuspidal de peso 12 con la siguiente expansión*

$$F_p(w) = (2\pi)^{12}\left(p^{11}\sum_{n=1}^{\infty}\tau(n)e^{2\pi inpw} + \sum_{n=1}^{\infty}\tau(np)e^{2\pi inw}\right) \tag{2.18}$$

Demostración. Dado que F_p es una combinación lineal de funciones holomorfas en H, entonces F_p es holomorfa en H, más aun, dado que

$$\Delta(z) = (2\pi)^{12}\sum_{n=1}^{\infty}\tau(n)e^{2\pi inz}$$

entonces

$$p^{11}\Delta(pw) = p^{11}(2\pi)^{12}\sum_{n=1}^{\infty}\tau(n)e^{2\pi inpw} \tag{2.19}$$

además, aplicando el lema (2.2.3) con $f = \Delta$, tenemos

$$\frac{1}{p}\sum_{\lambda=0}^{p-1}\Delta\Big(\frac{w+\lambda}{p}\Big) = (2\pi)^{12}\sum_{n=1}^{\infty}\tau(np)e^{2\pi inw} \tag{2.20}$$

Usando las ecuaciones (2.19) y (2.20), tenemos

$$\begin{aligned} F_p(w) &= p^{11}\Delta(pw) + \frac{1}{p}\sum_{\lambda=0}^{p-1}\Delta\Big(\frac{w+\lambda}{p}\Big) \\ &= p^{11}(2\pi)^{12}\sum_{n=1}^{\infty}\tau(n)e^{2\pi inpw} + (2\pi)^{12}\sum_{n=1}^{\infty}\tau(np)e^{2\pi inw} \\ &= (2\pi)^{12}\left(p^{11}\sum_{n=1}^{\infty}\tau(n)e^{2\pi inpw} + \sum_{n=1}^{\infty}\tau(np)e^{2\pi inw}\right) \end{aligned} \tag{2.21}$$

además, por el lema (2.2.4), tenemos que $F_p(w) = F_p(w+1)$ por lo cual la identidad (2.21), es la expansión como serie de Fourier de $F_p(w)$, $\tilde{F_p}(q)$, alrededor de $q = 0$, donde como siempre $q = e^{2\pi iw}$. Más aun, el lema (2.2.4) implica que F_p es débilmente modular de peso 12 y dado que la expansión de Fourier de F_p tiene coeficientes $a(n) = 0$ para toda $n \leq 0$, entonces F_p es holomorfa en ∞ y $\tilde{F_p}(0) = 0$, es decir $F_p(\infty) = 0$. Por lo tanto F_p es una forma cuspidal de peso 12 ■

Corolario 2.2.5.1. *Se tiene que $F_p(w) = \tau(p)\Delta(w)$, donde $\tau(p)$ es la función Tau de Ramanujan.*

Demostración. Por el lema (2.2.5) tenemos que F_p es una forma cuspidal de peso 12 pero, por el teorema (1.3.5), tenemos que el espacio de las formas cuspidales de peso 12 es de dimensión 1 y por lo tanto F_p es un múltiplo escalar de la forma cuspidal de peso 12, Δ, es decir tenemos $F_p = c\Delta$. Por otro lado usando la expansión de F_p encontrada en el lema (2.2.5) :

$$F_p(w) = (2\pi)^{12}\left(p^{11}\sum_{n=1}^{\infty}\tau(n)e^{2\pi inpw} + \sum_{n=1}^{\infty}\tau(np)e^{2\pi inw}\right)$$

y comparándola con la expansión de $c\Delta$:

$$c\Delta(w) = c(2\pi)^{12}\sum_{n=1}^{\infty}\tau(n)e^{2\pi inw}$$

tenemos, fijándonos en el coeficiente de $q = e^{2\pi iw}$:

$$(2\pi)^{12}\tau(p)e^{2\pi iw} = (2\pi)^{12}c\tau(1)e^{2\pi iw} = (2\pi)^{12}ce^{2\pi iw} \tag{2.22}$$

pues $\tau(1) = 1$, de donde se sigue que $c = \tau(p)$ y por lo tanto $F_p(w) = \tau(p)\Delta(w)$. ■

Estamos ahora en posición de terminar la prueba de L. Mordell acerca de las conjeturas de Ramanujan sobre la multiplicatividad de la función $\tau(n)$ y sobre su formula de recurrencia. Además, agregaremos una cota sobre el orden de $|\tau(n)|$, la cual en realidad es un corolario de un resultado del capítulo anterior, sin embargo la colocaremos aquí para reunir los resultados principales sobre la función τ de Ramanujan.

Teorema 2.2.6. *Sea $\tau(n)$ el n-esimo coeficiente de la serie de Fourier*

$$\sum_{n=1}^{\infty}\tau(n)e^{2\pi inw} = (2\pi)^{-12}\Delta(w) = e^{2\pi iw}\prod_{m=1}^{\infty}(1-e^{2\pi inw})^{24} \tag{2.23}$$

o escrito con la sustitución de costumbre, $q = e^{2\pi iw}$

$$\sum_{n=1}^{\infty}\tau(n)q^n = (2\pi)^{-12}\Delta(w) = q\prod_{m=1}^{\infty}(1-q^m)^{24} \tag{2.24}$$

y sea p un primo (positivo):

(i) Se tiene la relación de recurrencia

$$\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1}) \quad \textit{para } n \geq 1 \tag{2.25}$$

(ii) Sean m, n enteros positivos con $(m,n) = 1$, entonces

$$\tau(m)\tau(n) = \tau(mn) \tag{2.26}$$

(iii) $\tau(p) = O(p^6)$

Demostración. Para la demostración usaremos la función F_p definida en (2.2.1) por la ecuación

$$F_p(w) = p^{11}\Delta(pw) + \frac{1}{p}\sum_{\lambda=0}^{p-1}\Delta\Big(\frac{w+\lambda}{p}\Big)$$

la cual por el lema (2.2.5) sabemos que es una forma cuspidal de peso 12 con la expansión

$$F_p(w) = (2\pi)^{12}\left(p^{11}\sum_{n=1}^{\infty}\tau(n)e^{2\pi inpw} + \sum_{n=1}^{\infty}\tau(np)e^{2\pi inw}\right) \tag{2.27}$$

Sabemos además por el corolario (2.2.5.1) que $F_p(w) = \tau(p)\Delta(w)$ y que la expansión de $\tau(p)\Delta(w)$ es

$$\tau(p)\Delta(w) = \tau(p)(2\pi)^{12}\sum_{n=1}^{\infty}\tau(n)e^{2\pi inw} \tag{2.28}$$

Haciendo la sustitución $q = e^{2\pi iw}$ las ecuaciones (2.27) y (2.28) se convierten en:

$$F_p(w) = (2\pi)^{12}\left(p^{11}\sum_{n=1}^{\infty}\tau(n)q^{np} + \sum_{n=1}^{\infty}\tau(np)q^{n}\right) \tag{2.29}$$

y

$$\tau(p)\Delta(w) = \tau(p)(2\pi)^{12}\sum_{n=1}^{\infty}\tau(n)q^{n} \tag{2.30}$$

respectivamente. Por lo tanto fijando n en las ecuaciones (2.29) y (2.30) los coeficientes de q^n deben ser iguales, en particular, haciendo $n = p^{k+1}$ con $k \geq 1$, los coeficientes de q^{p^k} en las ecuaciones (2.29) y (2.30) deben ser iguales. Observemos que $F_p(w)$ puede ser visto como la suma de dos series:

$$(2\pi)^{12}p^{11}\sum_{n=1}^{\infty}\tau(n)q^{np} \tag{2.31}$$

y

$$(2\pi)^{12}\sum_{n=1}^{\infty}\tau(np)q^{n} \tag{2.32}$$

En la serie de la ecuación (2.31), para que el exponente de q sea p^k se debe tener que $np = p^k$, es decir $n = p^{k-1}$ y por lo tanto el coeficiente de q^{p^k} en (2.31) es:

$$(2\pi)^{12}p^{11}\tau(p^{k-1}) \tag{2.33}$$

En la serie de la ecuación (2.32), para que el exponente de q sea p^k se debe tener $n = p^k$ y por lo tanto el coeficiente de q^{p^k} en (2.32) es:

$$(2\pi)^{12}\tau(p^k p) = (2\pi)^{12}\tau(p^{k+1}) \tag{2.34}$$

En la serie de la ecuación (2.30), para que el exponente de q sea p^k se debe tener $n = p^k$ y por lo tanto el coeficiente de q^{p^k} en (2.30) es:

$$\tau(p)(2\pi)^{12}\tau(p^k) \tag{2.35}$$

Igualando (2.33) más (2.34) a (2.35), tenemos:

$$(2\pi)^{12}p^{11}\tau(p^{k-1}) + (2\pi)^{12}\tau(p^{k+1}) = \tau(p)(2\pi)^{12}\tau(p^k) \tag{2.36}$$

lo cual implica la identidad

$$\tau(p^{k+1}) = \tau(p)\tau(p^k) - p^{11}\tau(p^{k-1}) \quad \text{para } k \geq 1 \tag{2.37}$$

y prueba (i). Ahora de manera análoga a la que probamos (i), daremos una identidad más general. Sea $s \geq 1$ tal que $(s, p) = 1$ y sea α un entero mayor o igual a 2. Busquemos el coeficiente de $q^{sp^{\alpha-1}}$ en las expansiones de $F_p(w)$ y $\tau(p)\Delta(w)$, que como sabemos, dichos coeficientes deben ser iguales. En la serie de la ecuación (2.31), para que el exponente de q sea $sp^{\alpha-1}$ se debe tener que $np = sp^{\alpha-1}$, es decir $n = sp^{\alpha-2}$ (aquí se ha usado el hecho de que $\alpha \geq 2$) y por lo tanto el coeficiente de $q^{sp^{\alpha-1}}$ en (2.31) es:

$$(2\pi)^{12}p^{11}\tau(sp^{\alpha-2}) \tag{2.38}$$

En la serie de la ecuación (2.32), para que el exponente de q sea $sp^{\alpha-1}$ se debe tener $n = sp^{\alpha-1}$ y por lo tanto el coeficiente de $q^{sp^{\alpha-1}}$ en (2.32) es:

$$(2\pi)^{12}\tau(sp^{\alpha-1}p) = (2\pi)^{12}\tau(sp^{\alpha}) \tag{2.39}$$

En la serie de la ecuación (2.30), para que el exponente de q sea $sp^{\alpha-1}$ se debe tener $n = sp^{\alpha-1}$ y por lo tanto el coeficiente de $q^{sp^{\alpha-1}}$ en (2.30) es:

$$\tau(p)(2\pi)^{12}\tau(sp^{\alpha-1}) \tag{2.40}$$

Igualando (2.38) más (2.39) a (2.40), tenemos:

$$(2\pi)^{12}p^{11}\tau(sp^{\alpha-2}) + (2\pi)^{12}\tau(sp^{\alpha}) = \tau(p)(2\pi)^{12}\tau(sp^{\alpha-1}) \tag{2.41}$$

lo cual implica

$$\tau(sp^{\alpha}) = \tau(p)\tau(sp^{\alpha-1}) - p^{11}\tau(sp^{\alpha-2}) \quad \text{con } (s,p) = 1 \text{ y } \alpha \geq 2 \tag{2.42}$$

Ahora sea β un entero mayor o igual a cero y si $(s, p) = 1$, hacemos

$$g(\beta) = \tau(p^{\beta}s) - \tau(p^{\beta})\tau(s) \tag{2.43}$$

dado que $\tau(1) = 1$ tenemos:

$$g(0) = \tau(p^0 s) - \tau(p^0)\tau(s) = \tau(s) - \tau(s) = 0 \tag{2.44}$$

Además, sea s primo relativo con p, el término q^s no aparece en la serie de la ecuación (2.31), pues en esta serie el exponente de q siempre es múltiplo de p. Por otro lado en la serie de la ecuación (2.32) el coeficiente de q^s es

$$(2\pi)^{12}\tau(ps)$$

y en la serie de la ecuación (2.30), el coeficiente de q^s es

$$(2\pi)^{12}\tau(p)\tau(s)$$

y estos coeficientes deben ser iguales, por lo tanto:

$$\tau(ps) = \tau(p)\tau(s)$$

de donde se sigue que:

$$g(1) = \tau(ps) - \tau(p)\tau(s) = 0 \tag{2.45}$$

Por otro lado tenemos:

$$\begin{aligned}\tau(p)g(\beta) - p^{11}g(\beta-1) \\ &= \tau(p)(\tau(p^\beta s) - \tau(p^\beta)\tau(s)) - p^{11}(\tau(p^{\beta-1}s) - \tau(p^{\beta-1})\tau(s)) \\ &= (\tau(p)\tau(p^\beta s) - p^{11}\tau(p^{\beta-1}s)) - \tau(s)(\tau(p)\tau(p^\beta) - p^{11}\tau(p^{\beta-1}))\end{aligned} \tag{2.46}$$

y usando las ecuaciones (2.37) y (2.42) la ecuación (2.46) es igual a

$$\tau(p)g(\beta) - p^{11}g(\beta-1) = \tau(p^{\beta+1}s) - \tau(s)\tau(p^{\beta+1}) = g(\beta+1) \tag{2.47}$$

Con esto es ahora fácil probar por inducción que $g(\beta) = 0$ para todo $\beta \geq 0$. Sabemos por (2.2) y (2.45) que $g(0) = g(1) = 0$, nuestra base de inducción será $\beta = 2$. Sabemos por (2.47) que:

$$g(2) = \tau(p)g(1) - p^{11}g(0) = 0 \tag{2.48}$$

Nuestra hipótesis de inducción será que $g(i) = 0$ para todo $0 \leq i \leq t$. Ahora tenemos por (2.47) y por la hipótesis de inducción que:

$$g(t+1) = \tau(p)g(t) - p^{11}g(t-1) = 0 \tag{2.49}$$

de donde concluimos que $g(\beta) = 0$ para todo $\beta \geq 0$, es decir que para todo primo p y todo entero positivo s con $(s,p) = 1$ se cumple

$$\tau(p^\beta s) = \tau(p^\beta)\tau(s) \tag{2.50}$$

en particular si p_1 y p_2 son dos primos distintos, entonces

$$\tau(p_1^{\alpha_1}p_2^{\alpha_2}) = \tau(p_1^{\alpha_1})\tau(p_2^{\alpha_2}) \tag{2.51}$$

lo cual implica que $\tau(n)$ es multiplicativa y termina la demostración de (ii). Finalmente observamos que (iii) es el teorema (1.4.5) aplicado a $(2\pi)^{-12}\Delta$ que es una forma cuspidal de peso 12. ■

Lema 2.2.7.

$$\tau(m)\tau(n) = \sum_{d|(m,n)} d^{11}\,\tau\left(\frac{mn}{d^2}\right) \tag{2.52}$$

Demostración. Consideraremos primero el caso en el que m y n son potencias de un mismo primo, es decir cuando $m = p^a$ y $n = p^b$ con p primo. Supongamos sin perdida de generalidad que $a \geq b$. Se tiene entonces que $(p^a, p^b) = p^b$ y por lo tanto

$$\sum_{d|p^b} d^{11}\,\tau\left(\frac{p^a p^b}{d^2}\right) = \sum_{i=0}^{b} p^{11i}\,\tau(p^{a+b-2i}) \tag{2.53}$$

Para demostrar el lema en este caso fijaremos a y haremos inducción en b. Si $b = 1$ entonces queremos demostrar

$$\tau(p)\tau(p^a) = \sum_{i=0}^{1} p^{11i}\,\tau(p^{a+1-2i}) \tag{2.54}$$

$$= p^0\,\tau(p^{a+1}) + p^{11}\,\tau(p^{a-1}) \tag{2.55}$$

pero esto es simplemente otra forma de la identidad (2.25) probada en el teorema (2.2.6). Esto constituye nuestra base de inducción. Supongamos que la identidad

$$\tau(p^a)\tau(p^j) = \sum_{i=0}^{j} p^{11i}\,\tau(p^{a+j-2i}) \tag{2.56}$$

es cierta para $j = 1, \ldots, b-1$, entonces, usando (2.25) tenemos:

$$\begin{aligned}
\tau(p^a)\tau(p^b) &= \tau(p^a)[\tau(p)\tau(p^{b-1}) - p^{11}\tau(p^{b-2})] \\
&= [\tau(p^a)\tau(p)]\tau(p^{b-1}) - p^{11}\tau(p^a)\tau(p^{b-2}) \\
&= [\tau(p^{a+1}) + p^{11}\tau(p^{a-1})]\tau(p^{b-1}) - p^{11}\tau(p^a)\tau(p^{b-2}) \\
&= \tau(p^{a+1})\tau(p^{b-1}) + p^{11}\tau(p^{a-1})\tau(p^{b-1}) - p^{11}\tau(p^a)\tau(p^{b-2}) \qquad (2.57)
\end{aligned}$$

Ahora, como la hipótesis de inducción funciona para toda $a \geq b$ y toda $1 \leq j \leq b-1$, entonces, aplicando la hipótesis de inducción a el último renglón de (2.57), tenemos:

$$\begin{aligned}
\tau(p^a)\tau(p^b) &= \sum_{i=0}^{b-1} p^{11i}\,\tau(p^{a+b-2i}) + p^{11}\sum_{i=0}^{b-1} p^{11i}\,\tau(p^{a+b-2i-2}) - p^{11}\sum_{i=0}^{b-2} p^{11i}\,\tau(p^{a+b-2i-2}) \\
&= \sum_{i=0}^{b-1} p^{11i}\,\tau(p^{a+b-2i}) + p^{11b}\tau(p^{a+b-2(b-1)-2}) \\
&= \sum_{i=0}^{b} p^{11i}\,\tau(p^{a+b-2i}) \qquad (2.58)
\end{aligned}$$

lo cual concluye la demostración para el caso en que m y n son ambos potencias del mismo primo.

Por otro lado, sean $m = p_1^{\alpha_1} \cdot \ldots p_k^{\alpha_k}$ y $n = p_1^{\beta_1} \cdot \ldots p_k^{\beta_k}$ donde $\alpha_i, \beta_i \geq 0$, y definimos $c_i = \max\{\alpha_i, \beta_i\}$, entonces $l = (n, m) = p_1^{c_1} \cdot \ldots p_k^{c_k}$ y los divisores de l son de la forma $p_1^{\gamma_1} \cdot \ldots p_k^{\gamma_k}$ con $0 \leq \gamma_i \leq c_i$ y por lo tanto:

$$\begin{aligned}
\sum_{d|(m,n)} d^{11}\,\tau\left(\frac{mn}{d^2}\right) &= \sum_{i_1=0}^{c_1} \cdots \sum_{i_k=0}^{c_k} p_1^{11i_1} \ldots p_k^{11i_k}\tau(p_1^{\alpha_1+\beta_1-2i_1} \ldots p_k^{\alpha_k+\beta_k-2i_k}) \\
&= \sum_{i_1=0}^{c_1} \cdots \sum_{i_k=0}^{c_k} p_1^{11i_1} \ldots p_k^{11i_k}\tau(p_1^{\alpha_1+\beta_1-2i_1}) \ldots (p_k^{\alpha_k+\beta_k-2i_k}) \\
&= \prod_{j=1}^{k} \sum_{i_j}^{c_j} p_j^{11i_j}\tau(p_j^{\alpha_j+\beta_j-2i_j}) \\
&= \prod_{j=1}^{k} \tau(p_j^{\alpha_j})\tau(p_j^{\beta_j}) \\
&= \tau(p_1^{\alpha_1} \ldots p_k^{\alpha_k})\tau(p_1^{\beta_1} \ldots p_k^{\beta_k}) \\
&= \tau(m)\tau(n) \qquad (2.59)
\end{aligned}$$

■

2.3. Relación entre $\tau(n)$ y los coeficientes de j

Con la teoría que hemos desarrollado sobre el espacio de las formas modulares de peso $2k$, M_k, hemos obtenido algunas identidades como en la sección 1.4, las cuales recapitulamos a continuación.

Recordemos que según el corolario (1.4.3.1) se tiene la igualdad

$$G_k(z) = 2\zeta(2k)E_k(z)$$

con

$$E_k(z) = 1 + \gamma_k \sum_{n=1}^{\infty} \sigma_{2k-1}(n)q^n \tag{2.60}$$

y

$$\gamma_k = (-1)^k \frac{4k}{B_k} \tag{2.61}$$

Notemos que E_k es una forma modular de peso $2k$ tal que $E_k(\infty) = 1$[1] para todo $k > 2$. Lo anterior es cierto ya que $E_k(z)$ es un múltiplo escalar de la forma

[1]Algunos autores se refieren a E_k como la serie de Eisenstein normalizada de peso $2k$.

modular de peso $2k$, G_k y por lo tanto E_k es una forma modular de peso $2k$ además, la ecuación (2.60) nos da su expansión en infinito, la cual claramente tiene término $a_0 = 1$, es decir $E_k(\infty) = 1$.
Recordamos que las dimensiones de M_4 y M_5 son ambas 1, y por lo tanto las formas modulares de pesos 8 y 10 que valen 1 en infinito son únicas. Se debe tener entonces

$$E_2\,E_2 = E_4 \tag{2.62}$$
$$E_2\,E_3 = E_5 \tag{2.63}$$

Usando las identidades (2.60), (2.61) y los valores $B_2 = \frac{1}{30}$, $B_3 = \frac{1}{42}$ $B_4 = \frac{1}{30}$, $B_5 = \frac{5}{66}$, tenemos:

$$E_2 = 1 + \gamma_2 \sum_{n=1}^{\infty} \sigma_3(n) q^n = 1 + (-1)^2 \frac{8}{B_2} \sum_{n=1}^{\infty} \sigma_3(n) q^n = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n \tag{2.64}$$

$$E_3 = 1 + \gamma_3 \sum_{n=1}^{\infty} \sigma_5(n) q^n = 1 + (-1)^3 \frac{12}{B_3} \sum_{n=1}^{\infty} \sigma_5(n) q^n = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n \tag{2.65}$$

$$E_4 = 1 + \gamma_4 \sum_{n=1}^{\infty} \sigma_7(n) q^n = 1 + (-1)^4 \frac{16}{B_4} \sum_{n=1}^{\infty} \sigma_7(n) q^n = 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n) q^n \tag{2.66}$$

$$E_5 = 1 + \gamma_5 \sum_{n=1}^{\infty} \sigma_9(n) q^n = 1 + (-1)^5 \frac{20}{B_5} \sum_{n=1}^{\infty} \sigma_9(n) q^n = 1 - 264 \sum_{n=1}^{\infty} \sigma_5(n) q^n \tag{2.67}$$

y substituyendo estos valores en (2.62) y (2.63) y fijándonos en el coeficiente de q^n de ambos lados, tenemos:

$$\sigma_7(n) = \sigma_3 + 120 \sum_{m=1}^{n-1} \sigma_3(m)\,\sigma_3(n-m) \tag{2.68}$$

$$11\sigma_9(n) = 21\sigma_5 - 10\sigma_3 + 5040 \sum_{m=1}^{n-1} \sigma_3(m)\,\sigma_5(n-m) \tag{2.69}$$

Aplicando ahora el corolario (1.4.3.1) con $k = 6$, es decir las identidades (2.60) y (2.61) con $k = 6$ y usando el hecho de que $B_6 = \frac{691}{2730}$ Tenemos

$$E_6 = 1 + 24\frac{2730}{691} \sum_{n=1}^{\infty} \sigma_{11}(n) q^n = 1 + \frac{65520}{691} \sum_{n=1}^{\infty} \sigma_{11}(n) q^n \tag{2.70}$$

Recordemos ahora que se ha definido el invariante modular j como

$$j = 12^3\, g_2^3/\Delta \tag{2.71}$$

y que según las proposiciones (1.3.1) y (1.3.2), j es una función modular de peso 0 que es holomorfa en H y tiene un polo simple en ∞. Además por el corolario (1.4.3.3) tenemos

$$j(z) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c_n q^n \tag{2.72}$$

Recordemos también que

$$(2\pi)^{-12}\Delta(z) = \sum_{n=1}^{\infty} \tau(n) q^n \tag{2.73}$$

donde $\tau(n)$ es la función Tau de Ramanujan.

Lema 2.3.1. *Se tiene*

$$E_3^2(z) = (j(z) - 12^3)(2\pi)^{-12}\Delta(z) \tag{2.74}$$

Demostración. Usando (2.71) y el hecho de que $\Delta = g_2^3 - 27g_3^2$ tenemos:

$$\begin{aligned}
(j(z) - 12^3)\frac{\Delta(z)}{(2\pi)^{12}} &= \\
&= \frac{12^3}{(2\pi)^{12}}\left(\frac{g_2^3(z)}{\Delta(z)} - 1\right)\Delta(z) = \frac{12^3}{(2\pi)^{12}}(g_2^3(z) - \Delta(z)) \\
&= \frac{12^3}{(2\pi)^{12}}\,(g_2^3(z) - (g_2^3 - 27g_3^2)) = \frac{12^3}{(2\pi)^{12}}\,27g_3^2 \\
&= \frac{2^6 \cdot 3^6}{(2\pi)^{12}} \cdot g_3^2
\end{aligned} \tag{2.75}$$

Por otro lado como g_3 se define como $140\,G_3$ y el corolario (1.4.3.1) nos dice que $G_3(z) = 2\zeta(6)E_k(z)$ entonces, usando el valor conocido $\zeta(6) = \frac{\pi^6}{3^3\cdot 5\cdot 7}$, tenemos

$$g_3 = 140G_3 = 140(2\zeta(6)E_3(z)) = \frac{140 \cdot 2 \cdot \pi^6}{3^3 \cdot 5 \cdot 7}E_3(z) = \frac{(2\pi)^6}{2^3 \cdot 3^3}E_3(z) \tag{2.76}$$

por lo tanto

$$g_2^3 = \frac{(2\pi)^{12}}{2^6 \cdot 3^6}E_3^2 \tag{2.77}$$

y al usar la identidad (2.77) en la ecuación (2.75) tenemos

$$\begin{aligned}
(j(z) - 12^3)\frac{\Delta(z)}{(2\pi)^{12}} &= \frac{2^6 \cdot 3^6}{(2\pi)^{12}} \cdot g_3^2 \\
&= \frac{2^6 \cdot 3^6}{(2\pi)^{12}}\frac{(2\pi)^{12}}{2^6 \cdot 3^6}E_3^2 \\
&= E_3^2
\end{aligned}$$

■

Corolario 2.3.1.1. *Para todo $n \geq 0$ se tiene la identidad*

$$(504)^2 \sum_{k=0}^{n} \sigma_5(k)\sigma_5(n-k) = \tau(n+1) - 984\tau(n) + \sum_{k=1}^{n-1} c(k)\tau(n-k) \qquad (2.78)$$

donde $c(n)$ es el n-esimo coeficiente de la expansión de j dada por la ecuación (2.72), $\tau(n)$ es la función Tau de Ramanujan y se consideran $\sigma_5(0) = -1/504$, $\tau(0) = 0$ y la suma

$$\sum_{k=1}^{n-1} c(k)\tau(n-k)$$

es igual a 0 para $n = 0$ y $n = 1$.

Demostración. El lema (2.3.1) nos da la identidad

$$E_3^2(z) = (j(z) - 12^3)(2\pi)^{-12}\Delta(z) \qquad (2.79)$$

Ahora utilizando las expansiones dadas por las ecuaciones (2.65), (2.72) y (2.73) de E_3, j y $(2\pi)^{-12}\Delta$, respectivamente, y haciendo $\sigma_5(0) = -1/504$, y sustituyendo en (2.79), tenemos

$$\begin{aligned}\Big(504 \sum_{n=0}^{\infty} \sigma_5(n)q^n\Big)^2 &= \Big(-504 \sum_{n=0}^{\infty} \sigma_5(n)q^n\Big)^2 \\ &= \left(\frac{1}{q} + 744 + \sum_{n=1}^{\infty} c(n)q^n - 12^3\right)\left(\sum_{n=1}^{\infty} \tau(n)q^n\right) \\ &= \left(\frac{1}{q} - 984 + \sum_{n=1}^{\infty} c(n)q^n\right)\left(\sum_{n=1}^{\infty} \tau(n)q^n\right) \qquad (2.80)\end{aligned}$$

fijándonos en el coeficiente de q^n tenemos que el coeficiente de q^n en el lado izquierdo de (2.80) está dado por

$$(504)^2 \sum_{k=0}^{n} \sigma_5(k)\sigma_5(n-k) \qquad (2.81)$$

mientras que el coeficiente de q^n en el lado derecho de (2.80) está dado por la suma

$$\tau(n+1) - 984\tau(n) + \sum_{k=1}^{n-1} c(k)\tau(n-k) \qquad (2.82)$$

si $n \geq 2$. Los coeficientes de q^0 y q^1 en el lado derecho de (2.80) son 1 y $\tau(2) - 984\tau(1)$, respectivamente, por lo que con las precisiones hechas en el enunciado del corolario, juntando (2.81) y (2.82), tenemos el resultado. ■

Lema 2.3.2.
$$E_6 - \frac{65520}{691} \cdot \frac{\Delta}{(2\pi)^{12}} = E_3^2 + 1008 \cdot \frac{\Delta}{(2\pi)^{12}} \tag{2.83}$$

Demostración. Como E_3 es una forma modular de peso 6, entonces E_3^2 es una forma modular de peso 12, más aún dado que la expansión de E_3 como serie alrededor de $q = 0$ tiene coeficiente $a_0 = 1$ se tiene que la expansión de E_3^2 alrededor de $q = 0$ tiene también coeficiente $a_0' = 1$. Dicho de otra manera, dado que $E_3(\infty) = 1$, entonces $E_3^2(\infty) = 1$. Como E_6 es una forma modular de peso 12 con $E_6(\infty) = 1$ (es decir con coeficiente $b_0 = 1$ en su expansión alrededor de $q = 0$), se tiene que $E_6 - E_3^2$ es una forma modular cuspidal de peso 12 pero, sabemos por el teorema 1.3.5 que M_6^0, el espacio de las formas cuspidales de peso 12, tiene dimensión 1 y por lo tanto $E_6 - E_3^2$ debe ser un múltiplo escalar de la forma cuspidal de peso 12, $(2\pi)^{-12}\Delta$, es decir, tenemos

$$E_6 - E_3^2 = c \cdot \frac{\Delta}{(2\pi)^{12}} \tag{2.84}$$

Observemos los coeficientes de q en las series

$$E_6 = 1 + \frac{65520}{691} \sum_{n=1}^{\infty} \sigma_{11}(n) q^n \tag{2.85}$$

$$E_3^2 = \left(1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n\right)^2 = 1 - 1008 \sum_{n=1}^{\infty} \sigma_5(n) q^n + \left(\sum_{n=1}^{\infty} \sigma_5(n) q^n\right)^2 \tag{2.86}$$

$$\frac{\Delta}{(2\pi)^{12}} = \sum_{n=1}^{\infty} \tau(n) q^n \tag{2.87}$$

son

$$\frac{65520}{691}\sigma_{11}(1) = \frac{65520}{691} \tag{2.88}$$

$$1008\sigma_5(1) = -1008 \tag{2.89}$$

$$\tau(1) = 1 \tag{2.90}$$

en (2.85), (2.86) y (2.87), respectivamente. Tenemos entonces por las ecuaciones anterior que el coeficiente de q en el lado izquierdo de (2.84) es

$$\frac{65520}{691} + 1008 \tag{2.91}$$

mientras que el coeficiente de q en el lado derecho de (2.84) es simplemente c, de donde obtenemos

$$c = \frac{65520}{691} + 1008$$

y sustituyendo en (2.84), tenemos

$$E_6 - E_3^2 = \left(\frac{65520}{691} + 1008\right) \frac{\Delta}{(2\pi)^{12}}$$

que reordenando nos da la identidad

$$E_6 - \frac{65520}{691} \cdot \frac{\Delta}{(2\pi)^{12}} = E_3^2 + 1008 \cdot \frac{\Delta}{(2\pi)^{12}}$$

■

Con lo anterior podemos probar el siguiente teorema.

Teorema 2.3.3. *Para todo $n \geq 1$ se tiene*

$$\frac{65520}{691}(\sigma_{11}(n) - \tau(n)) = \tau(n+1) + 24\tau(n) + \sum_{k=1}^{n-1} c(k)\tau(n-k) \tag{2.92}$$

donde los $c(i)'s$ son los coeficientes de la expansión en infinito (alrededor de $q = 0$) del invariante modular j y $\tau(n)$ representa la función Tau de Ramanujan evaluada en n y, donde la suma

$$\sum_{k=1}^{n-1} c(k)\tau(n-k)$$

se considera igual a 0 si $n = 1$.

Demostración. Usando las expansiones

$$E_6 = 1 + \frac{65520}{691} \sum_{n=1}^{\infty} \sigma_{11}(n) q^n \tag{2.93}$$

$$\frac{\Delta}{(2\pi)^{12}} = \sum_{n=1}^{\infty} \tau(n) q^n \tag{2.94}$$

tenemos que el coeficiente de q^n para $n \geq 1$ de

$$E_6 - \frac{65520}{691} \cdot \frac{\Delta}{(2\pi)^{12}} \tag{2.95}$$

es

$$\frac{65520}{691}(\sigma_{11}(n) - \tau(n)) \tag{2.96}$$

Por otro lado, dado que en la prueba de la identidad

$$(504)^2 \sum_{k=0}^{n} \sigma_5(k)\sigma_5(n-k) = \tau(n+1) - 984\tau(n) + \sum_{k=1}^{n-1} c(k)\tau(n-k) \tag{2.97}$$

(ecuación (2.78)) del corolario 2.3.1.1 se ha usado que el lado izquierdo de dicha identidad es el coeficiente de q^n en la expansión en infinito de E_3^2 para todo $n \geq 1$ si convenimos que la suma

$$\sum_{k=1}^{n-1} c(k)\tau(n-k)$$

es igual a 0 si $n = 1$, se tiene que el coeficiente de q^n en la expansión en infinito de

$$E_3^2 + 1008 \cdot \frac{\Delta}{(2\pi)^{12}} \tag{2.98}$$

es igual a

$$(\tau(n+1) - 984\tau(n) + \sum_{k=1}^{n-1} c(k)\tau(n-k)) + 1008\tau(n)$$

es decir

$$\tau(n+1) + 24\tau(n) + \sum_{k=1}^{n-1} c(k)\tau(n-k) \tag{2.99}$$

Finalmente usando la identidad

$$E_6 - \frac{65520}{691} \cdot \frac{\Delta}{(2\pi)^{12}} = E_3^2 + 1008 \cdot \frac{\Delta}{(2\pi)^{12}}$$

es decir el lema 2.3.2 tenemos, al igualar los coeficientes de q^n de

$$E_6 - \frac{65520}{691} \cdot \frac{\Delta}{(2\pi)^{12}}$$

y

$$E_3^2 + 1008 \cdot \frac{\Delta}{(2\pi)^{12}}$$

encontrados en (2.96) y (2.99), respectivamente, tenemos

$$\frac{65520}{691}(\sigma_{11}(n) - \tau(n)) = \tau(n+1) + 24\tau(n) + \sum_{k=1}^{n-1} c(k)\tau(n-k)$$

■

Corolario 2.3.3.1. *Para todo $n \geq 1$ se tiene*

$$\sigma_{11}(n) \equiv \tau(n) \pmod{691} \tag{2.100}$$

Demostración. Dado que en la ecuación

$$\frac{65520}{691}(\sigma_{11}(n) - \tau(n)) = \tau(n+1) + 24\tau(n) + \sum_{k=1}^{n-1} c(k)\tau(n-k)$$

(ecuación (2.92)) del teorema 2.3.3 el lado derecho es un entero pues $c(n)$ y $\tau(n)$ son enteros para toda $n \geq 1$, entonces se debe tener que el lado izquierdo de dicha identidad debe ser también un entero y como $(65520, 691) = 1$ se debe tener $691 | \sigma_{11}(n) - \tau(n)$ de donde se sigue el resultado. ■

Vale la pena observar que el teorema (2.3.3) nos proporciona una formula de recurrencia para obtener los coeficientes $c(n)$ en términos de σ_{11} y τ.

2.4. Resultados sobre la recurrencia de la función τ

Pongamos ahora nuestra atención en la recurrencia lineal de grado 2 de la ecuación (2.25) del teorema 2.2.6:

$$\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1}) \quad \text{para } n \geq 1 \tag{2.101}$$

donde p es un primo.
Las recursiones lineales de grado 2 con coeficientes enteros han sido bien estudiadas[2], sin embargo daremos a continuación pruebas particulares sobre algunas propiedades aritméticas de los términos de la forma $\tau(p^n)$ donde p es un primo. Comencemos con el siguiente resultado.

Lema 2.4.1. *Si $p|\tau(p^r)$ para algún entero $r \geq 1$, entonces $p|\tau(p^n)$ para toda $n \geq 1$.*

Demostración. Usaremos argumentos inductivos y la formula de recurrencia

$$\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1}) \quad \text{para } n \geq 1$$

Veamos primero que si $p|\tau(p)$, entonces $p|\tau(p^n)$ para toda $n \geq 1$. Supongamos entonces que $p|\tau(p)$ y que $p|\tau(p^i)$ para todo $1 \leq i \leq k$. Usando la formula de recursión para calcular $\tau(p^{k+1})$ tenemos

$$\tau(p^{k+1}) = \tau(p)\tau(p^k) - p^{11}\tau(p^{k-1})$$

y como estamos suponiendo que $p|\tau(p^k)$, entonces p divide al lado derecho de la igualdad, de donde se sigue que p divide también a $\tau(p^{k+1})$. Por inducción $p|\tau(p^n)$ para toda $n \geq 1$. De manera similar si $p|\tau(p^n)$ para algún $n > 1$, entonces, usando la identidad

$$\tau(p^n) = \tau(p)\tau(p^{n-1}) - p^{11}\tau(p^{n-2})$$

se tiene que $p|\tau(p)$ o $p|\tau(p^{n-1})$. Si $p|\tau(p)$ estamos en el caso anterior, si no, entonces $p|\tau(p^{n-1})$ y podemos iterar el proceso. En cualquier caso, como el exponente en la expresión $p|\tau(p^n)$ disminuye de 1 en 1, llegaremos a $p|\tau(p)$ y en ese caso ya vimos que $p|\tau(p^n)$ para toda $n \geq 1$. ■

Corolario 2.4.1.1. *Si p no divide a $\tau(p)$, entonces p no divide a $\tau(p^n)$ para ningún $n \geq 1$.*

Demostración. El corolario se sigue directamente del lema 2.4.1, pues si $p|\tau(p^n)$ para algún $n \geq 1$, entonces p dividiría a $\tau(p)$. ■

---
[2] Ver por ejemplo [12]

Lema 2.4.2. *Si a y b son enteros con $a \geq b \geq 0$, se tiene*

$$\tau(p^{a+b-1}) = \tau(p^{a-1})\tau(p^b) - p^{11}\tau(p^{a-2})\tau(p^{b-1}) \tag{2.102}$$

donde $\tau(n) = 0$ si $n < 0$.

Demostración. Primero observemos que la identidad se cumple trivialmente si $b = 0$ o $a = b = 1$. Por lo anterior, podemos suponer que $a \geq 2$ y $b \geq 1$. Primero supongamos que $a > b$ (que implica $b \leq a-1$ y $b-1 \leq a-2$), usando el lema 2.2.7 con $m = p^{a-1}$ y $n = p^b$, tenemos

$$\tau(p^{a-1})\tau(p^b) = \sum_{d|p^b} d^{11}\,\tau\left(\frac{p^{a-1}p^b}{d^2}\right) = \sum_{i=0}^{b} p^{11i}\,\tau(p^{a+b-1-2i}) \tag{2.103}$$

y usando el lema 2.2.7 con $m = p^{a-2}$ y $n = p^{b-1}$, tenemos

$$\begin{aligned} p^{11}\tau(p^{a-2})\tau(p^{b-1}) &= \\ &= p^{11}\sum_{d|p^{b-1}} d^{11}\,\tau\left(\frac{p^{a-2}p^{b-1}}{d^2}\right) \\ &= p^{11}\sum_{j=0}^{b-1} p^{11j}\,\tau(p^{a+b-1-2(j+1)}) \\ &= \sum_{j=0}^{b-1} p^{11(j+1)}\,\tau(p^{a+b-1-2(j+1)}) \\ &= \sum_{i=1}^{b} p^{11i}\,\tau(p^{a+b-1-2i}) \end{aligned} \tag{2.104}$$

por lo que juntando las ecuaciones (2.103) y (2.104) tenemos

$$\begin{aligned} \tau(p^{a-1})\tau(p^b) - p^{11}\tau(p^{a-2})\tau(p^{b-1}) &= \\ &= \sum_{i=0}^{b} p^{11i}\,\tau(p^{a+b-1-2i}) - \sum_{i=1}^{b} p^{11i}\,\tau(p^{a+b-1-2i}) \\ &= p^{11\cdot 0}\tau(p^{a+b-1-2\cdot 0}) = \tau(p^{a+b-1}) \end{aligned} \tag{2.105}$$

Si ahora sucede que $a = b$ la prueba es análoga, solamente cambiará el indice superior en las sumas pues en este caso $a-1 < b$ y $a-2 < b-1$. Tenemos entonces

$$\tau(p^{a-1})\tau(p^a) = \sum_{d|p^{a-1}} d^{11}\,\tau\left(\frac{p^{a-1}p^a}{d^2}\right) = \sum_{i=0}^{a-1} p^{11i}\,\tau(p^{2a-1-2i}) \tag{2.106}$$

y

$$
\begin{aligned}
p^{11}\tau(p^{a-2})\tau(p^{a-1}) = \\
&= p^{11}\sum_{d|p^{a-2}} d^{11}\,\tau\left(\frac{p^{a-2}p^{a-1}}{d^2}\right)\\
&= p^{11}\sum_{j=0}^{a-2} p^{11j}\,\tau(p^{2a-1-2(j+1)})\\
&= \sum_{j=0}^{a-2} p^{11(j+1)}\,\tau(p^{2a-1-2(j+1)})\\
&= \sum_{i=1}^{a-1} p^{11i}\,\tau(p^{2a-1-2i}) \qquad (2.107)
\end{aligned}
$$

y juntando las ecuaciones (2.106) y (2.107), tenemos

$$
\begin{aligned}
\tau(p^{a-1})\tau(p^{a}) - p^{11}\tau(p^{a-2})\tau(p^{a-1}) = \\
&= \sum_{i=0}^{a-1} p^{11i}\,\tau(p^{2a-1-2i}) - \sum_{i=1}^{a-1} p^{11i}\,\tau(p^{2a-1-2i})\\
&= p^{11\cdot 0}\tau(p^{2a-1-2\cdot 0}) = \tau(p^{2a-1}) \qquad (2.108)
\end{aligned}
$$

lo que concluye la demostración. ■

Hagamos ahora algunos cambios en la notación con el fin de simplificarla.

Definición 2.4.1. *Sea p un primo fijo. Definimos la sucesión P_k como*

$$
P_k = \begin{cases} 0 & si\ k=0 \\ \tau(1)=1 & si\ k=1 \\ \tau(p^{k-1}) & si\ k>1 \end{cases} \qquad (2.109)
$$

Con esta notación la recurrencia

$$
\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1}) \quad \text{para } n \geq 1
$$

se convierte en

$$
P_{n+2} = P_2P_{n+1} - p^{11}P_n \quad \text{para } n \geq 0 \qquad (2.110)
$$

Con esta notación el lema (2.4.1) nos dice que si $p|P_r$ para algún $r \geq 2$, entonces p divide a P_n para todo $n \geq 2$ y el corolario 2.4.1.1 nos dice que si p no divide a $P_2 = \tau(p)$, entonces $(p, P_n) = 1$ para toda $n \geq 2$.

Definición 2.4.2. *Decimos que un primo p es ordinario si $p \nmid \tau(p) = P_2$ y decimos que p es no-ordinario si sucede lo contrario.*

Con esto tenemos que si un primo p es ordinario entonces $p \nmid P_n$ excepto para $n = 0$.

Lema 2.4.3. *Si p es un primo ordinario, entonces $(P_{n+1}, P_n) = 1$ para toda $n \geq 1$*

Demostración. Haremos la prueba por inducción. Para $n = 1$ tenemos $P_1 = 1$ y por lo tanto $(P_2, P_1) = 1$. Ahora supongamos que $(P_n, P_{n-1}) = 1$. Usando la recursión (2.110), tenemos

$$P_{n+1} = P_2 P_n - p^{11} P_{n-1}$$

entonces $d = (P_{n+1}, P_n)$ divide a $p^{11} P_{n-1}$ pero, como p es ordinario $(d, p) = 1$ y entonces $d | P_{n-1}$ y entonces p es un divisor común de P_n y P_{n-1} y por la hipótesis de inducción, se tiene que $d = 1$ ■

Podemos ahora probar el siguiente lema

Lema 2.4.4. *Sean n y m enteros no negativos y p un primo ordinario, se tiene entonces*

$$(P_m, P_n) = P_{(m,m)} \tag{2.111}$$

Demostración. Si alguno de m o n son cero, el resultado se sigue trivialmente ya que $P_0 = 0$. Ahora veamos por inducción el caso $n = mk$. En este caso como $(mk, m) = m$ se debe tener que $P_m | P_{mk}$ para todo $k \geq 0$. Si $k = 0$ y $k = 1$ el resultado es cierto pues es simplemente $P_m | 0$ o $P_m | P_m$, respectivamente. Supongamos ahora que para toda $0 \leq j \leq k$ se tiene $P_m | P_{mj}$. Usando el lema 2.4.2 con $a = mk$ y $b = m$ y usando el hecho de que $P_s = \tau(p^{s-1})$ si $n \geq 1$, tenemos

$$P_{m(k+1)} = P_{mk+m} = P_{mk} P_{m+1} - p^{11} P_{mk-1} P_m \tag{2.112}$$

y como por hipótesis $P_m | P_{mk}$, entonces el lado derecho de (2.112) divisible por P_m y por lo tanto también debe serlo el lado izquierdo, es decir $P_m | P_{m(k+1)}$.

Supongamos ahora sin perdida de generalidad que $m < n$. Sea $n = mk + r$, como ya resolvimos el caso en el que $m|n$, podemos suponer que $0 < r < m$. Se tiene que con la notación $P_s = \tau(p^{s-1})$, el lema 2.4.2 con $a = mk$ y $b = r$ se convierte en

$$P_n = P_{mk+r} = P_{mk} P_{r+1} - p^{11} P_{mk-1} P_r \tag{2.113}$$

como $P_m | P_{mk}$ por lo visto al principio de la prueba, $(P_m, p) = 1$ porque p es ordinario y $(P_m, P_{mk-1}) = 1$ por el lema 2.4.3, se tiene que $(P_m, P_{mk+r}) = (P_m, P_r)$. Podemos repetir el proceso con r y m pero, esto es justamente el algoritmo de la división de Euclides por lo que llegaremos a $(P_m, P_{mk+r}) = (P_d, 0) = P_d$ donde $d = (m, n)$. ■

2.4.1. La conjetura de Lehmer

Hemos estudiado algunas propiedades aritméticas de la función $\tau(n)$ y para ello hemos dividido a los primos en ordinarios, si $p \nmid \tau(p)$ y no-ordinarios de lo contrario. Si sucediera que $\tau(p) = 0$ para algún primo p, entonces $p \mid \tau(p) = 0$, por lo que p tendría que ser no-ordinario. En el artículo [6] se menciona que hasta ese momento (noviembre de 2013) los únicos primos no-ordinarios conocidos eran 2, 3, 5, 7, 2411, 7758337633. En el momento de escribir este trabajo esos siguen siendo los únicos primos no-ordinarios conocidos.

Lehmer conjeturo en 1947 que $\tau(n) \neq 0$ para todo entero positivo n. Hasta el momento la conjetura permanece abierta y el mayor n conocido tal que $\tau(m) \neq 0$ si $1 \leq m < n$ es

$$n = 816212624008487344127999 \approx 8 \cdot 10^{23}$$

dicha cota fue demostrada por Derickx, van Hoeij, y Zeng en 2013 en [7].
Dado que $\tau(n)$ es una función multiplicativa, es fácil ver que si $\tau(m) = 0$ para algún entero positivo m, entonces $\tau(p^r) = 0$ para un primo p tal que $m = p^r s$ con $(p, s) = 1$. Esta observación y el siguiente lema probarán que si $\tau(m) = 0$ para algún entero positivo m, entonces $\tau(p) = 0$, donde p es un primo que divide a m. Sin embargo para demostrar el lema siguiente utilizaremos un resultado fuerte conjeturado por Ramanujan y probado por Deligne en 1974 como consecuencia de su demostración de las conjeturas de Weil en [4]. El resultado, aplicado al caso particular de la función Tau de Ramanujan nos dice

$$|\tau(p)| \leq 2p^{11/2} \quad \text{para todo primo } p. \tag{2.114}$$

La siguiente tabla muestra los primeros valores de $\tau(n)$[3]

n	$\tau(n)$
1	1
2	-24
3	252
4	-1472
5	4830
6	-6048
7	-16744
8	84480
9	-113643
10	-115920
11	534612

Cuadro 2.1: Primeros valores de la función Tau de Ramanujan

[3] Esta tabla fue extraída de [13, p. 97]

Lema 2.4.5. *Si $\tau(p) \neq 0$ para algún primo p y $p^s \parallel \tau(p)$, es decir $p^s \mid \tau(p)$ pero $p^{s+1} \nmid \tau(p)$, entonces $p^{sk} \parallel \tau(p^k)$.*

Demostración. Del Cuadro 3.1 podemos observar que la máxima potencia de 2 que divide a $\tau(2) = -24$ es 2^3 y la máxima potencia de 3 que divide a $\tau(3) = 252$ es 3^2. Además si $p \geq 5$, se sigue de (2.114) que

$$|\tau(p)|^2 \leq 4p^{11} < p^{12}$$

y como $|\tau(p)|^2$ es un cuadrado, entonces, si $\tau(p) \neq 0$, la máxima potencia de p que divide a $|\tau(p)|^2$ debe ser de la forma p^{2s} y por lo tanto $2s < 12$ es decir $0 \leq s \leq 5$. Tenemos entonces que para todo primo p tal que $\tau(p) \neq 0$ se tiene que si $p^s \parallel \tau(p)$, entonces $0 \leq s \leq 5$ pues cuando $p = 2$ o $p = 3$ los valores explícitos nos dan el resultado. Concluiremos ahora la prueba con inducción. Supongamos que $\tau(p) \neq 0$ y $p^s \parallel \tau(p)$, en este caso esta sería nuestra base de inducción. Nuestra hipótesis de inducción es que para todo $1 \leq j \leq k$ se tiene que $p^{sj} \parallel \tau(p^j)$. Ahora, usando la identidad de recursión (2.101) con $n = k$, tenemos

$$\tau(p^{k+1}) = \tau(p)\tau(p^k) - p^{11}\tau(p^{k-1})$$

y usando la hipótesis de inducción tenemos

$$\begin{aligned} p^{s+sk} &\parallel \tau(p)\tau(p^k) \\ p^{11+s(k-1)} &\parallel -p^{11}\tau(p^{k-1}) \end{aligned}$$

y como $s \leq 5$, entonces $2s \leq 10 < 11$ y por lo tanto

$$p^{s(k+1)} \parallel \tau(p)\tau(p^k) - p^{11}\tau(p^{k-1}) = \tau(p^{k+1})$$

■

Con lo anterior, y como ya habíamos mencionado tenemos la siguiente proposición.

Proposición 2.4.1. *si $\tau(m) = 0$ para algún entero positivo m, entonces $\tau(p) = 0$, donde p es un primo que divide a m*

Demostración. Como $\tau(m)$ es multiplicativa se debe tener que $\tau(p^s) = 0$ para un primo p tal que $m = p^s k$ con $(p, k) = 1$. Por le lema anterior si $\tau(p) \neq 0$, entonces existe un entero α tal que $p^{\alpha s} \parallel \tau(p^s)$, en particular $p^{\alpha s+1} \nmid \tau(p^s) = 0$ lo cual es una contradicción. Por lo tanto si $\tau(p^s) = 0$, entonces $\tau(p) = 0$. ■

A. Productos Infinitos

Este apéndice es incluido con los objetivos de dar una definición formal de producto infinito (en $\mathbb{C}$ o en $\mathbb{R}$), así como dar algunos criterios simples de convergencia para un producto infinito de números complejos, los cuales son utilizados en esta tesis para demostrar la convergencia de algunos productos infinitos, siendo el más importante de este trabajo la convergencia de

$$\frac{\Delta}{(2\pi)^{12}} = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n$$

es decir del producto infinito que determina a la función Tau de Ramanujan.

Definición 2.4.3. *Si $\{z_n\}$ es una sucesión de números complejos y si*

$$z = \lim_{n\to\infty}\prod_{k=1}^{n} z_k$$

existe, entonces z es el producto infinito de números z_n y se denota por

$$z = \prod_{n=1}^{\infty} z_n$$

.

Supongamos que ninguno de los números z_n es cero, que $z = \prod_{n=1}^{\infty} z_n$ existe y que además no es cero. Sea $p_n = \prod_{k=1}^{n} z_k$ para $n \geq 1$; entonces ningún p_n es cero y $\dfrac{p_n}{p_{n-1}} = z_n$. Como $z \neq 0$ y $p_n \to z$, tenemos que $\lim\limits_{n\to\infty} z_n = 1$. Por lo tanto, excepto para los casos donde el cero aparece en la sucesión $\{z_n\}$ o como el limite del producto infinito, una condición necesaria para la convergencia de productos infinitos es que el $n-$ésimo termino debe converger a 1. Por otro lado, notemos que para $z_n = a$ para toda n y $|a| < 1$, $\prod z_n = 0$ a pesar que $\lim\limits_{n\to\infty} z_n = a \neq 0$. Debido al hecho de que la exponencial de una suma es el producto de las exponenciales de los términos individuales, es posible discutir la convergencia de un producto infinito (cuando el cero no está involucrado) discutiendo la convergencia de la serie $\sum \log z_n$, donde log es la rama principal del logaritmo. Sin embargo, para que tenga sentido trabajar con $\log z_n$ debemos restringir a z_n. Si el producto debe ser distinto de cero, entonces $z_n \to 1$. Así que, sin pérdida de generalidad, podemos suponer que $\Re(z_n) > 0$. Ahora, supongamos que la serie $\sum \log z_n$ converge. Si $s_n = \sum_{k=1}^{n} \log z_k$ y $s_n \to s$, entonces $e^{s_n} \to e^s$. Pero $e^{s_n} = \prod_{k=1}^{n} z_k$, por lo tanto $\prod_{k=1}^{n} z_k$ converge a $z = e^s \neq 0$.

Proposición 2.4.2. *Sea $\Re(z_n) > 0$ para todo $n \geq 1$. Entonces $\displaystyle\prod_{k=1}^{n} z_k$ converge a un número distinto de cero si y solo si la serie $\displaystyle\sum_{k-1}^{\infty} \log z_k$ converge.*

Demostración. Sea $p_n = \prod_{k=1}^{n} z_k$, $z = re^{i\theta}$, $-\pi < \theta \leq \pi$ y sea $l(p_n) = \log|p_n| + i\theta_n$ la rama principal de logaritmo, donde $\theta - \pi < \theta_n \leq \theta + \pi$. Si $s_n = \sum_{k=1}^{n} \log z_k$, entonces $e^{s_n} = p_n$ de tal forma que $s_n = l(p_n) + 2i\pi k_n$ para algún entero k_n. Ahora supongamos que $p_n \to z$. Entonces $s_n - s_{n-1} = \log z_n \to 0$; también $l(p_n) - l(p_{n-1}) \to 0$. Entonces, $(k_n - k_{n-1}) \to 0$ cuando $n \to \infty$. Como cada k_n es un entero esto significa que existe un n_0 y una k tal que $k_m = k_n = k$ para $m, n \geq n_0$. Así que $s_n \to l(z) + 2i\pi k$; esto es, que la serie $\sum ln(z_n)$ converge. Como el regreso fue probado arriba, esto completa la prueba. ■

Considera la expansión en series de potencias de $\log(1 + z)$ alrededor de $z = 0$:

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

la cual tiene radio de convergencia igual a 1. Si $|z| < 1$ entonces

$$\begin{aligned}\left|1 - \frac{\log(1+z)}{z}\right| &= \left|\frac{1}{2}z - \frac{1}{3}z^2 + \dots\right| \\ &\leq \frac{1}{2}(|z| + |z|^2 + \dots) \\ &= \frac{1}{2}\frac{|z|}{1-|z|}\end{aligned}$$

Si requerimos además que $|z| < \frac{1}{2}$, entonces tenemos que

$$\left|1 - \frac{\log(1+z)}{z}\right| \leq \frac{1}{2}$$

Lo cual nos dice que para $|z| < \frac{1}{2}$ tenemos que

$$\frac{1}{2}|z| \leq |\log(1+z)| \leq \frac{3}{2}|z| \tag{2.115}$$

Proposición 2.4.3. *Sea $\Re(z_n) > -1$; entonces la serie $\sum \log(1+z_n)$ converge absolutamente si y solo si la serie $\sum z_n$ converge absolutamente.*

Demostración. Si $\sum |z_n|$ converge, entonces $z_n \to 0$; entonces tenemos que eventualmente $|z_n| < \dfrac{1}{2}$. Por la ecuación (2.115), tenemos que $\sum \log(1+z_n)$ está dominado por una serie convergente, por lo que también converge. Para el regreso, tenemos que $\sum \log(1+z_n)$ converge entonces tenemos que $|z_n| < \dfrac{1}{2}$ para una n lo suficientemente grande. De nuevo, lo anterior nos permite concluir que $\sum |z_n|$ converge. ■

B. Identidad de Euler para Cotangente

En este apéndice daremos una prueba de la identidad de Euler para $\pi \cot \pi z$. Esta identidad es crucial en esta tesis ya que juega un papel fundamental en la prueba de que el producto infinito

$$q \prod_{n=1}^{\infty} (1-q^n)^{24}$$

es una forma modular cuspidal de peso 12, lo que nos permite deducir que

$$q \prod_{n=1}^{\infty} (1-q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n$$

donde $\tau(n)$ es la función Tau de Ramanujan.
Veamos una prueba de dicha identidad la cual fue primero probada por Euler en 1748[4].

$$\pi \cot \pi z = \sum_{-\infty}^{\infty} \frac{1}{z+n} = \lim_{N\to\infty} \sum_{|n|\leq N} \frac{1}{z+n} = \frac{1}{z} + \sum_{n=1}^{\infty} \frac{2z}{z^2-n^2} \tag{2.116}$$

Esta fórmula se cumple cuando z no es un entero. La suma $\sum_{-\infty}^{\infty} \dfrac{1}{z+n}$ debe ser propiamente entendida, ya que las mitades separadas que corresponden a cuando n es positiva y cuando n es negativa no convergen. Únicamente cuando se interpreta simétricamente, como $\lim \sum_{|n|\leq N} \dfrac{1}{z+n}$, la cancelación de los términos nos lleva a la serie convergente dada por la ecuación (2.116).
Para demostrar (2.116), mostraremos que $\pi \cot \pi z$ y la serie de la derecha en (2.116) tiene las mismas propiedades estructurales. De hecho, observemos que si $F(z) = \pi \cot(\pi z)$, entonces F tiene las siguiente tres propiedades:

1. $F(z+1) = F(z)$ cuando z no es un entero.

[4]Está prueba fue tomada de [14]. Una prueba para el caso real puede encontrarse en [8].

2. $F(z) = \dfrac{1}{z} + F_0(z)$, donde F_0 es una función analítica cerca del cero.
3. $F(z)$ tiene polos simples en los enteros y no tiene ninguna otra singularidad

Entonces notamos que la función

$$\sum_{-\infty}^{\infty} \frac{1}{z+n} = \lim_{N\to\infty} \sum_{|n|\leq N} \frac{1}{z+n}$$

también cumple con las mismas tres propiedades. De hecho, la propiedad 1 se obtiene de observar que pasar de z a $z+1$ simplemente cambia los términos de la suma infinita. Para ser precisos,

$$\sum_{|n|\leq N} \frac{1}{z+1+n} = \frac{1}{z+1+N} - \frac{1}{z-N} + \sum_{|n|\leq N} \frac{1}{z+n}$$

Si hacemos a N tender al infinito probamos dicha afirmación. Las propiedades 2 y 3 son evidentes de la representación $\dfrac{1}{z} + \sum_{n=1}^{\infty} \dfrac{2z}{z^2-n^2}$ de la suma.
Por lo tanto, la función definida como

$$\Delta(z) = F(z) - \sum_{-\infty}^{\infty} \frac{1}{z+n}$$

es periódica en el sentido de que $\Delta(z) = \Delta(z+1)$, y por la propiedad 2 la singularidad de Δ en el origen es removible, y, por lo tanto, por la periodicidad de Δ, las singularidades en todos los enteros también son removibles; esto implica que Δ es una función entera.

Para demostrar nuestra fórmula, será suficiente mostrar que la función Δ está acotada en el plano complejo. Por la periodicidad de arriba, es suficiente acotarla en la franja $|\Re(z)| \leq 1/2$. Esto se debe a que cada $z' \in \mathbb{C}$ es de la forma $z' = z + k$, donde z está en la franja antes mencionada y k es un entero. Como Δ es holomorfa, está acotada en el rectángulo $|\Im(z)| \leq 1$ y solo necesitamos controlar el comportamiento de la función Δ para $|\Im(z)| > 1$. Si $\Im(z) > 1$ y $z = x + iy$, entonces

$$\cot \pi z = i\,\frac{e^{i\pi z} + e^{-i\pi z}}{e^{i\pi z} - e^{-i\pi z}} = i\,\frac{e^{-2\pi y} + e^{-2i\pi x}}{e^{2\pi y} - e^{-2i\pi x}},$$

lo cual, en valor absoluto, está acotado.
Además

$$\frac{1}{z} + \sum_{n=1}^{\infty} \frac{2z}{z^2-n^2} = \frac{1}{x+iy} + \sum_{n=1}^{\infty} \frac{2(x+iy)}{x^2-y^2-n^2+2ixy};$$

por lo tanto si $y > 1$, tenemos que

$$\left| \frac{1}{z} + \sum_{n=1}^{\infty} \frac{2z}{z^2-n^2} \right| \leq C + C\sum_{n=1}^{\infty} \frac{y}{y^2+n^2}.$$

La suma del lado derecho es mayorizada por

$$\int_0^\infty \frac{y}{y^2 + n^2} dx$$

porque la función $y/(y^2 + n^2)$ es decreciente en x; más aún, como lo muestra el cambio de variable $x \to xy$, la integral es independiente de y y por lo tanto está acotada. Por un argumento similar, Δ está acotada en la parte de la franja donde $\Im(z) < -1$, y por lo tanto está acotada en toda la franja $|\Re(z)| \leq \frac{1}{2}$. Por lo tanto, Δ está acotada en $\mathbb{C}$, y por el Teorema de Liouville, $\Delta(z)$ es constante. La observación de que Δ es impar muestra que esta constante debe ser 0 y concluye la prueba de la fórmula (2.116).

Bibliografía

[1] AHLFORS, LARS V., *Complex Analysis: An Introduction to the Theory of Analytic Functions of One Complex Variable. 2D. ed*, McGraw-Hill, 1966.

[2] APOSTOL, TOM M., *Modular Functions and Dirichlet Series in Number Theory*, Graduate Texts in Mathematics 41, Springer-Verlag, 1990.

[3] CONWAY, JOHN B., *Functions of One Complex Variable I*, Graduate Texts in Mathematics 11, Springer-Verlag. 1978.

[4] DELIGNE, P., *La conjecture de Weil I*, Publ. Math. I.H.E.S., 43, pp 273-307, 1974.

[5] KARATSUBA, ANATOLIJ A., *Basic Analytic Number Theory*, Springer-Verlag Berlin Heidelberg, 1993.

[6] LYGEROS, N. & ROZIER, O. , *Odd prime values of the Ramanujan tau function*, The Ramanujan Journal, Volume 32, Issue 2, pp 269–280, Springer, 2013.

[7] MAARTEN DERICKX, MARK VAN HOEIJ, JINXIANG ZENG, *Computing Galois representations and equations for modular curves $XH(l)$*, arXiv:1312.6819v2 [math.NT], 2014.

[8] MARTIN AIGNER GÜNTER M. ZIEGLER, *Proofs from the Book*, Springer-Verlag Berlin Heidelberg, 2010.

[9] MORDELL, L., *On Mr. Ramanujan's empirical expansions of modular functions*, Proceedings of the Cambridge Philosophical Society, Volume 19, pp 117–124, 1917.

[10] RAMANUJAN, S., *On certain arithmetical functions*, Transactions of the Cambridge Philosophical Society, XXII, No.9, pp 159 − 184, 1916.

[11] REMMERT, REINHOLD, *Theory of Complex Functions*, Readings in Mathematics 122, Springer-Verlag New York, 1991.

[12] RIBENBOIM, P., *The New Book of Prime Number Records*, Springer, Berlin, 1996.

[13] Serre, J-P., *A Course in Arithmetic*, Graduate Texts in Mathematics 7, Springer-Verlag New York, 1973.

[14] Stein, E. & Shakarchi, R., *Complex Analysis*, Princeton Lectures in Analysis, Volumen 2, Princeton University Press, 2003.