Universidad Nacional Autónoma de México

FACULTAD DE CIENCIAS

FUNCIONES ELIPTICAS

T E S I S

Que para obtener el Título de

M A T E M A T I C O

p r e s e n t a

CARLOS ALONSO INFANTE VARGAS

México, D.F. Agosto 1993

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

INDICE

INTRODUCCION

En el desarrollo de esta tesis presentamos una introducción a la teoría de las "Funciones Elípticas". Dada la amplitud de esta teoría, nos hemos limitado a una exposición general de las Funciones Elípticas dejando de lado el estudio de las "Curvas Elípticas"y otros de sus aspectos geométricos y algebraicos. Tampoco profundizamos en el estudio de las relaciones entre las Funciones Modulares con los dominios fundamentales y las funciones theta. Por lo tanto los tres primeros capítulos están dedicados a la construcción de algunas funciones elípticas clásicas junto con sus propiedades elementales, así como a la de otras funciones estrechamente relacionadas con ellas que (aunque ya no son elípticas) nos sirven para expresarlas.

Como una aplicación de la teoría, en el capítulo IV se presenta una demostración de la "Ley de Reciprocidad Cuadrática". La selección de éste teorema se debe a que es el primer problema básico de la teoría de los restos cuadráticos y al hecho de que se han publicado alrededor de 150 demostraciones de él, de las cuales el propio Gauss proporcionó no menos de ocho. Concluímos el capítulo IV con algunos corolarios referentes a la "Conjetura de Goldbach".

La relación entre las Funciones Elípticas y la prueba de la Ley de Reciprocidad (que esta basada en una fórmula de transformación para la función θ_3) no es directa ni inmediata. La razón radica en que las Funciones Theta, al igual que las funciones ζ y σ, ya no son elípticas y de ello pareciera desprenderse la pérdida del concepto de "periodicidad". Sin embargo, los teoremas 2.16 y 3.6 rescatan éste concepto al proporcionarnos la expresión de cualquier función elíptica en términos de éstas funciones.

Finalmente hemos de mencionar que este trabajo proporciona una bella demostración de la fuerza de los métodos analíticos en otras ramas de la Matemática como lo es la "Teoría Analítica de los Números".

Nota: A lo largo del texto "!" significará que se ha llegado a una contradicción.

CAPITULO 1. FUNCIONES ELIPTICAS Y SUS PROPIEDADES

En este capítulo introduciremos el concepto de función elíptica, así como algunas de sus propiedades principales. Históricamente las funciones elípticas surgieron a partir de las integrales elípticas por "inversión", donde una integral elíptica es una integral de la forma

$$\int_a^t R(x,y)\,dx$$

con $R(x,y)$ una función racional de x, y y y^2 una cúbica o cuártica en x sin factores repetidos.

El comienzo de la teoría de las integrales elípticas puede relacionarse con el descubrimiento de Conte G.C. di Fagnano (y después de Euler) de dos propiedades de una integral asociada con la longitud de arco de la lemniscata, a saber:

$$\int_0^r \frac{dx}{(1-x^4)^{\frac{1}{2}}} = 2\int_0^u \frac{dx}{(1-x^4)^{\frac{1}{2}}}, \text{ con } r^2 = \frac{4u^2(1-u^4)}{(1+u^4)^2}$$

que está relacionado con el problema de la duplicación de la longitud de arco de la lemniscata y para el que Euler, alrededor de 1761, dió su famoso teorema de adición:

$$s(u) + s(v) = s(r)$$

donde

$$s(u) = \int_0^u \frac{dx}{(1-x^4)^{\frac{1}{2}}},\ 0 \le u \le 1$$

y

$$r = \frac{u(1-v^4)^{\frac{1}{2}} + v(1-u^4)^{\frac{1}{2}}}{1+u^2v^2}.$$

DEFINICION 1.1 *Sea f una función meromorfa, decimos que f es periódica si existe una constante $w \in \mathbf{C}$ no cero, tal que $f(z+w) = f(z)$, $\forall z \in \mathbf{C}$. A w se le llama un periódo de f.*

De aquí en adelante $S = \{w \in \mathbf{C} | w \text{ es un periódo de } f\}$.

OBSERVACION: Si w y w' son dos periodos de f, entonces $w + w'$ y nw, $\forall n \in \mathbf{Z}$ también son periodos de f.

PROPOSICION 1.2 *Si f es una función periódica no constante, entonces*

$$\inf_{S-\{0\}} |w| = \delta > 0.$$

Demostración: Si no fuera así, se tendría que $\forall \epsilon > 0$, $\exists w_\epsilon \neq 0$ un periódo de f, tal que $|w_\epsilon| < \epsilon$. Pero entonces existiría una sucesión $\{w_k\}$ de periodos distintos de f, tal que $\lim_{k\to\infty} w_k = 0$. Si tomamos $z_0 \in \mathbf{C}$ un punto en el cual f es analítica, entonces $f(z_0) = f(z_0 + w_k)$, $\forall k \in \mathbf{N}$ y así la función $f(z) - f(z_0)$ tendría una infinidad de ceros distintos en los puntos $z_0 + w_k$ y a z_0 como un punto de acumulación finito para ellos, por tanto $f(z) - f(z_0) \equiv 0$, es decir $f(z) = f(z_0)$ constante!.

■

PROPOSICION 1.3 *Los periodos de una función meromorfa f no constante no tienen puntos de acumulación finitos.*

Demostración: Si w fuera uno de tales puntos de acumulación, entonces $\forall \epsilon > 0$ podríamos encontrar w_1, w_2 dos periodos distintos de f en el disco: $|z - w_0| < \frac{\epsilon}{2}$. Pero $w = w_1 - w_2$ es un periódo de f con $|w| < \epsilon$!.

■

OBSERVACION: Si $\inf_{S-\{0\}} |w| = \delta$ no se alcanzara en algún periódo de f, entonces existiría una sucesión $\{w_n\}$ de periodos tal que $\lim_{n\to\infty} |w_n| = \delta$ y entonces $\lim_{n\to\infty} w_n$ sería un punto de acumulación finito para los periodos de f !. Por lo tanto existe un periódo w_1 de f con norma mínima (es decir $|w_1| = \delta$).

El siguiente teorema nos dice como son todos los periodos de f.

TEOREMA 1.4 *Sea f una función periódica, entonces se cumple una de las siguientes:*

i) $S = \{nw_1 | n \in \mathbf{Z}\}$

ii) $S = \{nw_1 + mw_2 | n, m \in \mathbf{Z}\}$

para w_1 un periódo de f de norma mínima (es decir $|w_1| = \delta$) y w_2 un periódo de norma mínima para el cual $\frac{w_2}{w_1} \notin \mathbf{R}$ y $Im\frac{w_2}{w_1} > 0$.

Demostración: Sea w_1 un periódo de f de norma mínima.

i) Si todo periódo w de f es tal que $\frac{w}{w_1} \in \mathbf{R}$, sea $n = \left[\frac{w}{w_1}\right] \in \mathbf{Z}$, entonces $0 \leq \frac{w}{w_1} - n < 1$, es decir $0 \leq \frac{w - nw_1}{w_1} < 1$. Pero tomando normas tenemos que $w - nw_1$ es un periódo de f con $0 \leq |w - nw_1| < |w_1|$, por lo tanto la única posibilidad es que $w - nw_1 = 0$, de donde $w = nw_1$. Así, en este caso todos los periodos de f son de la forma $w = nw_1$ con $n \in \mathbf{Z}$.

ii) En el caso de que existan periodos w de f con $\frac{w}{w_1} \notin \mathbf{R}$, sea w_2 uno de tales periodos con norma mínima y $\tau = \frac{w_2}{w_1}$ (su existencia está garantizada por la proposición 1.3). Podemos suponer que $Im\tau > 0$, ya que si no es así tomamos $-w_2$ en lugar de w_2. Además dada la elección de w_1 tenemos que $|\tau| \geq 1$.

Ahora, para cualquier periódo w de f existen $x, y \in \mathbf{R}$ tales que $w = xw_1 + yw_2$, con $x = m + \rho$, $y = n + \sigma$, $m, n \in \mathbf{Z}$ y $-\frac{1}{2} \leq \rho, \sigma < \frac{1}{2}$ (basta tomar $m = [x]$, luego $0 \leq \rho < 1$. Si ocurre que $\frac{1}{2} \leq \rho < 1$, tomando $m' = m + 1$ y $x = m' + \rho - 1$ tenemos que $-\frac{1}{2} \leq \rho - 1 < 0$; haciendo lo mismo para σ si es necesario) de donde $w_0 = w - mw_1 - nw_2 = \rho w_1 + \sigma w_2$ es un periódo y

$$|w_0| = |\rho w_1 + \sigma w_2| \leq |\rho w_1| + |\sigma w_2|$$
$$\leq \frac{1}{2}|w_1| + \frac{1}{2}|w_2| \leq \frac{1}{2}|w_2| + \frac{1}{2}|w_2| = |w_2|$$

Pero dado que $\frac{w_2}{w_1} \notin \mathbf{R}$, la primera desigualdad es estricta y se tiene que $|w_0| < |w_2|$. Por tanto $\frac{w_0}{w_1} = \rho + \sigma\tau \in \mathbf{R}$ (dada la elección de w_2) y entonces $\sigma = 0$. Así $\frac{w_0}{w_1} = \rho$ y dado que $|\frac{w_0}{w_1}| = |\rho| \leq \frac{1}{2}$ se tiene que $w_0 = 0$. Por lo tanto en este segundo caso los periodos de f son de la forma $nw_1 + mw_2$, con $n, m \in \mathbf{Z}$.

■

DEFINICION 1.5 *En el caso i) del teorema anterior f se llama simplemente periódica, en el caso ii) f se llama doblemente periódica.*

DEFINICION 1.6 *Una función meromorfa doblemente periódica se llama elíptica.*

OBSERVACION: Si f es elíptica, el inciso ii) del teorema 1.4 nos asegura la existencia de un par de periodos (w_1, w_2) tales que $Im\frac{w_2}{w_1} > 0$.

DEFINICION 1.7 *Cualquier par de periodos (w_1, w_2) de f como en el inciso ii) del teorema 1.4 se llaman primitivos o reducidos y se dice que forman una base del conjunto de periodos en el sentido de que todo periódo w de f se expresa en la forma $nw_1 + mw_2$ con $n, m \in \mathbf{Z}$.*

El conjunto de periodos w de f se dicé que forman una latiz de periodos. Un par de periodos que formen una base para la latiz de periodos se llaman básicos.

OBSERVACION: Por formar una base para S, todo par de periodos básicos (w_1, w_2) debe satisfacer que $\frac{w_2}{w_1} \notin \mathbf{R}$. También todo par de periodos reducidos de f es básico, pero no todo básico tiene que ser reducido.

DEFINICION 1.8 *Una transformación entre latices del tipo:*

$$w_1^* = mw_1 + nw_2$$

$$w_2^* = pw_1 + qw_2, \qquad (*)$$

con $m, n, p, q \in \mathbf{Z}$ y $mq - np = \pm 1$ se llama unimodular.

Si $mq - np = +1$ la transformación se denomina propia.

TEOREMA 1.9 *Sea (w_1, w_2) un par de periodos reducidos (básicos) de la función elíptica f. Los números complejos (w_1^*, w_2^*) son un par de periodos básicos para f si, y sólo si, están relacionados con (w_1, w_2) por una transformación unimodular.*

Demostración: Por ser (w_1, w_2) primitivos (básicos) se tiene:

$$w_1^* = mw_1 + nw_2,\ w_2^* = pw_1 + qw_2$$

También por ser (w_1^*, w_2^*) básicos:

$$w_1 = m'w_1^* + n'w_2^*,\ w_2 = p'w_1^* + q'w_2^*,$$

con $m, n, p, q, m', n', p', q' \in \mathbf{Z}$. Sustituyendo w_1^*, w_2^* en la segunda expresión tenemos:

$$w_1 = (m'm + n'p)w_1 + (m'n + n'q)w_2$$

$$w_2 = (p'm + q'p)w_1 + (p'n + q'q)w_2.$$

Por ser (w_1, w_2) periodos primitivos (básicos) de f se tiene que $\frac{w_2}{w_1} \notin \mathbf{Q}$, de donde:

$$mm' + n'p = 1, \qquad m'n + n'q = 0$$
$$p'm + q'p = 0, \qquad p'n + q'q = 1$$

o en forma matricial:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} m' & n' \\ p' & q' \end{pmatrix} \begin{pmatrix} m & n \\ p & q \end{pmatrix}$$

Tomando determinantes obtenemos:

$$1 = (m'q' - n'p')(mq - np)$$

y por tanto $mq - np = \pm 1$ (ya que ambos factores son enteros).

Inversamente, dada la tranformación unimodular en (*) podemos resolver para w_1 y w_2, y obtener:

$$w_1 = \pm(qw_1^* - nw_2^*),\ w_2 = \pm(-pw_1^* + mw_2^*)$$

Ahora, si $w = aw_1 + bw_2$ con $a, b \in \mathbf{Z}$ es un periódo de f, entonces:

$$w = a'w_1^* + b'w_2^* \text{ para algunos } a', b' \in \mathbf{Z}.$$

y así (w_1^*, w_2^*) es un par de periodos básicos.

■

TEOREMA 1.10 *Un par de periodos básicos (w_1, w_2) de f es un par de periodos reducidos si, y sólo si, se tiene: $|\tau| \geq 1$, $Im\tau > 0$, $-\frac{1}{2} \leq Re\tau \leq \frac{1}{2}$, para $\tau = \frac{w_2}{w_1}$.*

Demostración: Sea $\tau = \xi + i\eta$. Si (w_1, w_2) es un par de periodos reducidos, entonces $Im\tau > 0$, $|\tau| \geq 1$. Además por ser $\frac{w_2 \pm w_1}{w_1} = 1 \pm \tau \notin \mathbf{R}$ se tiene que $|w_2 \pm w_1| \geq |w_2| \geq |w_1|$ y por tanto $|\tau \pm 1|^2 \geq |\tau|^2 \geq 1$, es decir $(\xi \pm 1)^2 + \eta^2 \geq \xi^2 + \eta^2 \geq 1$ de donde $\pm 2\xi + 1 \geq 0$ y $\frac{1}{2} \geq \xi \geq -\frac{1}{2}$.
Inversamente, como $|\frac{w_2}{w_1}| = |\tau| \geq 1$ y $Im\tau > 0$, entonces $\frac{w_2}{w_1} \notin \mathbf{R}$. Sea $w = mw_1 + nw_2$, con $m, n \in \mathbf{Z}$ un periódo distinto de cero.
Si $n = 0$, entonces $\frac{w}{w_1} = m \in \mathbf{R}$ y $|w| = |mw_1| \geq |w_1|$, y por tanto w_1 tiene norma mínima.
Si $n \neq 0$, entonces $\frac{w}{w_1} = m + n\tau \notin \mathbf{R}$. Sea

$$D = |m + n\tau|^2 - |\tau|^2 = (m + n\xi)^2 - \xi^2 + (n^2 - 1)\eta^2.$$

Si $n \neq \pm 1$, entonces $n^2 - 1 \geq 3$ y como $\eta^2 = (\xi^2 + \eta^2) - \xi^2 \geq 1 - \frac{1}{4} = \frac{3}{4}$ (ya que $|\xi| \leq \frac{1}{2}$) se tiene que $D \geq -\xi^2 + (n^2 - 1)\eta^2 \geq -\frac{1}{4} + 3\frac{3}{4} = 2 > 0$.
Si $n = \pm 1$, entonces $D = (m \pm \xi)^2 - \xi^2 = m^2 \pm 2m\xi \geq 0$ (ya que $|\xi| \leq \frac{1}{2}$, por tanto $|2m\xi| \leq |m| \leq m^2$).
En cualquier caso $D \geq 0$, es decir $|w| \geq |w_2|$ y w_2 tiene norma mínima entre aquellos que cumplen $\frac{w}{w_1} \notin \mathbf{R}$. Además por hipótesis $|w_2| \geq |w_1|$ y así (w_1, w_2) es primitivo.

■

TEOREMA 1.11 *Dada una función elíptica f no constante, existe un par de periodos básicos (w_1, w_2) de f, tal que $\tau = \frac{w_2}{w_1}$ satisface:*

$$Im\tau > 0, |\tau| \geq 1, -\frac{1}{2} \leq Re\tau < \frac{1}{2},$$

con $Re\tau \leq 0$ si $|\tau| = 1$ (y entonces por el teorema 1.10 (w_1, w_2) es primitivo).
Además si (w_1^*, w_2^*) es otro par de periodos primitivos tales que:

$$w_1^* = mw_1 + nw_2,$$

$$w_2^* = pw_1 + qw_2$$

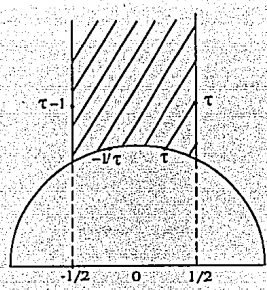
y $\tau^* = \frac{w_2^*}{w_1^*}$ satisface:

$$Im\tau^* > 0, |\tau^*| \geq 1, -\frac{1}{2} \leq Re\tau^* < \frac{1}{2},$$

con $Re\tau^* \leq 0$ si $|\tau^*| = 1$; entonces $\tau^* = \tau$.

Demostración: El inciso ii) del teorema 1.4 nos asegura la existencia de un par de periodos primitivos (w_1, w_2) de f, además el teorema 1.10 nos dice que: $|\tau| \geq 1$, $Im\tau > 0$ y $-\frac{1}{2} \leq Re\tau \leq \frac{1}{2}$.
Si τ está en la línea: $Re\tau = \frac{1}{2}$, entonces $\tau - 1$ está en la línea: $Re\tau = -\frac{1}{2}$.

Si τ está en el arco: $|\tau| = 1$ con $0 < Re\tau < \frac{1}{2}$, entonces $-\frac{1}{\tau} = -\overline{\tau}$ está en el arco: $|\tau| = 1$ con $-\frac{1}{2} < Re(-\overline{\tau}) < 0$.



Como las transformaciones:

$$w_1^* = w_1,$$

$$w_2^* = -w_1 + w_2$$

y

$$w_1^* = w_2,$$

$$w_2^* = -w_1$$

son unimodulares propias y llevan $\tau \mapsto \tau - 1$, $\tau \mapsto -\frac{1}{\tau}$, respectivamente y dado que $Im\tau^* = Im\left(\frac{q\tau+p}{n\tau+m}\right) = \frac{(mq-np)Im\tau}{|n\tau+m|^2} = \frac{Im\tau}{|n\tau+m|^2}$ (*), entonces $Im\tau^* > 0$ si $Im\tau > 0$. Como también la composición de transformaciones unimodulares propias es unimodular propia, se han cubierto todos los casos posibles y se tiene la primera parte del teorema.

Para la segunda parte, por el teorema 1.9: $mq - np = \pm 1$ y como $Im\tau, Im\tau^* > 0$ entonces $mq - np = 1$. Por ser (w_1, w_2) y (w_1^*, w_2^*) primitivos se tiene $|w_1^*| \leq |w_1|, |w_2|$ y $|w_1| \leq |w_1^*|, |w_2^*|$ por lo tanto $|w_1^*| = |w_1| \leq |w_2|$. Luego $1 = |\frac{w_1^*}{w_1}| = |m + n\tau|$ y por (*) $Im\tau^* = Im\tau$.

Sean $\tau = \xi + i\eta$ y $\tau^* = \xi^* + i\eta$. Si $n = 0$, entonces $mq = 1$ y $m = q = \pm 1$, por tanto $\tau^* = \tau \pm p$ y como $-\frac{1}{2} \leq \xi^*, \xi < \frac{1}{2}$, se tiene que $p = 0$. Así $\tau^* = \tau$. Si $n \neq 0$, tenemos:

$$\begin{aligned}
\tau^* &= \frac{1}{n^2}\left(\frac{n^2(q\tau+p)}{n\tau+m}\right) \\
&= \frac{1}{n^2}\left(\frac{qn(n\tau+m) - qnm + pn^2}{n\tau+m}\right) \\
&= \frac{1}{n^2}\left(qn - \frac{n}{n\tau+m}\right) \\
&= \frac{1}{n^2}(qn - n(n\overline{\tau}+m)) \\
&= \frac{1}{n^2}(qn - nm - n^2(\xi - i\eta)) \\
&= \frac{1}{n}(q-m) - (\xi - i\eta)
\end{aligned}$$

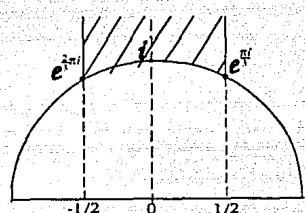
por tanto

$$\xi^* + \xi = \frac{1}{n}(q - m) \qquad (**)$$

Dado que $1 = |m + n\tau|^2 = (m + n\xi)^2 + (n\eta)^2$ no puede ser $|n| \geq 2$ (ya que entonces $n^2 \geq 4$ y como $\eta^2 \geq \frac{3}{4}$ se tendría: $n^2\eta^2 \geq 3$ y por tanto $|m + n\tau^2| \geq 3$!), de donde $|n| \leq 1$, es decir $n = \pm 1$. Así, $|m \pm \tau|^2 = 1$ y dado que $|\tau| \geq 1$ y $-\frac{1}{2} \leq Re\tau < \frac{1}{2}$, entonces $m = 0$ ó $m = 1$.

Caso 1: Si $m = 0$, se tiene $1 = |\pm\tau| = |\tau|$ y como por $(**)$ $-1 \leq \xi^* + \xi = \pm q < 1$, entonces: $q = 0$ ó $q = -1$.

Si $q = 0$, entonces $\tau^* = \frac{q\tau + p}{n\tau + m} = \frac{p}{n\tau}$, pero $1 = mq - np = -np$; por tanto $n, p = \pm 1$ y tienen signos opuestos. Así $\tau^* = -\frac{1}{\tau}$ y por tanto $|\tau^*| = |\overline{\tau}| = 1$. Pero por hipótesis $\xi^*, \xi \leq 0$ y como $\xi^* + \xi = 0$, se tiene que: $\xi^* = \xi = 0$ y $\tau^* = i\eta = \tau$. Como $|\tau| = 1$ y $Im\tau > 0$, debe ser $\tau^* = \tau = i$.



Si $q = -1$, entonces $\xi^* + \xi = -1$. Por tanto $\xi^* = \xi = -\frac{1}{2}$ y dado que $|\tau| = 1$ entonces $\tau^* = \tau = e^{\frac{2}{3}\pi i}$.

Caso 2: Si $m = 1$, entonces $|\tau \pm 1| = 1$; pero no puede ser $|\tau - 1| = 1$ (porque solo $\tau = e^{\frac{\pi i}{3}}$ lo cumple y en este caso $\xi = \frac{1}{2}$!) por lo tanto $|\tau + 1| = 1$ y dado que $|\tau| \geq 1$ se tiene $\tau = e^{\frac{2}{3}\pi i}$. Además $Im\tau^* = Im\tau$ y $|\tau^*| \geq 1$ por lo tanto $\tau^* = \tau = e^{\frac{2}{3}\pi i}$.

■

DEFINICION 1.12 *Sea $z \in \mathbf{C}$ y $a, b, c, d \in \mathbf{Z}$. La transformación:*

$$M : z \mapsto z' = \frac{az + b}{cz + d}$$

con $ad - bc = 1$ y $cz + d \neq 0$, se llama transformación modular.

Puesto que $Imz' = \frac{Imz}{|cz+d|^2} > 0$ si $Imz > 0$, entonces se tiene que M mapea el semiplano superior en sí mismo. Las transformaciones modulares forman un subgrupo de las transformaciones de Moebius.

PROPOSICION 1.13 *El grupo de las transformaciones modulares está generado por las dos transformaciones:*

$$A : z \mapsto z + 1,$$

$$B : z \mapsto -\frac{1}{z}.$$

Demostración: Observemos que $B^2 = I$ es la identidad.

Sean $M : z \mapsto \frac{az+b}{cz+d}$ y $m = min\{|c|, |d|\}$.

Podemos considerar que $|c| \leq |d|$, puesto que si $|c| > |d|$, entonces la transformación:

$$MB : z \mapsto \frac{bz - a}{dz - c} = \frac{a'z + b'}{c'z + d'}$$

tiene la propiedad $|c'| < |d'|$, por lo cual basta considerar las transformaciones con $|c| \leq |d|$. Procederemos por inducción sobre m.

Si $m = 0$, entonces $c = 0$ y $ad = 1$, por tanto $M : z \mapsto z \pm b$ y $M = A^{\pm b}$. Supongamos que para cualquier M con $m \leq n - 1$ $(n \geq 1)$, M esta generada por A y B. Ahora, sea M tal que $m = n$; por consiguiente $|c| = m$. Podemos suponer que $c > 0$, pues si no tomamos $-a, -b, -c, -d$ en M lo cual define la misma transformación. Luego $m = c = n$.

Consideremos $MA^k : z \mapsto \frac{az+(ak+b)}{cz+(ck+d)}$ con $k \in \mathbf{Z}$ tal que $0 \leq ck + d < c$ (es decir $-\frac{d}{c} \leq k < 1 - \frac{d}{c}$). Para ésta k tenemos: $min\{c, ck+d\} = ck+d \leq n-1$ y por hipótesis de inducción $MA^k = \langle A, B\rangle$ esta generada por A y B, de donde se sigue que $M = \langle A, B\rangle A^{-k}$ también esta generada por A y B.

■

PROPOSICION 1.14 *Dado $z \in \mathbf{C}$ con $Imz > 0$, existe una transformación modular M^* tal que: $Im(M^*z)$ es máximo. Si $M^*z = z^*$, entonces $|z^*| \geq 1$.*

Demostración: Si $M^*z = x^* + iy^*$, entonces $y^* = \frac{y}{|cz+d|^2} > 0$ y por lo tanto y^* alcanza su máximo cuando $|cz + d|$ es mínimo. Pero las parejas $\{c, d\}$ de enteros tales que $|cz + d| < K < \infty$ para alguna constante K, son finitas (porque z es fijo). Así, tomamos una de tales parejas de enteros con norma mínima. Para ésta pareja tenemos $(c, d) = 1$ (ya que si no $\{\frac{c}{(c,d)}, \frac{d}{(c,d)}\}$ sería un par de enteros tales que $\left|\frac{c}{(c,d)}z + \frac{d}{(c,d)}\right| < |cz + d|$!). Por lo tanto si definimos $M^* : z \mapsto \frac{az-b}{cz+d}$, donde $a, b \in \mathbf{Z}$ son tales que $bc + ad = (c, d) = 1$, se cumple que $Im(M^*z)$ es máximo.

Por último, si $|z^*| < 1$, entonces $Im\left(-\frac{1}{z^*}\right) = Im\left(-\frac{\overline{z^*}}{|z^*|^2}\right) = \frac{y^*}{|z^*|^2} > y^*$!. Por tanto $|z^*| \geq 1$.

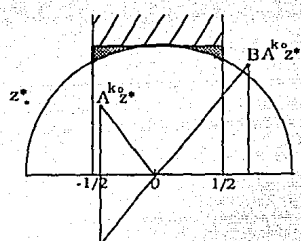
■

PROPOSICION 1.15 *Sea* $F = \{z | Imz > 0, |z| \geq 1, |Rez| \leq \frac{1}{2}\}$. *Dado* $z \in \mathbf{C}$ *con* $Imz > 0$, *existe una transformación modular* M, *tal que* $Mz \in F$.

Demostración: De la proposición 1.14 tenemos que existe M^* tal que $Im(M^*z) > 0$ es máximo y $|z^*| \geq 1$.

i) Si $Im(M^*z) \geq 1$, entonces $Im(A^k M^* z)$ sigue siendo máximo y $|A^k M^* z| \geq 1$, $\forall k \in \mathbf{Z}$ (ya que es una traslación paralela al eje real). Por lo cual basta escoger una k adecuada tal que $A^k M^* z \in F$ y tomar $M = A^k M^*$.

ii) Si $Im(M^*z) < 1$ también existe $k_0 \in \mathbf{Z}$ tal que $A^{k_0} z^*$ está en la banda $\{z \in \mathbf{C} | Im(z) > 0, |Re(z)| \leq \frac{1}{2}\}$. Aseguramos que $A^{k_0} z^*$ pertenece a la zona sombreada de F indicada en la figura.



Ya que si $|A^{k_0} z^*| < 1$, entonces $|BA^{k_0} z^*| > 1$ (para B como en la proposición 1.13) y por semejanza de triángulos se tiene que:

$$\frac{Im(BA^{k_0} z^*)}{|BA^{k_0} z^*|} = \frac{Im(A^{k_0} z^*)}{|A^{k_0} z^*|}$$

de donde

$$Im(BA^{k_0} z^*) = \frac{Im(A^{k_0} z^*)|BA^{k_0} z^*|}{|A^{k_0} z^*|} = Im(A^{k_0} z^*)|BA^{k_0} z^*|^2.$$

Pero $Im(A^{k_0} z^*)$ es máxima ya que $Im(z^*)$ lo es, por tanto $Im(BA^{k_0} z^*) \leq Im(A^{k_0} z^*)$ y entonces $|BA^{k_0} z^*|^2 \leq 1$!.

■

DEFINICION 1.16 *Sean* $z_1, z_2 \in \mathbf{C}$ *tales que* $Imz_1, Imz_2 > 0$. *Se dice que* z_1 *y* z_2 *son congruentes (con respecto al grupo modular) si existe una transformación modular* M, *tal que* $z_2 = Mz_1$. *En tal caso escribimos* $z_1 \sim z_2$. *Claramente "*$\sim$*"es una relación de equivalencia.*

PROPOSICION 1.17 *Si* $z_1, z_2 \in F$, $z_1 \neq z_2$ *y* $z_1 \sim z_2$, *entonces* $Rez_1 = \frac{1}{2}$ *y* $z_2 = z_1 - 1$; *ó* $Rez_1 = -\frac{1}{2}$ *y* $z_2 = z_1 + 1$; *ó* $|z_1| = 1$ *y* $z_2 = -\frac{1}{z_1}$.

Demostración: Sabemos que existe M tal que: $Mz_1 = z_2 = \frac{az_1+b}{cz_1+d}$, con $ad-bc=1$. Podemos suponer que $Imz_2 \geq Imz_1$ (si no es así, tomamos $z_1 = M^{-1}z_2$ y cambiamos z_2 por z_1) es decir $|cz_1+d| \leq 1$. Entonces $1 \geq |cz_1+d|^2 \geq c^2(Imz_1)^2 \geq \frac{3}{4}c^2$ (ya que $|Rez_1| \leq \frac{1}{2}$ y $|z_1| \geq 1$ por estar z_1 en F, por tanto $Imz_1 \geq \frac{\sqrt{3}}{2}$) de donde $\frac{4}{3} \geq c^2$ y por lo tanto $c = 0$ ó $c = \pm 1$.

Si $c = -1$, al multiplicar a, b, c, d por -1 en M no se altera la transformación, por lo cual podemos considerar que $c = 1$. Luego, sólo debemos considerar cuando $c = 0, 1$.

i) Si $c = 0$, entonces $1 \geq |cz_1+d|^2 = |d|^2$ y como $|cz_1+d| \neq 0$, debe ser $d = \pm 1$ y entonces $a = \pm 1$. De hecho $d = a = +1$ ya que a, b, c, d y $-a, -b, -c, -d$ definen la misma transformación M; así: $z_2 = Mz_1 = z_1 + b = A^{+b}z_1$. Pero $|Rez_1|, |Rez_2| \leq \frac{1}{2}$, por tanto $b = 0$ ó $|b| = 1$. Si $b = 0$, entonces $z_1 = z_2$!. Así debe ser $|b| = 1$. Si $b = 1$, entonces $Rez_1 = -\frac{1}{2}$ y $z_2 = z_1 + 1$. Si $b = -1$, entonces $Rez_1 = \frac{1}{2}$ y $z_2 = z_1 - 1$.

ii) Si $c = 1$, entonces $|cz_1 + d| = |z_1 + d| \leq 1$. Pero $|z_1| \geq 1$ ya que $z_1 \in F$, por consiguiente debe ser $d = 0, \pm 1$.

a) Si $d = 0$, entonces $|z_1| \leq 1$, por tanto $|z_1| = 1$ y $ad - bc = -b = 1$, de donde $z_2 = Mz_1 = a - \frac{1}{z_1}$. Entonces $z_2 + \frac{1}{z_1} = a$ y $Rez_2 + Re\frac{1}{z_1} = a$, luego $|a| \leq |Rez_2| + |Re\frac{1}{z_1}| = |Rez_2| + |Re\overline{z_1}| = |Rez_2| + |Rez_1| \leq 1$ (pues $z_1, z_2 \in F$) de donde $a = 0$ ó $a = \pm 1$.

Si $a = 0$, entonces $z_2 = -\frac{1}{z_1}$.

Si $a = 1$, entonces $z_2 = 1 - \frac{1}{z_1} = 1 - \overline{z_1}$ con $|z_1| = 1$. Por tanto $Rez_2 = 1 - Rez_1$, de donde $Rez_2 = Rez_1 = \frac{1}{2}$ y entonces, como $|z_1| = 1$, debe ser $z_1 = z_2 = e^{\frac{\pi i}{3}}$!

Si $a = -1$, entonces $z_2 = -1 - \frac{1}{z_1} = -1 - \overline{z_1}$ y $z_1 = z_2 = e^{\frac{2\pi i}{3}}$!

b) Si $d = 1$, entonces $|z_1 - (-d)| \leq 1$ define un disco circular con centro en $-d = -1$ y radio 1. Pero $z_1 \in F$, entonces $z_1 = e^{\frac{2\pi i}{3}}$.

Como $c = d = 1$ y $ad - bc = a - b = 1$ entonces:

$$z_2 = \frac{az_1 + (a-1)}{z_1 + 1} = \frac{a(z_1+1)-1}{z_1+1} = a - \frac{1}{z_1+1} = a + z_1$$

Como $|Rez_1| = -\frac{1}{2}$ y $|Rez_2| \leq \frac{1}{2}$, entonces $a = 0$ ó $a = 1$. Pero si $a = 0$ se tiene $z_2 = z_1$!, por lo cual debe ser $a = 1$ y así $z_2 = z_1 + 1$.

c) Si $d = -1$, razonando como en *b)* tenemos $a = -1$ y $z_2 = z_1 - 1$.

■

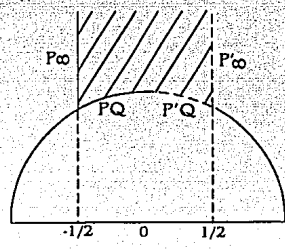
COROLARIO 1.18 *Sea* $F_0 = \{z | Imz > 0, |z| \geq 1, -\frac{1}{2} \leq Rez \leq 0\} \cup \{z | Imz > 0, |z| > 1, 0 < Rez < \frac{1}{2}\}$. *Si* $z_1 \neq z_2$ *y* $z_1, z_2 \in F_0$, *entonces* $z_1 \not\sim z_2$.

Además dado $z \in \mathbf{C}$ *con* $Imz > 0$, *existe* $z' \in F_0$ *tal que* $z' \sim z$.

Demostración: Tenemos que $\text{int}F = \text{int}F_0$ y si $z_1, z_2 \in \text{int}F_0$ y $z_1 \neq z_2$, entonces por la proposición 1.17 tenemos que $z_1 \not\sim z_2$.

La otra afirmación se desprende de la proposición 1.15 y del hecho de que el arco: $P'Q(Im z > 0, |z| = 1, 0 \leq Re z \leq \frac{1}{2})$ es llevado en el arco: $PQ(Im z > 0, |z| = 1, -\frac{1}{2} \leq Re z \leq 0)$ por la transformación modular $z \mapsto -\frac{1}{z}$ y la línea: $P'\infty(Re = \frac{1}{2}, Im z \geq \frac{\sqrt{3}}{2})$ es llevada en la línea: $P\infty(Re = -\frac{1}{2}, Im z \geq \frac{\sqrt{3}}{2})$ por la transformación modular $z \mapsto z - 1$.

■



DEFINICION 1.19 *Sea P el paralelogramo en el plano complejo formado por los puntos $z = xw_1 + yw_2$, con $0 \leq x, y < 1$. Llamamos a P un paralelogramo de periodos fundamental asociado con f para (w_1, w_2) como periodos básicos y $Im\tau > 0$.*

Definimos el recorrido en el sentido de los vértices $0, w_1, w_1 + w_2, w_2$ de ∂P como positivo. Sea $\Omega = mw_1 + nw_2$ con $m, n \in \mathbf{Z}$, entonces $P_{m,n}$ denota el trasladado de P por Ω y esta dado por los puntos $xw_1 + yw_2$, con $m \leq x < m + 1$, $n \leq y < n + 1$. $P_{m,n}$ es llamado un paralelogramo de periodos ($P_{0,0} = P$).

Cada $z \in \mathbf{C}$ vive en exactamente un $P_{m,n}$, por lo que dada la periodicidad de f basta estudiarla en P.

TEOREMA 1.20 *Toda función elíptica y entera $E(z)$ es constante.*

Demostración: Si $E(z)$ es analítica en $\overline{P}$, entonces por continuidad $|E(z)| < M < \infty$, $\forall z \in \overline{P}$ y por tanto $\forall z \in \mathbf{C}$. Así, por el teorema de Liouville, tenemos que f es constante.

■

Dado que f es meromorfa se tiene el siguiente corolario:

COROLARIO 1.21 *Una función elíptica no constante tiene por lo menos un polo en cualquier paralelogramo de periodos.*

TEOREMA 1.22 *La suma de los residuos de los polos de una función elíptica en un paralelogramo de periodos es cero.*

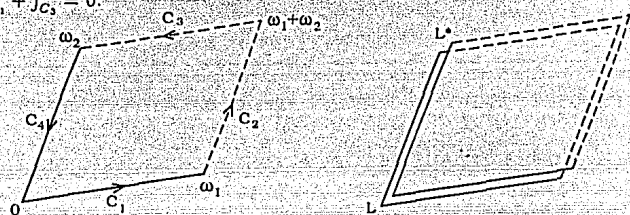
Demostración: Sea $E(z)$ una función elíptica y $L = \partial P$ orientada positivamente. Supongamos que $E(z)$ no tiene polos en L, entonces

$$\sum_{k=1}^{N} Res_{z=z_k} E(z) = \frac{1}{2\pi i} \int_L E(z)\, dz.$$

Pero por la periodicidad de $E(z)$:

$$\int_{C_1} E(z)\, dz = \int_{C_1} E(z + w_2)\, dz = -\int_{C_3} E(z)\, dz$$

de donde $\int_{C_1} + \int_{C_3} = 0$.



Similarmente $\int_{C_2} + \int_{C_4} = 0$, por tanto

$$\int_L E(z)\, dz = 0$$

y

$$\sum_{k=1}^{N} Res_{z=z_k} E(z) = 0.$$

Si uno o más polos están en L, entonces movemos L hacia L^* de forma que sus lados sean paralelos a los de L, sobre L^* no haya polos y contenga en su interior todos los polos de P (esto se puede hacer ya que los polos son aislados). Observemos que los polos que se encontraban sobre C_2 ahora pertenecen al interior de L^*. Pero

$$Res_{z=z_k+w_1} E(z) = \int_{\Gamma^*} E(z)\, dz$$

donde z_k es un polo en C_4 y Γ^* es una curva que lo encierra en su interior. Así, podemos tomar $\Gamma^* = \Gamma + w_1$ donde Γ es una curva que encierra en su interior a z_k y por lo tanto

$$\begin{aligned} Res_{z=z_k+w_1} E(z) &= \int_{\Gamma^*} E(z)\, dz \\ &= \int_{\Gamma+w_1} E(z + w_1)\, dz \\ &= \int_{\Gamma} E(z)\, dz \\ &= Res_{z=z_k} E(z). \end{aligned}$$

Por lo tanto $\int_{L^*} E(z)\, dz = \int_L E(z)\, dz = 0$ y se tiene el resultado.

■

Del teorema anterior se sigue el corolario:

COROLARIO 1.23 *Una función elíptica no constante no puede tener sólo un polo simple en un paralelogramo de periodos. Así por lo menos debe tener dos polos simples o un único polo que no sea simple.*

TEOREMA 1.24 *El número de ceros de una función elíptica no constante en un paralelogramo de periodos P es igual al número de polos en P(los ceros y los polos contados de acuerdo a su multiplicidad).*

Demostración: Sea $E(z)$ una función elíptica no constante, entonces $E'(z)$ es meromorfa y tiene por lo menos como periodos a aquellos de $E(z)$, por consiguiente $E'(z)$ también es elíptica y como el conjunto de las funciones elípticas con un par de periodos primitivos dado forman un campo, tenemos que $\frac{E'(z)}{E(z)}$ es elíptica y por el teorema 1.22 la suma de los residuos en P es cero, esto es:

$$0 = Res_{z=z_k} \frac{E'(z)}{E(z)} = \frac{1}{2\pi i} \int_L \frac{E'(z)}{E(z)}\, dz.$$

Para calcular esta última integral observemos que los polos de $\frac{E'(z)}{E(z)}$ están en los ceros o polos de $E(z)$. Pero si a es un cero de $E(z)$ de orden k, entonces $E(z) = (z-a)^k f(z)$, con $f(z)$ analítica en a tal que $f(a) \neq 0$, por tanto:

$$E'(z) = k(z-a)^{k-1} f(z) + (z-a)^k f'(z)$$

de donde

$$\frac{E'(z)}{E(z)} = \frac{k}{z-a} + \frac{f'(z)}{f(z)}$$

así, a es un polo simple de $\frac{E'(z)}{E(z)}$ y $Res_{z=a} \frac{E'(z)}{E(z)} = k$.

Si b es un polo de $E(z)$ de orden l, entonces $E(z) = \frac{f(z)}{(z-b)^l}$, con $f(z)$ analítica en b tal que $f(b) \neq 0$, por lo tanto:

$$E'(z) = \frac{f'(z)(z-b)^l - f(z)l(z-b)^{l-1}}{(z-b)^{2l}}$$

y

$$\frac{E'(z)}{E(z)} = \frac{f'(z)}{f(z)} - \frac{l}{z-b}$$

de donde b es polo simple de $\frac{E'(z)}{E(z)}$ y $Res_{z=b} \frac{E'(z)}{E(z)} = -l$.

Así, concluímos que:

$$0 = \sum_{a \text{ ceros}} k_a - \sum_{b \text{ polos}} l_b.$$

■

DEFINICION 1.25 *El orden de una función elíptica es el número de polos que tiene en P (cada polo contado de acuerdo a su multiplicidad).*

TEOREMA 1.26 *Una función elíptica no constante de orden h toma en P cualquier valor complejo exactamente h veces.*

Demostración: Sea $c \in \mathbf{C}$ y $F(z) = E(z) - c$, así $F(z)$ tiene los mismos polos que $E(z)$ y en estos la misma parte principal que $E(z)$, por lo tanto $F(z)$ también es elíptica de orden h y sus ceros son las raíces de $E(z) = c$ con la misma multiplicidad en cada caso. Pero por el teorema 1.24, $F(z)$ tiene h ceros (contando multiplicidades).

■

TEOREMA 1.27 *Sean $a_1, a_2, \cdots, a_h$ los ceros y $b_1, b_2, \cdots, b_h$ los polos de la función elíptica no constante $E(z)$ en P, cada uno contado de acuerdo a su multiplicidad. La suma de los ceros de $E(z)$ en P difiere de la suma de los polos en un periódo.*

Demostración: Consideremos $G(z) = z\frac{E'(z)}{E(z)}$ la cual es analítica en $\overline{P}$ salvo, posiblemente, para los puntos donde $E(z)$ tiene ceros o polos. Razonando como en la demostración del teorema 1.24 se tiene que si a es un cero de $E(z)$ de orden k, entonces

$$G(z) = \frac{zk}{z-a} + \frac{zf'(z)}{f(z)} = k + \frac{ak}{z-a} + \frac{zf'(z)}{f(z)}$$

de modo que a es un polo de $G(z)$ con $Res_{z=a}G(z) = ak$ y si b es un polo de $E(z)$ de orden l, entonces

$$G(z) = \frac{zf'(z)}{f(z)} - \frac{zl}{z-b} = \frac{zf'(z)}{f(z)} - l - \frac{bl}{z-b}$$

de modo que b es un polo de $G(z)$ con $Res_{z=b}G(z) = -bl$.

Si asumimos que no hay ceros ni polos de $E(z)$ en L, entonces por el teorema de los residuos tenemos:

$$\frac{1}{2\pi i}\int_L G(z)\,dz = \sum_{a \text{ ceros}} ak - \sum_{b \text{ polos}} bl = \sum_{i=1}^{h} a_i - \sum_{i=1}^{h} b_i.$$

Si hacemos $w = \frac{1}{2\pi i}\int_L G(z)\,dz$, entonces

$$\begin{aligned} 2\pi i w &= \int_{C_1} z\frac{E'(z)}{E(z)}\,dz + \int_{C_2} z\frac{E'(z)}{E(z)}\,dz + \int_{C_3} z\frac{E'(z)}{E(z)}\,dz + \int_{C_4} z\frac{E'(z)}{E(z)}\,dz \\ &= \int_{C_1} z\frac{E'(z)}{E(z)}\,dz - \int_{C_4} (z+w_1)\frac{E'(z+w_1)}{E(z+w_1)}\,dz - \int_{C_1} (z+w_2)\frac{E'(z+w_2)}{E(z+w_2)}\,dz + \int_{C_4} z\frac{E'(z)}{E(z)}\,dz \end{aligned}$$

$$= -w_2 \int_{C_1} \frac{E'(z)}{E(z)}\,dz - w_1 \int_{C_4} \frac{E'(z)}{E(z)}\,dz = -w_2 \int_0^{w_1} \frac{E'(z)}{E(z)}\,dz - w_1 \int_{w_2}^0 \frac{E'(z)}{E(z)}\,dz$$
$$= w_1 \int_0^{w_2} \frac{E'(z)}{E(z)}\,dz - w_2 \int_0^{w_1} \frac{E'(z)}{E(z)}\,dz = w_1 \log E(z)]_0^{w_2} - w_2 \log E(z)]_0^{w_1}.$$

Dado que $E(0) = E(w_1)$, entonces $\log E(0) = \log E(w_1) + 2\pi i n_1$ con $n_1 \in \mathbf{Z}$ para cualquier rama fija del logaritmo. Similarmente $\log E(0) = \log E(w_2) + 2\pi i n_2$, con $n_2 \in \mathbf{Z}$ y por lo tanto $w = -n_2 w_1 + n_1 w_2$ es un periódo de $E(z)$.

Si hay ceros o polos de $E(z)$ sobre L movemos ésta como en el teorema 1.22.

■

CAPITULO 2. LAS FUNCIONES $\wp(z)$, $\zeta(z)$ Y $\sigma(z)$

La primera función elíptica con la que trataremos será la función $\wp(z)$ de Weierstrass cuya importancia se pondrá de manifiesto en el teorema 2.9. También estudiaremos la estrecha relación que existe entre las funciones $\wp(z)$, $\zeta(z)$ y $\sigma(z)$ (es importante resaltar el hecho de que éstas dos últimas funciones ya no son elípticas).

La función $\wp(z)$ y todo lo tratado aquí fue dado originalmente por K.Weierstrass. Fue G.Eisenstein quien descubrió que las funciones elípticas pueden ser generadas a partir de el producto infinito $\prod(1-\frac{z}{n})$. H.A. Schwarz introduce la función $\sigma(z)$ por medio de un producto infinito, así como la representación de $\wp(z)$ por medio de una serie.

DEFINICION 2.1 *Sean $w_1, w_2 \in \mathbf{C}$ ambos no cero y $\tau = \frac{w_2}{w_1}$, con $Im\tau > 0$. Sea S la latiz determinada por (w_1, w_2). Definimos para $\rho \in \mathbf{R}$:*

$$\sum_w{}' \frac{1}{|w|^\rho} = \sum_{\substack{w \in S \\ w \neq 0}} \frac{1}{|w|^\rho} = \sum_{\substack{(m,n) \in \mathbf{Z} \times \mathbf{Z} \\ (m,n) \neq (0,0)}} \frac{1}{|mw_1 + nw_2|^\rho}$$

TEOREMA 2.2 *La serie $\sum_w{}' |w|^{-\rho}$ converge para $\rho > 2$ y diverge para $\rho \leq 2$.*

Demostración: Sean $S_k = \sum'_{|m|,|n| \leq k} |w|^{-\rho}$, $T_k = S_k - S_{k-1}$ para $k \in \mathbf{N}$ y $S_0 = 0$. Observemos que $\sum_w{}' |w|^{-\rho}$ converge si, y sólo si, $\sum_{k=1}^{\infty} T_k$ converge (ya que como los sumandos de $\sum_w{}' |w|^{-\rho}$ son todos positivos se tiene que si esta converge, entonces también converge cualquier reordenamiento de ella; en particular ir sumando por "cuadrados"como en T_k).

Hay $(2k+1)^2 - 1$ términos en S_k y $(2(k-1)+1)^2 - 1$ términos en S_{k-1}, por lo tanto en T_k hay $(2k+1)^2 - (2k-1)^2 = 8k$ términos y cada uno de ellos es de la forma:

$$w = \pm k w_1 + n w_2, \quad |n| \leq k$$

ó

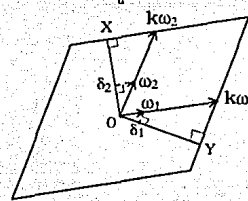
$$w = m w_1 \pm k w_2, \quad |m| \leq k$$

es decir

$$\underbrace{k(|w_1| + |w_2|)}_{b'} \geq \begin{cases} k|w_1| + |n||w_2| \geq |\pm k w_1 + n w_2| = |w| \\ \text{ó} \\ |m||w_1| + k|w_2| \geq |m w_1 \pm k w_2| = |w| \end{cases}$$

También, si X y Y son los ejes perpendiculares a w_1 y a w_2 respectivamente, δ_1 y δ_2 las proyecciones respectivas de w_1 sobre Y y de w_2 sobre X, entonces

$$\underbrace{k\,min\{\delta_1,\delta_2\}}_{a'} \leq |w|$$



Aquí a' y b' no dependen de k, por lo tanto para $0 < a < a'$ y $0 < b' < b$ se tiene que $ak < |w| < bk$. De donde

$$b^{-\rho}k^{-\rho} < |w|^{-\rho} < a^{-\rho}k^{-\rho}$$

y

$$8b^{-\rho}k^{1-\rho} < \sum_{\substack{w=nw_1+nw_2 \\ (|m|=k \ o \ |n|=k)}} |w|^{-\rho} < 8a^{-\rho}k^{1-\rho}$$

por tanto $\sum T_k$ converge si, y sólo si, $\sum_{k=1}^{\infty} k^{1-\rho}$ converge, lo cual sucede si, y sólo si, $\rho - 1 > 1$ es decir si, y sólo si, $\rho > 2$.

■

COROLARIO 2.3 *Para cualquier $R > 0$ y $z \in \mathbf{C}$, la serie $\sum_{\substack{w\in S \\ |w|>2R}} |z-w|^{-\rho}$ para $\rho > 2$ converge uniformemente en el círculo $|z| \leq R$. Así la serie $\sum_w |z-w|^{-\rho}$ con $\rho > 2$ converge uniformemente en cualquier círculo de radio finito si descartamos un número suficiente de términos iniciales.*

Demostración: Tomemos $|z| < R < \frac{1}{2}|w|$, así $|z| + |w| \leq \frac{3}{2}|w|$. Como $2|z| < |w|$, entonces $0 < |w| - 2|z|$ y por tanto

$$|w| < 2|w| - 2|z| = 2(|w| - |z|).$$

por consiguiente:

$$\frac{1}{|w-z|} \leq \frac{1}{|w|-|z|} \leq \frac{2}{|w|}$$

y

$$\frac{1}{|z-w|} \geq \frac{1}{|w|+|z|} \geq \frac{2}{3}\frac{1}{|w|}.$$

Por lo tanto para $\rho > 0$:

$$\left(\frac{2}{3}\right)^{\rho} \frac{1}{|w|^{\rho}} \leq \frac{1}{|z-w|^{\rho}} \leq \frac{2^{\rho}}{|w|^{\rho}}$$

y el resultado se sigue del teorema 2.2.

■

COROLARIO 2.4 *La serie* $\sum_{\substack{w\in S\\ w\neq 0}}\left\{\frac{1}{(z-w)^2}-\frac{1}{w^2}\right\}$ *converge absolutamente para* $z\notin S$ *y así la suma es independiente del orden de los términos. Para cualquier* $R>0$ *finito, la serie converge uniformemente en el círculo* $|z|\leq R$ *después de omitir un número suficiente de términos iniciales.*

Demostración: Dado $R>0$, tenemos que $|w|>2R$, $\forall w\in S$ excepto para un número finito de puntos $w\in S$. Si $|z|\leq R$, entonces $2|z|\leq 2R<|w|$. Por tanto $\left|\frac{z}{w}\right|<\frac{1}{2}$ y por consiguiente:

$$\left|2-\frac{z}{w}\right|\leq 2+\left|\frac{z}{w}\right|<2+\frac{1}{2}=\frac{5}{2}$$

y

$$\left|1-\frac{z}{w}\right|\geq 1-\left|\frac{z}{w}\right|>1-\frac{1}{2}=\frac{1}{2}$$

De donde $|1-\frac{z}{w}|^2>\frac{1}{4}$ y por tanto

$$\begin{aligned}\left|\frac{1}{(z-w)^2}-\frac{1}{w^2}\right| &= \left|\frac{z(2w-z)}{w^2(z-w)^2}\right| \\ &= \left|\frac{zw(2-\frac{z}{w})}{w^4(\frac{z}{w}-1)^2}\right| \quad \text{(pues } w\neq 0\text{)} \\ &= \frac{|z|}{|w|^3}\frac{|2-\frac{z}{w}|}{|1-\frac{z}{w}|^2} \\ &\leq 10\frac{|z|}{|w|^3}\leq 10\frac{R}{|w|^3}.\end{aligned}$$

Por el teorema 2.2 la serie $\sum_{\substack{w\in S\\ w\neq 0}}\frac{1}{|w|^{-3}}$ converge, por lo tanto $\sum_{\substack{w\in S\\ w\neq 0}}\left\{\frac{1}{(z-w)^2}-\frac{1}{w^2}\right\}$ converge absolutamente para $z\notin S$.

Así, $\sum_{\substack{w\in S\\ w\neq 0}}\left\{\frac{1}{(z-w)^2}-\frac{1}{w^2}\right\}$ converge uniformemente en $|z|\leq R$ si omitimos algunos de los términos iniciales (a saber sumandos con $|w|\leq 2R$).

■

DEFINICION 2.5 *Para* $z\in \mathbf{C}-S$ *definimos la función* $\wp(z)$ *de Weierstrass por:*

$$\wp(z)=\frac{1}{z^2}+\sum_{\substack{w\in S\\ w\neq 0}}\left\{\frac{1}{(z-w)^2}-\frac{1}{w^2}\right\}.$$

PROPOSICION 2.6 *La función* $\wp(z)$ *es elíptica con periodos primitivos* w_1, w_2*, polos dobles en los puntos* $w\in S$ *y tiene las siguientes propiedades:*

(i) La parte principal de $\wp(z)$ *en* $z=0$ *es* $\frac{1}{z^2}$.

(ii) $\lim_{z\to 0}\left(\wp(z)-\frac{1}{z^2}\right)=0$.

(iii) $\wp(z)=\wp(-z)$.

(iv) $\wp'(-z)=-\wp'(z)$.

Demostración: Por el corolario 2.4 la serie $\sum_{\substack{w\in S\\ w\neq 0}}\left\{\frac{1}{(z-w)^2}-\frac{1}{w^2}\right\}$ converge uniformemente en $|z|\leq R$ siempre que se omitan aquellos sumandos con $w\in S$ tales que $|w|\leq 2R$. Además $\frac{1}{(z-w)^2}-\frac{1}{w^2}$ es analítica en $|z|\leq R$ para $|w|>2R$. Por tanto, por el teorema de Weierstrass, $\wp(z)$ es analítica en $|z|\leq R$ para cualquier $R>0$, salvo en los puntos $w\in S$ donde tiene polos dobles. Así $\wp(z)$ es meromorfa con polos dobles en S.

(i) Tenemos que $\wp(z)-\frac{1}{z^2}=\sum_{\substack{w\in S\\ w\neq 0}}\left\{\frac{1}{(z-w)^2}-\frac{1}{w^2}\right\}$ es analítica en una vecindad alrededor de $z=0$ (que no contenga a ningún $w\in S$), por consiguiente $\frac{1}{z^2}$ es la parte principal de $\wp(z)$ en $z=0$.

(ii)

$$\lim_{z\to 0}\left\{\wp(z)-\frac{1}{z^2}\right\}=\lim_{z\to 0}\sum_{\substack{w\in S\\ w\neq 0}}\left\{\frac{1}{(z-w)^2}-\frac{1}{w^2}\right\}$$

$$=\sum_{\substack{w\in S\\ w\neq 0}}\lim_{z\to 0}\left\{\frac{1}{(z-w)^2}-\frac{1}{w^2}\right\}=0$$

(iii)

$$\wp(-z)=\frac{1}{(-z)^2}+\sum_{\substack{w\in S\\ w\neq 0}}\left\{\frac{1}{(-z-w)^2}-\frac{1}{w^2}\right\}$$

$$=\frac{1}{z^2}+\sum_{\substack{w\in S\\ w\neq 0}}\left\{\frac{1}{(z+w)^2}-\frac{1}{(-w)^2}\right\}$$

$$=\frac{1}{z^2}+\sum_{\substack{w\in S\\ w\neq 0}}\left\{\frac{1}{(z-(-w))^2}-\frac{1}{(-w)^2}\right\}=\wp(z),$$

ya que el conjunto $\{-w|w\in S, w\neq 0\}$ es el mismo que $\{w\in S|w\neq 0\}$.

(iv) Derivando en *(iii)* obtenemos: $\wp'(-z)=-\wp'(z)$.

Por el corolario 2.2 $\wp'(z)=-2\sum_{w\in S}\frac{1}{(z-w)^3}$ converge absolutamente para $z\notin S$ y dado que $\{w-w_1|w\in S\}$ es el mismo conjunto que S, se tiene $\wp'(z+w_1)=\wp'(z)$. Similarmente $\wp'(z+w_2)=\wp'(z)$, por lo tanto $\wp'(z)$ es elíptica. Integrando tenemos: $\wp(z+w_1)=\wp(z)+c$. Para $z=-\frac{w_1}{2}$, obtenemos: $\wp(\frac{w_1}{2})=\wp(-\frac{w_1}{2})+c$, y por (iii) $c=0$, de donde $\wp(z+w_1)=\wp(z)$. Igualmente $\wp(z+w_2)=\wp(z)$ y $\wp(z)$ es elíptica con periodos (w_1,w_2) y $Im\tau>0$ para $\tau=\frac{w_2}{w_1}$.

■

TEOREMA 2.7 *$\wp(z)$ satisface la ecuación diferencial:*

$$\wp'^2(z) = 4\wp^3(z) - g_2\wp(z) - g_3$$

donde $g_2 = 60\sum_{\substack{w\in S\\ w\neq 0}} w^{-4}$; $g_3 = 140\sum_{\substack{w\in S\\ w\neq 0}} w^{-6}$.

Demostración: Por el corolario 2.4: $\sum_{|w|>2R>0}\left\{\frac{1}{(z-w)^2} - \frac{1}{(w)^2}\right\}$ converge absoluta y uniformemente en $|z| \leq R$. Si $|w| > 2R \geq |z|$, desarrollando en serie de Taylor alrededor de $z = 0$ obtenemos:

$$\frac{1}{(z-w)^2} - \frac{1}{w^2} = \frac{2z}{w^3} + \frac{3z^2}{w^4} + \frac{4z^3}{w^5} + \frac{5z^4}{w^6} + \cdots$$

por lo tanto la expansión de $\wp(z)$ en serie de Laurent alrededor de $z = 0$ está dada por (recordando que $\wp(z)$ es par):

$$\begin{aligned}\wp(z) &= \frac{1}{z^2} + 3z^2\sum_{\substack{w\in S\\ w\neq 0}} w^{-4} + 5z^4\sum_{\substack{w\in S\\ w\neq 0}} w^{-6} + \cdots + (2n+1)z^{2n}\sum_{\substack{w\in S\\ w\neq 0}} w^{-(2n+2)}\\ &= \frac{1}{z^2} + b_1z^2 + b_2z^4 + \cdots + b_nz^{2n} + \cdots\end{aligned}$$

por consiguiente

$$\begin{aligned}\wp^3(z) &= z^{-6}(1 + b_1z^4 + b_2z^6 + \cdots + b_nz^{2n+2} + \cdots)^3\\ &= z^{-6}(1 + 3b_1z^4 + 3b_2z^6 + \cdots)\\ &= \frac{1}{z^6} + \frac{3b_1}{z^2} + 3b_2 + 3b_3z^2 + \cdots\end{aligned}$$

Pero derivando obtenemos:

$$\wp'(z) = -2z^{-3} + 2b_1z + 4b_2z^3 + 6b_3z^5 + \cdots$$

por tanto

$$\begin{aligned}\wp'^2(z) &= z^{-6}(-2 + 2b_1z^4 + 4b_2z^6 + \cdots)^2\\ &= z^{-6}(4 - 8b_1z^4 - 16b_2z^6 + \cdots)\\ &= \frac{4}{z^6} - \frac{8b_1}{z^2} - 16b_2 - 24b_3z^2 + \cdots\end{aligned}$$

luego

$$\wp'^2(z) - 4\wp^3(z) = -\frac{20b_1}{z^2} - 28b_2 + z^2P(z) = -\frac{g_2}{z^2} - g_3 + z^2P(z)$$

(con $P(z)$ un polinomio en z) tiene un polo de orden dos en $z = 0$, de donde

$$G(z) = \wp'^2(z) - 4\wp^3(z) + g_2\wp(z) + g_3$$

(que claramente es elíptica) es analítica en 0 y por tanto en todos los puntos de la latiz de periodos. Pero $G(z)$ no tiene polos y es analítica en P, por lo tanto $G(z) = c$.

Además, como

$$G(z) = g_2 \sum_{\substack{w \in S \\ w \neq 0}} \left\{ \frac{1}{(z-w)^2} - \frac{1}{w^2} \right\} + z^2 P(z)$$

es tal que $G(0) = 0$, entonces $\wp'^2(z) - 4\wp^3(z) + g_2\wp(z) + g_3 = 0$.

■

TEOREMA 2.8 *Sea P un paralelogramo de periodos asociado con $\wp(z)$. Sean a_k, b_ℓ con $k, \ell \in \{1, 2, \cdots, h\}$, $2h$ números complejos en P tales que $a_k \neq b_\ell$. Si $\sum_{k=1}^{h} a_k - \sum_{\ell=1}^{h} b_\ell = w$ es un periódo de $\wp(z)$, entonces existe una función elíptica que tiene en P justamente las a_k's como ceros y los b_ℓ's como polos; y cualesquiera dos de tales funciones difieren sólo por un factor constante no cero.*

Demostración: Sin pérdida de generalidad podemos suponer que el paralelogramo es $P = \{z | z = xw_1 + yw_2,\ 0 \leq x, y < 1\}$.

Si $E_1(z)$ y $E_2(z)$ son dos funciones elípticas con los ceros y polos preescritos en P, entonces $\frac{E_1(z)}{E_2(z)}$ es una función elíptica de orden 0 (ya que no tiene polos), por tanto $\frac{E_1(z)}{E_2(z)} = c \neq 0$.

Ahora demostraremos que existe $E(z)$ del tipo requerido.

Si $h = 0$, definimos $E(z) = 1$. El caso $h = 1$ no se puede dar, ya que $a_1 - b_1$ no puede ser un periódo si $a_1, b_1 \in P$. Así, sea $h \geq 2$.

Caso (i) Si $b_i = 0$, $\forall i \in \{1, \cdots, h\}$, tenemos que $\sum_i a_i = w$ es un periódo. Definimos $\forall r \in \mathbf{N}$ las siguientes funciones elípticas:

$$P_{2r}(z) = \wp^r(z),\ P_1(z) = 1,\ P_{2r+1}(z) = \wp'(z)\wp^{r-1}(z).$$

La función $P_n(z)$ para $n \geq 2$ tiene en P un polo en $z = 0$ de orden n (ya que $\wp(z)$ tiene en $z = 0$ un polo doble y $\wp'(z)$ un polo de orden 3). $P_1(z)$ no tiene polos.

Sean $\alpha_1, \alpha_2, \cdots, \alpha_q$ los números distintos entre sí en $\{a_k | k \in \{1, \cdots, h\}\}$ y sea n_ℓ el número de veces que se repite α_ℓ en él; así $n_1 + n_2 + \cdots + n_q = h$.

Definimos $E(z) = c_1P_1(z) + c_2P_2(z) + \cdots + c_hP_h(z)$ para algunas constantes $c_1, \cdots, c_h$, las cuales se eligirán de forma que las ecuaciones $E^{(k)}(\alpha_\ell) = 0$ con $\ell \in \{1, \cdots, q\}$, $k \in \{0, \cdots, n_\ell - 1\}$ sean satisfechas.

Con estas condiciones obtenemos $n_1 + n_2 + \cdots + n_q = h$ ecuaciones lineales homogéneas en las indeterminadas $c_1, \cdots, c_h$.

Para obtener una solución distinta de la trivial omitimos la última ecuación: $E^{(n_q-1)}(\alpha_q) = 0$ que corresponde al cero a_h. Este sistema consta de $h - 1$ ecuaciones en h incógnitas, por lo tanto tiene una solución no trivial $c_1, \cdots, c_h$.

Estas $c's$ satisfacen que α_ℓ es cero de multiplicidad n_ℓ, $\forall \ell \in \{1, \cdots, q-1\}$ y α_q es cero de multiplicidad n_{q-1}. Para ver que con estas $c's$ también α_q es un cero de multiplicidad

n_i, notemos que $E(z) = c_1P_1(z) + c_2P_2(z) + \cdots + c_hP_h(z)$ no es idénticamente cero (ya que $P_1(z), \cdots, P_h(z)$ tienen polos de diferentes ordenes en $z = 0$ y $P_1(z)$ es constante en todo punto) y tiene $h-1$ ceros en $a_1, a_2, \cdots, a_{h-1}$ y como el único polo de $E(z)$ en P es $z = 0$ con orden a lo más h, entonces el orden de $E(z)$ es h ó $h-1$.

Si fuera $h-1$ se tendría que $a_1, a_2, \cdots, a_{h-1}$ son todos los ceros de $E(z)$ en P y por el teorema 1.27: $a_1 + a_2 + \cdots + a_{h-1} - 0 = w^*$ es un periódo (ya que la suma de los polos es cero). Entonces $\sum a_i - w^* = w - w^* = a_h$ es también un periódo! (ya que $a_h \in P$ y $a_h \neq 0$ porque $a_k \neq b_\ell = 0$) por tanto el orden de $E(z)$ es h y $E(z)$ tiene h ceros en los puntos $a_1, a_2, \cdots, a_{h-1}, a$. Como $a_1 + \cdots + a_{h-1} + a - 0$ es un periódo (por el teorema 1.27) y por hipótesis $\sum a_i = w$ es un periódo, entonces $w - (a_1 + \cdots + a_{h-1} + a) = a_h - a$ es también un periódo en P; pero $a_h, a \in P$ de donde $a_h - a = 0$, por tanto $a_h = \alpha_q$ es cero de multiplicidad n_q y $E(z)$ tiene sus ceros en α_ℓ con ordenes n_ℓ, $\forall \ell \in \{1, \cdots, q\}$.

Para el caso $a_1 = \cdots = a_h = 0$, reemplazamos las $a'_k s$ por las $b'_k s$ en el caso anterior para construir $E(z)$ y la función requerida será $\frac{1}{E(z)}$.

Caso (ii) Supondremos que no todas las $a'_k s$ ni todas las $b'_k s$ son cero.

Escojamos $a_0 \in P$ tal que $a_0 + a_1 + \cdots + a_h$ sea un periódo. Si hacemos $b_0 = a_0$, entonces dado que $\sum_{i=1}^{h} a_i - \sum_{k=1}^{h} b_k = w$ se tiene: $\sum_{i=0}^{h} a_i - \sum_{k=0}^{h} b_k = w$ y por tanto $\sum_{k=0}^{h} b_k = \sum_{i=0}^{h} a_i - w$ es un periódo.

Si m de los $h+1$ números $a_0, a_1, \cdots, a_h$ son cero y n de los $h+1$ números $b_0, b_1, \cdots, b_h$ son cero, entonces $m, n < h+1$. Si quitamos aquellas $a'_k s$ que son cero seguimos teniendo que la suma de las $h+1-m$ restantes $a'_k s$ es un periódo. Construyamos $E_1(z) = c_1P_1(z) + c_2P_2(z) + \cdots + c_\mu P_\mu(z)$ como en el *caso (i)* con constantes $c_1, c_2, \cdots, c_\mu$ con $c_\mu \neq 0$, $\mu = h+1-m > 1$ y ceros en P en $a_k \neq 0$ y un polo en $z = 0$ de orden μ.

Igualmente construyamos $E_2(z) = d_1P_1(z) + d_2P_2(z) + \cdots + d_\nu P_\nu(z)$ con constantes $d_1, d_2, \cdots, d_\nu$ con $d_\nu \neq 0$, $\nu = h+1-n > 1$, ceros en P en $b_\ell \neq 0$ y un polo en $z = 0$ de orden ν.

Sea $E(z) = \frac{E_1(z)}{E_2(z)}$. Si $a_0 \neq 0$, entonces dado que $a_0 = b_0$, éste es un cero común de $E_1(z)$ y $E_2(z)$. Si $a_0 = 0$ no estamos añadiendo nada. Para $a_k \neq 0$ $(k > 0)$, estos son ceros de $E_1(z)$. Similarmente los $b_\ell \neq 0$ $(\ell > 0)$ son ceros de $E_2(z)$ y por tanto

$$\begin{aligned} E(z) = \frac{E_1(z)}{E_2(z)} &= \frac{z^{-\mu} f_1(z)}{z^{-\nu} f_2(z)} \\ &= \frac{z^{\nu-\mu} f_1(z)}{f_2(z)} \\ &= \frac{z^{m-n} f_1(z)}{f_2(z)}. \end{aligned}$$

Si $m > n$, $z = 0$ es cero de orden $m - n$ de $E(z)$.

Si $m < n$, $z = 0$ es polo de orden $n - m$ de $E(z)$.

Si $m = n$, $z = 0$ no es polo ni cero de $E(z)$. Así $E(z)$ es la función buscada.

■

El siguiente teorema nos dice como son todas las funciones elípticas en términos de la función $\wp(z)$ y su derivada.

TEOREMA 2.9 *Toda función elíptica puede ser expresada en forma única como:*

$$E(z) = S(\wp(z)) + \wp'(z)T(\wp(z))$$

con $S(\wp(z))$ y $T(\wp(z))$ funciones racionales de $\wp(z)$ con coeficientes constantes. Inversamente toda expresión de la forma $S(\wp(z)) + \wp'(z)T(\wp(z))$ es una función elíptica.

Demostración: Sea h el orden de $E(z)$.

Si $h = 0$, entonces $E(z) = c$, así tomamos $S(\wp(z)) = c$ y $T(\wp(z)) = 0$

Si $h > 0$, sean $a_i, a_2, \cdots, a_h$ los ceros y $b_1, b_2, \cdots, b_h$ los polos de $E(z)$ en P. Entonces $\sum_{i=1}^{h} a_i - \sum_{i=1}^{h} b_i = w$ es un periódo (por el teorema 1.27).

Como en el teorema 2.8 construyamos:

$$E_1'(z) = c_1 P_1(z) + c_2 P_2(z) + \cdots + c_h P_h(z),$$

$$E_2(z) = d_1 P_1(z) + d_2 P_2(z) + \cdots + d_h P_h(z)$$

tales que $E(z) = c\frac{E_1'(z)}{E_2(z)}$.

Si tomamos $E_1(z) = cE_1'(z)$, entonces $E(z) = \frac{E_1(z)}{E_2(z)}$.

Pero $E_1(z) = A(\wp(z)) + \wp'(z)B(\wp(z))$, $E_2(z) = C(\wp(z)) + \wp'(z)D(\wp(z))$, con $A(\wp(z)), B(\wp(z))$, $C(\wp(z)), D(\wp(z))$ polinomios en $\wp(z)$ con coeficientes constantes dada la definición de $P_n(z)$ en el teorema 2.8.

Sea $E_0(z) = C(\wp(z)) - \wp'(z)D(\wp(z))$ la cual no puede anularse idénticamente en z, ya que $C(\wp(z))$ es una función par de z y $\wp'(z)D(\wp(z))$ es una función impar de z.

Así tenemos:

$$E_0(z)E_1(z) = C(\wp(z))A(\wp(z)) + \wp'(z)(C(\wp(z))B(\wp(z)) - D(\wp(z))A(\wp(z))) - \wp'(z)^2 D(\wp(z))B(\wp(z))$$

$$= C(\wp(z))A(\wp(z)) + \wp'(z)(C(\wp(z))B(\wp(z)) - D(\wp(z))A(\wp(z))) + (-4\wp(z)^3 + g_2\wp(z) + g_3)(D(\wp(z))B(\wp(z)))$$

(por el teorema 2.7) por tanto $E_0(z)E_1(z) = A_1(\wp(z)) + \wp'(z)B_1(\wp(z))$ con $A_1(\wp(z)), B_1(\wp(z))$ polinomios en $\wp(z)$.

De igual forma

$$\begin{aligned} E_0(z)E_2(z) &= C^2(\wp(z)) - \wp'(z)^2 D^2(\wp(z)) \\ &= C^2(\wp(z)) - (4\wp(z)^3 - g_2\wp(z) - g_3)D^2(\wp(z)) = C_1(\wp(z)) \end{aligned}$$

polinomio en $\wp(z)$ no idénticamente cero.

Haciendo $S(\wp(z)) = \frac{A_1(\wp(z))}{C_1(\wp(z))}$, $T(\wp(z)) = \frac{B_1(\wp(z))}{C_1(\wp(z))}$ tenemos: $E(z) = \frac{E_1(z)}{E_2(z)} = S(\wp(z)) + \wp'(z)T(\wp(z))$.

Para ver la unicidad supongamos que también $E(z) = S^*(\wp(z)) + \wp'(z)T^*(\wp(z))$, si definimos $S_0(z) = S(\wp(z)) - S^*(\wp(z))$ y $T_0(z) = T(\wp(z)) - T^*(\wp(z))$, entonces tenemos que $S_0(\wp(z)) + \wp'(z)T_0(\wp(z)) = 0$. Como $\wp(z)$ es par y $\wp'(z)$ es impar, entonces $S_0(\wp(z)) - \wp'(z)T_0(\wp(z)) = 0$. Por tanto $2S_0(\wp(z)) = 0$ y $S_0(\wp(z)) = 0$, de donde $\wp'(z)T_0(\wp(z)) = 0$. Pero $\wp'(z)$ no es idénticamente cero, luego $T_0(\wp(z)) = 0$.

Finalmente dado que las funciones elípticas con un par de periodos básicos (w_1, w_2) forman un campo, se tiene que $S(\wp(z)) + \wp'(z)T(\wp(z))$ es una función elíptica para $S(\wp(z))$ y $T(\wp(z))$ funciones racionales de $\wp(z)$ con coeficientes constantes.

■

PROPOSICION 2.10 *La serie* $\sum_{|w|>2R>0} \left\{ \frac{1}{z-w} + \frac{1}{w} + \frac{z}{w^2} \right\}$ *converge uniformemente en* $|z| \leq R$, *para* $R > 0$ *fijo.*

Demostración: Tenemos $|w| > 2R \geq 2|z|$, por lo tanto:

$$\begin{aligned} \left| \frac{1}{z-w} + \frac{1}{w} + \frac{z}{w^2} \right| &= \frac{|z|^2}{|1 - \frac{z}{w}||w^3|} \\ &\leq \frac{|z|^2}{\left(1 - \frac{|z|}{|w|}\right)|w^3|} \leq 2\frac{|z|^2}{|w|^3} \quad \text{(ya que } 2|z| \leq |w|\text{)} \\ &\leq 2\frac{R^2}{|w|^3}. \end{aligned}$$

y dado que $\sum_{\substack{w \in S \\ w \neq 0}} |w|^{-3}$ converge, se tiene el resultado.

■

De la proposición 2.10 se sigue que la serie

$$\frac{1}{z} + \sum_{\substack{w \in S \\ w \neq 0}} \left\{ \frac{1}{z-w} + \frac{1}{w} + \frac{z}{w^2} \right\}$$

converge absolutamente para $z \notin S$. Y para $R > 0$ finito converge uniformemente en $|z| \leq R$, después de omitir un cierto número de términos iniciales.

DEFINICION 2.11 *Definimos* $\forall z \in \mathbf{C} - S$:

$$\zeta(z) = \frac{1}{z} + \sum_{\substack{w \in S \\ w \neq 0}} \left\{ \frac{1}{z-w} + \frac{1}{w} + \frac{z}{w^2} \right\}$$

con $Im\frac{w_2}{w_1} > 0$.

OBSERVACION: $\zeta(z)$ es analítica excepto en $z = w$, donde tiene un polo simple con residuo 1 y por tanto $\zeta(z)$ no es elíptica. También observemos que $\zeta(-z) = -\zeta(z)$.

TEOREMA 2.12 *Se tiene:*

$$\zeta'(z) = -\wp(z)$$

$$\zeta(z + w_i) = \zeta(z) + 2\eta_i,$$

donde (w_1, w_2) *es un par de periodos básicos,* $w_3 = w_1 + w_2$ *y* $\eta_i = \zeta\left(\frac{w_i}{2}\right)$ *para* $i \in \{1, 2, 3\}$.

Demostración: Tenemos:

$$\zeta'(z) = -\frac{1}{z^2} + \sum_{\substack{w \in S \\ w \neq 0}} \left\{ -\frac{1}{(z-w)^2} + \frac{1}{w^2} \right\}$$

$$= -\left(\frac{1}{z^2} + \sum_{\substack{w \in S \\ w \neq 0}} \left\{ \frac{1}{(z-w)^2} - \frac{1}{w^2} \right\} \right)$$

$$= -\wp(z).$$

Integrando $\wp(z + w_1) = \wp(z)$ obtenemos: $\zeta(z + w_1) = \zeta(z) + 2\eta_1$

Para $z = -\frac{w_1}{2}$ tenemos:

$$\zeta\left(\frac{w_1}{2}\right) = \zeta\left(-\frac{w_1}{2}\right) + 2\eta_1 = -\zeta\left(\frac{w_1}{2}\right) + 2\eta_1,$$

de donde $\eta_1 = \zeta\left(\frac{w_1}{2}\right)$.

Análogamente se tiene:

$$\zeta(z + w_2) = \zeta(z) + 2\eta_2.$$

Como

$$\begin{aligned} \zeta(z + w_3) &= \zeta(z + w_1 + w_2) \\ &= \zeta(z) + 2(\eta_1 + \eta_2) \\ &= \zeta(z) + 2\left(\zeta\left(\frac{w_1}{2}\right) + \zeta\left(\frac{w_2}{2}\right)\right) \end{aligned}$$

y

$$\begin{aligned} \zeta\left(\frac{w_1 + w_2}{2}\right) &= \zeta\left(w_1 + w_2 - \left(\frac{w_1 + w_2}{2}\right)\right) \\ &= \zeta\left(-\left(\frac{w_1 + w_2}{2}\right)\right) + 2(\eta_1 + \eta_2) \\ &= -\zeta\left(\frac{w_1 + w_2}{2}\right) + 2\eta_3 \quad \text{(haciendo } \eta_3 = \eta_1 + \eta_2\text{)} \end{aligned}$$

entonces

$$\zeta\left(\frac{w_1 + w_2}{2}\right) = \eta_3.$$

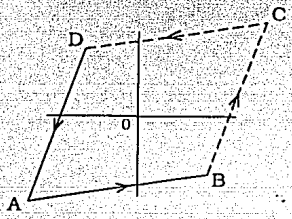
■

TEOREMA 2.13 *(Legendre) Si (w_1, w_2) es un par de periodos básicos de $\wp(z)$ con $Im\frac{w_2}{w_1} > 0$, entonces*

$$\pi i = \eta_1 w_2 - \eta_2 w_1,$$

con η_1 y η_2 como en el teorema anterior.

Demostración: Tomemos un paralelogramo de periodos de $\wp(z)$ con vértices A, B, C, D y de forma que el origen (es decir el polo $z = 0$) sea su centro.



Por el teorema del residuo de Cauchy:

$$\frac{1}{2\pi i}\int_{ABCDA} \zeta(z)\,dz = Res_{z=0}\zeta(z) = 1$$

Pero por el teorema 2.12 tenemos:

$$\begin{aligned}\int_{CD} \zeta(z)\,dz &= \int_{BA} \zeta(z + w_2)\,dz \\ &= \int_{BA} \zeta(z)\,dz + 2\eta_2 \int_{BA} dz \\ &= \int_{BA} \zeta(z)\,dz + 2\eta_2 \int_{\frac{w_1}{2}}^{-\frac{w_1}{2}} dz \\ &= \int_{BA} \zeta(z)\,dz + 2\eta_2(-w_1)\end{aligned}$$

por lo tanto

$$\int_{AB} \zeta(z)\,dz + \int_{CD} \zeta(z)\,dz = -2\eta_2 w_1.$$

En forma similar

$$\int_{BC} \zeta(z)\,dz + \int_{DA} \zeta(z)\,dz = 2\eta_1 w_2$$

de donde

$$2\pi i = \int_{ABCDA} \zeta(z)\,dz = -2\eta_2 w_1 + 2\eta_1 w_2$$

y por tanto $\pi i = \eta_1 w_2 - \eta_2 w_1$.

■

DEFINICION 2.14 *Definimos para* $z \in \mathbf{C}$:

$$\sigma(z) = z \prod_{\substack{w \in S \\ w \neq 0}} \left(1 - \frac{z}{w}\right) e^{\frac{z}{w} + \frac{1}{2}\left(\frac{z}{w}\right)^2}.$$

La cual es una función entera de z que no es constante y por lo tanto $\sigma(z)$ no es elíptica. Observemos que $\sigma(-z) = -\sigma(z)$ y que tiene ceros simples en $w \in S$.

TEOREMA 2.15 *Se tienen las siguientes propiedades:*

$$\zeta(z) = \frac{\sigma'(z)}{\sigma(z)} \quad \forall z \notin S$$

$$\sigma(z + w_i) = -\sigma(z)\, e^{2\eta_i\left(z + \frac{w_i}{2}\right)}$$

para $i \in \{1, 2, 3\}$ *y con* w_i, η_i *como en el teorema 2.12.*

Demostración: Para $z \notin S$ y $\operatorname{Log} z$ la rama principal de la función logaritmo, tenemos:

$$\begin{aligned}
\frac{\sigma'(z)}{\sigma(z)} &= \frac{d}{dz}\left(\operatorname{Log}\sigma(z) + 2\pi i n\right) \quad (\text{con } n \in \mathbf{Z}) \\
&= \frac{d}{dz}\left(\operatorname{Log} z + \sum_{w \neq 0}\left\{\operatorname{Log}\left(1 - \frac{z}{w}\right) + \frac{z}{w} + \frac{1}{2}\left(\frac{z}{w}\right)^2\right\}\right) \\
&= \frac{1}{z} + \sum_{w \neq 0}\left\{\frac{1}{\left(1 - \frac{z}{w}\right)}\left(-\frac{1}{w}\right) + \frac{1}{w} + \frac{z}{w^2}\right\} \\
&= \frac{1}{z} + \sum_{w \neq 0}\left\{\frac{1}{z - w} + \frac{1}{w} + \frac{z}{w^2}\right\} = \zeta(z)
\end{aligned}$$

De $\zeta(z + w_1) = \zeta(z) + 2\eta_1$, obtenemos al integrar:

$$\operatorname{Log}(\sigma(z + w_1)) = \operatorname{Log}\sigma(z) + 2\eta_1 z + c_1$$

de donde

$$\sigma(z + w_1) = \sigma(z)\, e^{2\eta_1 z}\, e^{c_1} = c\, e^{2\eta_1 z}\, \sigma(z)$$

haciendo $z = -\frac{w_1}{2}$, obtenemos:

$$\sigma\left(\frac{w_1}{2}\right) = -c\, e^{-\eta_1 w_1}\, \sigma\left(\frac{w_1}{2}\right)$$

por lo tanto $c = -e^{\eta_1 w_1}$ y $\sigma(z + w_1) = -e^{2\eta_1\left(z + \frac{w_1}{2}\right)}\sigma(z)$.

En forma similar se obtiene $\sigma(z + w_2) = -e^{2\eta_2\left(z + \frac{w_2}{2}\right)}\sigma(z)$ y $\sigma(z + w_3) = -e^{2\eta_3\left(z + \frac{w_3}{2}\right)}\sigma(z)$.

■

TEOREMA 2.16 *Sea $f(z)$ una función elíptica con (w_1, w_2) un par de periodos reducidos. Sean $a_1, a_2, \cdots, a_n$ los ceros y $b_1, b_2, \cdots, b_n$ los polos de $f(z)$ en P (contados de acuerdo a su multiplicidad) con $\sum_{i=1}^{n} a_i - \sum_{i=1}^{n} b_i = w$ (I) un periódo de $f(z)$. Entonces*

$$f(z) = c\frac{\sigma(z-a_1)\cdots\sigma(z-a_n)}{\sigma(z-b_1)\cdots\sigma(z-b_n-w)}, \text{ con } c \text{ una constante.}$$

Inversamente cualquier función de esta forma con los $a_i's$ y $b_i's$ tales que satisfacen (I) es una función elíptica.

Demostración: La función meromorfa

$$\varphi(z) = \frac{\sigma(z-a_1)\cdots\sigma(z-a_n)}{\sigma(z-b_1)\cdots\sigma(z-b_n-w)}$$

tiene precisamente los mismos ceros y polos que $f(z)$ en P, ya que $c_k \in \{a_k, b_k | 1 \leq k \leq n\}$ es el único cero de $\sigma(z-c_k)$ en P y $\sigma(z)$ es entera (para $k = n$ tenemos: $\sigma(b_n - b_n - w) = \sigma(-w) = -\sigma(w) = 0$).

Además por el teorema 2.15:

$$\begin{aligned}
\varphi(z+w_1) &= \frac{\sigma(z-a_1+w_1)\cdots\sigma(z-a_n+w_1)}{\sigma(z-b_1+w_1)\cdots\sigma(z-b_n-w+w_1)} \\
&= \frac{(-1)^n\, e^{2\eta_1(z-a_1+\frac{w_1}{2})+\cdots+2\eta_1(z-a_n+\frac{w_1}{2})}\,\sigma(z-a_1)\cdots\sigma(z-a_n)}{(-1)^n\, e^{2\eta_1(z-b_1+\frac{w_1}{2})+\cdots+2\eta_1(z-b_n-w+\frac{w_1}{2})}\,\sigma(z-b_1)\cdots\sigma(z-b_n-w)} \\
&= \frac{e^{2\eta_1(nz-a_1-\cdots-a_n+n\frac{w_1}{2})}\,\sigma(z-a_1)\cdots\sigma(z-a_n)}{e^{2\eta_1(nz-b_1-\cdots-b_n-w+n\frac{w_1}{2})}\,\sigma(z-b_1)\cdots\sigma(z-b_n-w)} \\
&= \frac{e^{2\eta_1(nz-a_1-\cdots-a_n+n\frac{w_1}{2})}\,\sigma(z-a_1)\cdots\sigma(z-a_n)}{e^{2\eta_1(nz-a_1-\cdots-a_n+n\frac{w_1}{2})}\,\sigma(z-b_1)\cdots\sigma(z-b_n-w)} \\
&= \varphi(z).
\end{aligned}$$

De igual forma $\varphi(z+w_2) = \varphi(z)$. Así, $\frac{f(z)}{\varphi(z)}$ es una función doblemente periódica sin polos y ceros, por tanto $\frac{f(z)}{\varphi(z)} = c$ constante.

Inversamente, si las $a_i's$ y $b_i's$ satisfacen (I), entonces $\varphi(z+w_1) = \varphi(z+w_2) = \varphi(z)$ y por tanto $\varphi(z)$ es elíptica.

■

CAPITULO 3. LAS FUNCIONES THETA

En este capítulo definiremos la función theta de Weiertrass en forma de una serie infinita junto con otras tres funciones theta muy similares. En el teorema 3.6 veremos la relación que guarda con la función sigma del capítulo 2. Finalmente la fórmula que nos permitirá demostrar la Ley de Reciprocidad Cuadrática en el próximo capítulo será la fórmula de transformación del teorema 3.8 para la función θ_3. La primera de las funciones tipo theta que apareció en análisis fue la función partición $\prod_{n=1}^{\infty}(1-x^n z)^{-1}$ de Euler. En sí, las funciones theta aparecieron en la "Teoría Analítica del Calor"de J.Fourier, y el estudio de éstas funciones fue desarrollada a partir de la teoría de las funciones elípticas por Jacobi en sus "Fundamenta Nova", obteniendo por métodos puramente algebraicos muchos de los resultados de este capítulo, descubriendo también las expresiones en forma de productos para las funciones theta. El mismo Jacobi fue quien obtuvo la fórmula de transformación a partir de la teoría de las funciones elípticas. La primera prueba directa de esta fórmula por medio de integrales de contorno se debe a G.Landsberg.

DEFINICION 3.1 *Sea* $v \in \mathbf{C}$, $q = e^{\pi i \tau}$ *con* $Im\tau > 0$. *Definimos la función* θ *como:*

$$\theta(v,\tau) = \frac{1}{i}\sum_{n=-\infty}^{\infty}(-1)^n q^{(n+\frac{1}{2})^2} e^{(2n+1)\pi i v}.$$

PROPOSICION 3.2 *La función* $\theta(v,\tau)$ *converge absoluta y uniformemente en cualquier subconjunto compacto del* v*-plano y entonces representa una función entera de* v *para* τ *fija.*

Demostración: Dado que $|q| = e^{-\pi Im\tau} < 1$ (ya que $Im\tau > 0$), entonces

$$|q^{(n+\frac{1}{2})^2} e^{\pm i(2n+1)\pi v}| \leq |q|^{\frac{1}{4}(2n+1)^2} e^{|(2n+1)\pi v|}$$

por tanto si consideramos τ fija, tenemos que en un subconjunto compacto del v-plano: $e^{|\pi v|} \leq M$ y por el criterio de la ràiz $\lim_{n\to\infty}\sqrt[n]{|q|^{\frac{1}{4}n^2}M^n} = M\lim_{n\to\infty}|q|^{\frac{1}{4}n} \to 0$ (pues $|q|<1$), luego $\sigma(v,\tau)$ es absolutamente convergente.

■

TEOREMA 3.3 *Se tienen las propiedades:*

(i)

$$\theta(v,\tau) = 2\sum_{n=0}^{\infty}(-1)^n q^{(n+\frac{1}{2})^2}\operatorname{sen}((2n+1)\pi v),$$

(ii)

$$\theta(v+1,\tau) = -\theta(v,\tau),$$

(iii)

$$\theta(v+\tau,\tau) = -q^{-1}\,e^{-2\pi i v}\,\theta(v,\tau)$$

(iv) Los puntos de la forma $\{m_1+m_2\tau | m_1, m_2 \in \mathbf{Z}\}$ *son los únicos ceros de* θ.

Demostración: *(i)* Como $e^{-(2n+1)\pi i v} = e^{(2(-(n+1))+1)\pi i v}$ y $q^{(-(n+1)+\frac{1}{2})^2} = q^{(n+\frac{1}{2})^2}$, tenemos:

$$\begin{aligned}\theta(v,\tau) &= \frac{1}{i}\sum_{n=0}^{\infty}\left\{(-1)^n q^{(n+\frac{1}{2})^2} e^{(2n+1)\pi i v} + (-1)^{-(n+1)} q^{(-(n+1)+\frac{1}{2})^2} e^{(2(-(n+1))+1)\pi i v}\right\}\\ &= \frac{1}{i}\sum_{n=0}^{\infty}(-1)^n q^{(n+\frac{1}{2})^2}\left(e^{(2n+1)\pi i v} - e^{-(2n+1)\pi i v}\right)\\ &= 2\sum_{n=0}^{\infty}(-1)^n q^{(n+\frac{1}{2})^2}\operatorname{sen}((2n+1)\pi v)\end{aligned}$$

(ii)

$$\begin{aligned}\theta(v+1,\tau) &= \frac{1}{i}\sum_{n=-\infty}^{\infty}(-1)^n q^{(n+\frac{1}{2})^2} e^{(2n+1)\pi i v} e^{(2n+1)\pi i}\\ &= \frac{1}{i}\sum_{n=-\infty}^{\infty}(-1)^n q^{(n+\frac{1}{2})^2} e^{(2n+1)\pi i v}(-1)\\ &= -\theta(v,\tau)\end{aligned} \tag{1}$$

(iii)

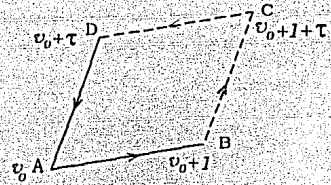
$$\begin{aligned}\theta(v+\tau,\tau) &= \frac{1}{i}\sum_{n=-\infty}^{\infty}(-1)^n q^{(n+\frac{1}{2})^2} e^{(2n+1)\pi i(v+\tau)}\\ &= \frac{1}{i}\sum_{n=-\infty}^{\infty}(-1)^n q^{(n+\frac{1}{2})^2} e^{(2n+1)\pi i v}\, q^{(2n+1)}\\ &= \frac{1}{i}\sum_{m=-\infty}^{\infty}(-1)^{m-1} q^{(m-\frac{1}{2})^2+(2m-1)} e^{(2m-1)\pi i v}\\ &= \frac{1}{i}\sum_{m=-\infty}^{\infty}(-1)(-1)^m q^{(m+\frac{1}{2})^2} q^{-1} e^{(2m+1)\pi i v} e^{-2\pi i v}\\ &= -q^{-1} e^{-2\pi i v}\,\theta(v,\tau)\end{aligned} \tag{2}$$

(iv) Si $m_1, m_2 \in \mathbf{Z}$, entonces:

$$\begin{aligned}\theta(m_1+m_2\tau,\tau) &= (-1)^{m_2} q^{-m_2} e^{-2m_2\pi i m_1}\,\theta(m_1,\tau) \quad \text{por (2)}\\ &= (-1)^{m_2} q^{-m_2} e^{-2m_2\pi i m_1}(-1)^{m_1}\theta(0,\tau) = 0 \quad \text{por (1)}.\end{aligned}$$

Para ver que $\{m_1 + m_2\tau\}$ son los únicos ceros, sea $ABCD$ el paralelogramo en el v-plano de vértices A, B, C, D localizados en $v_0, v_0+1, v_0+1+\tau, v_0+\tau$, donde v_0 no es cero de $\theta(v,\tau)$. Veremos que $\theta(v,\tau)$ tiene sólo un cero en el paralelogramo $ABCD$.

Consideremos $\int_{ABCD} \frac{\theta'(v,\tau)}{\theta(v,\tau)}dv$ sobre la curva orientada positivamente.



Derivando $\theta(v+\tau,\tau)$ con respecto a v, tenemos:

$$\theta'(v+\tau,\tau) = -q^{-1}e^{-2\pi iv}\theta'(v,\tau) + 2\pi i \underbrace{q^{-1}e^{-2\pi iv}\theta(v,\tau)}_{-\theta(v+\tau,\tau)}$$

por tanto

$$\frac{\theta'(v+\tau,\tau)}{\theta(v+\tau,\tau)} = \frac{\theta'(v,\tau)}{\theta(v,\tau)} - 2\pi i$$

y como de *(ii)* se tiene:

$$\frac{\theta'(v+1,\tau)}{\theta(v+1,\tau)} = \frac{-\theta'(v,\tau)}{-\theta(v,\tau)} = \frac{\theta'(v,\tau)}{\theta(v,\tau)}$$

entonces

$$\left(\int_{BC} + \int_{DA}\right)\frac{\theta'(v,\tau)}{\theta(v,\tau)}dv = 0$$

y

$$\left(\int_{AB} + \int_{CD}\right)\frac{\theta'(v,\tau)}{\theta(v,\tau)}dv = 2\pi i$$

por consiguiente

$$\frac{1}{2\pi i}\int_{ABCD}\frac{\theta'(v,\tau)}{\theta(v,\tau)}dv = 1$$

por tanto $\theta(v,\tau)$ sólo tiene un cero en $ABCD$ y como sólo existe un número de la forma $m_1 + m_2\tau$ dentro de $ABCD$ y tal punto es un cero de $\theta(v,\tau)$, se sigue el resultado.

■

DEFINICION 3.4 *Sea* $q = e^{\pi i\tau}$, $Im\tau > 0$ *y* $v \in \mathbf{C}$, *definimos:*

$$\theta_1(v,\tau) = \sum_{n=-\infty}^{\infty} q^{\left(n+\frac{1}{2}\right)^2} e^{(2n+1)\pi iv},$$

$$\theta_2(v,\tau) = \sum_{n=-\infty}^{\infty} (-1)^n q^{n^2} e^{2n\pi iv},$$

$$\theta_3(v,\tau) = \sum_{n=-\infty}^{\infty} q^{n^2} e^{2n\pi i v}.$$

Similarmente a θ, para τ fijo, estas son funciones enteras de v.

PROPOSICION 3.5 *Se tienen las siguientes relaciones:*

(i)

$$\theta(v,\tau) = \theta_3\left(v+\frac{1}{2}+\frac{\tau}{2},\tau\right) q^{\frac{1}{4}} e^{\pi i v} \frac{1}{i},$$

(ii)

$$\theta_1(v,\tau) = \theta_3\left(v+\frac{\tau}{2},\tau\right) q^{\frac{1}{4}} e^{\pi i v},$$

(iii)

$$\theta_2(v,\tau) = \theta_3\left(v+\frac{1}{2},\tau\right).$$

Demostración: *(i)*

$$\begin{aligned}
\theta_3\left(v+\frac{1}{2}+\frac{\tau}{2},\tau\right) q^{\frac{1}{4}} e^{\pi i v}(-i) &= (-i) \sum_{n=-\infty}^{\infty} q^{n^2+\frac{1}{4}+n} e^{2n\pi i\left(v+\frac{1}{2}\right)+\pi i v} \\
&= (-i) \sum_{n=-\infty}^{\infty} q^{\left(n+\frac{1}{2}\right)^2} e^{(2n+1)\pi i v} e^{n\pi i} \\
&= (-i) \sum_{n=-\infty}^{\infty} q^{\left(n+\frac{1}{2}\right)^2} e^{(2n+1)\pi i v}(-1)^n \\
&= \theta(v,\tau).
\end{aligned}$$

(ii)

$$\begin{aligned}
\theta_3\left(v+\frac{\tau}{2},\tau\right) q^{\frac{1}{4}} e^{\pi i v} &= \sum_{n=-\infty}^{\infty} q^{n^2+\frac{1}{4}} e^{2n\pi i\left(v+\frac{\tau}{2}\right)+\pi i v} \\
&= \sum_{n=-\infty}^{\infty} q^{\left(n+\frac{1}{2}\right)^2} e^{(2n+1)\pi i v} \\
&= \theta_1(v,\tau).
\end{aligned}$$

(iii)

$$\begin{aligned}
\theta_3\left(v+\frac{1}{2},\tau\right) &= \sum_{n=-\infty}^{\infty} q^{n^2} e^{2n\pi i\left(v+\frac{1}{2}\right)} \\
&= \sum_{n=-\infty}^{\infty} q^{n^2} e^{2n\pi i v}(-1)^n \\
&= \theta_2(v,\tau).
\end{aligned}$$

■

Ahora examinaremos la conexión entre las funciones θ y σ.

TEOREMA 3.6 *Se tiene:*

$$\sigma(z) = \theta\left(\frac{z}{w_1}, \tau\right) \frac{w_1}{\theta'(0,\tau)} e^{\eta_1 \frac{z^2}{w_1}},$$

donde θ' es la derivada con respecto a v, $\eta_1 = \zeta\left(\frac{w_1}{2}\right)$, (w_1, w_2) un par de periodos primitivos de $\wp(z)$ y $\tau = \frac{w_2}{w_1}$.

Demostración: Sea

$$\varphi(z) = \theta\left(\frac{z}{w_1}, \tau\right),$$

por consiguiente $\varphi(z)$ es una función entera e impar de z, con ceros simples en $z = mw_1 + nw_2$, $m, n \in \mathbf{Z}$ ya que:

$$\varphi(mw_1 + nw_2 z) = \theta(m + n\tau, \tau) = 0.$$

También

$$\varphi(z + w_1) = \theta\left(\frac{z}{w_1} + 1, \tau\right) = -\theta\left(\frac{z}{w_1}, \tau\right) = -\varphi(z) \quad \text{(por el teorema 3.3)}$$

y

$$\begin{aligned}
\varphi(z + w_2) &= \theta\left(\frac{z}{w_1} + \tau, \tau\right) \\
&= -e^{-\pi i \tau} e^{-2\pi i \frac{z}{w_1}} \theta\left(\frac{z}{w_1}, \tau\right) \quad \text{(por el teorema 3.3)} \\
&= -e^{-\pi i \frac{w_2}{w_1} - 2\pi i \frac{z}{w_1}} \theta\left(\frac{z}{w_1}, \tau\right) \\
&= -e^{-\pi i \frac{w_2}{w_1} - 2\pi i \frac{z}{w_1}} \varphi(z).
\end{aligned}$$

Haciendo

$$\psi(z) = \varphi(z) e^{\eta_1 \frac{z^2}{w_1}} \frac{w_1}{\theta'(0,\tau)}$$

tenemos que $\psi(z)$ es impar (ya que θ lo es) y entera como función de z, con los mismos ceros que $\varphi(z)$.

Ahora

$$\begin{aligned}
\psi(z + w_2) &= \varphi(z + w_2) e^{\eta_1 \frac{(z+w_2)^2}{w_1}} \frac{w_1}{\theta'(0,\tau)} \\
&= -e^{-\pi i \frac{w_2}{w_1} - 2\pi i \frac{z}{w_1}} \varphi(z) e^{\eta_1 \frac{(z^2 + 2z w_2 + w_2^2)}{w_1}} \frac{w_1}{\theta'(0,\tau)} \\
&= -\varphi(z) e^{\eta_1 \frac{z^2}{w_1}} \frac{w_1}{\theta'(0,\tau)} e^{-\pi i \frac{w_2}{w_1} - 2\pi i \frac{z}{w_1} + \eta_1 \frac{2z w_2}{w_1} + \eta_1 \frac{w_2^2}{w_1}} \qquad (*).
\end{aligned}$$

Pero por el teorema 2.13:

$$\eta_1 w_2 - \eta_2 w_1 = \pi i,$$

entonces

$$2\eta_1 w_2 \frac{z}{w_1} = (2\pi i + 2\eta_2 w_1)\frac{z}{w_1} = 2\eta_2 z + \frac{2\pi i z}{w_1}$$

y

$$\eta_1 \frac{w_2^2}{w_1} = (\pi i + \eta_2 w_1)\frac{w_2}{w_1} = \pi i \frac{w_2}{w_1} + \eta_2 w_2$$

por tanto (*) queda:

$$\begin{aligned}\varphi(z+w_2) &= -\psi(z)\, e^{-\pi i \frac{w_2}{w_1} - 2\pi i \frac{z}{w_1} + 2\eta_2 z + 2\pi i \frac{z}{w_1} + \pi i \frac{w_2}{w_1} + \eta_2 w_2} \\ &= -\psi(z)\, e^{2\eta_2 z + \eta_2 w_2}\end{aligned}$$

De manera similar

$$\psi(z+w_1) = -\psi(z)\, e^{2\eta_1 z + \eta_1 w_1}$$

Pero también

$$\sigma(z+w_1) = -\sigma(z)\, e^{2\eta_1 z + \eta_1 w_1}$$

$$\sigma(z+w_2) = -\sigma(z)\, e^{2\eta_2 z + \eta_2 w_2}$$

por tanto

$$\frac{\psi(z+w_1)}{\sigma(z+w_1)} = \frac{\psi(z)}{\sigma(z)}$$

y

$$\frac{\psi(z+w_2)}{\sigma(z+w_2)} = \frac{\psi(z)}{\sigma(z)}$$

y como $\psi(z)$ y $\sigma(z)$ tienen los mismos ceros y del mismo orden, entonces $\frac{\psi(z)}{\sigma(z)} = c$. Dado que ψ y σ son impares, alrededor de $z = 0$ tenemos:

$$\frac{\psi(z)}{\sigma(z)} = \frac{\psi(0) + \psi'(0)z + \frac{\psi'''(0)z^3}{3!} + \cdots}{z + a_3 z^3 + \cdots}.$$

Pero

$$\psi(0) = \varphi(0)\frac{w_1}{\theta'(0,\tau)} = \theta(0,\tau)\frac{w_1}{\theta'(0,\tau)} = 0$$

y

$$\psi'(z) = \frac{w_1}{\theta'(0,\tau)}\left(\varphi'(z)\, e^{\eta_1 \frac{z^2}{w_1}} + \varphi(z)\frac{2\eta_1}{w_1} e^{\eta_1 \frac{z^2}{w_1}}\right)$$

entonces

$$\begin{aligned}\psi'(0) &= \frac{w_1}{\theta'(0,\tau)}\left(\varphi'(0) + \varphi(0)\frac{2\eta_1}{w_1}\right) \\ &= \frac{w_1}{\theta'(0,\tau)}\left(\theta'(0,\tau)\frac{1}{w_1}\right) = 1\end{aligned}$$

por lo tanto

$$\frac{\psi(z)}{\sigma(z)} = \frac{z + b_3 z^3 + \cdots}{z + a_3 z^3 + \cdots} = \frac{1 + b_3 z^2 + \cdots}{1 + a_3 z^2 + \cdots}$$

de donde $\frac{\psi(0)}{\sigma(0)} = 1$ y entonces $c = 1$. Luego $\psi(z) = \sigma(z)$, es decir $\sigma(z) = \theta\left(\frac{z}{w_1}, \tau\right)\frac{w_1}{\theta'(0,\tau)} e^{\eta_1 \frac{z^2}{w_1}}$.

■

DEFINICION 3.7 *Definimos:*

$$\sigma_1(z) = \frac{e^{\eta_1 z}\,\sigma\left(\frac{w_1}{2} - z\right)}{\sigma\left(\frac{w_1}{2}\right)}$$

$$\sigma_2(z) = \frac{e^{\eta_2 z}\,\sigma\left(\frac{w_2}{2} - z\right)}{\sigma\left(\frac{w_2}{2}\right)}$$

$$\sigma_3(z) = \frac{e^{\eta_3 z}\,\sigma\left(\frac{w_3}{2} - z\right)}{\sigma\left(\frac{w_3}{2}\right)}.$$

Similarmente al teorema 3.6 se tienen las relaciones:

$$\sigma_i(z) = \theta_i\left(\frac{z}{w_1}, \tau\right) e^{\eta_1 \frac{z^2}{w_1}} \frac{1}{\theta_i(0,\tau)}, \quad \forall i \in \{1,2,3\}$$

donde $\tau = \frac{w_2}{w_1}$, $Im\tau > 0$

Ahora veremos el efecto de la transformación $\tau \mapsto -\frac{1}{\tau}$ sobre θ_3, lo cual nos proporcionará una valiosa fórmula de transformación para la función θ_3.

TEOREMA 3.8 *Sean $v, \tau \in \mathbf{C}$, con $Im\tau > 0$. Entonces se tiene:*

$$\theta_3\left(v, -\frac{1}{\tau}\right) = \sqrt{\frac{\tau}{i}} \sum_{n=-\infty}^{\infty} e^{\pi i \cdot (n+v)^2}$$

donde

$$\theta_3(v,\tau) = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 \tau + 2\pi i n v}$$

y $\sqrt{\frac{\tau}{i}} = +1$ para $\tau = i$.

De aquí:

$$\sqrt{\frac{\tau}{i}}\theta_3(v,\tau) = e^{-\frac{\pi i v^2}{\tau}}\,\theta_3\left(\frac{v}{\tau}, -\frac{1}{\tau}\right).$$

Demostración: Sea τ fijo con $Im\tau > 0$ y $q' = e^{-\pi Im\tau}$, entonces para $|v| \leq \rho < \infty$ se tiene:

$$|\, e^{\pi i \tau (n+v)^2} \,| \leq q'^{n^2} M^{|n|} M'$$

para M y M' constantes. Pero como $q' < 1$, entonces por el criterio de la raíz se tiene la convergencia uniforme de $F(v) = \sum_{n=-\infty}^{\infty} e^{\pi i \tau (n+v)^2}$ en todo subconjunto compacto del v-plano con τ fijo.

Además $F(v)$ es periódica de periódo 1, ya que:

$$F(v+1) = \sum_{n=-\infty}^{\infty} e^{\pi i \tau ((n+1)+v)^2} = \sum_{m=-\infty}^{\infty} e^{\pi i \tau (m+v)^2} = F(v).$$

Primero consideremos que $v \in \mathbf{R}$ y $\tau = iy$ con $y > 0$. Así, para la función de variable real $F(v)$ con periódo 1, su serie de Fourier está dada por:

$$F(v) = \sum_{k=-\infty}^{\infty} \alpha_k \, e^{2\pi i k v}$$

donde

$$\begin{aligned}
\alpha_k &= \int_0^1 \left(\sum_{n=-\infty}^{\infty} e^{\pi i \tau (n+v)^2} \right) e^{-2\pi i k v} \, dv \\
&= \int_0^1 \sum_{n=-\infty}^{\infty} e^{\pi i \tau (n+v)^2 - 2\pi i k (v+n)} \, dv \quad \text{(ya que } e^{-2\pi i k n} = 1\text{)} \\
&= \sum_{n=-\infty}^{\infty} \int_0^1 e^{\pi i \tau (n+v)^2 - 2\pi i k (v+n)} \, dv \quad \text{(por la convergencia uniforme)} \\
&= \int_{-\infty}^{\infty} e^{\pi i \tau v^2 - 2\pi i k v} \, dv \\
&= \int_{-\infty}^{\infty} e^{\pi i \tau \left(v^2 - \frac{2kv}{\tau} \right)} \, dv \\
&= \int_{-\infty}^{\infty} e^{\pi i \tau \left(v - \frac{k}{\tau} \right)^2 - \pi i \tau \left(\frac{k}{\tau} \right)^2} \, dv \\
&= e^{-\pi i \frac{k^2}{\tau}} \int_{-\infty}^{\infty} e^{\pi i \tau \left(v - \frac{k}{\tau} \right)^2} \, dv.
\end{aligned}$$

Sea

$$\begin{aligned}
s &= \sqrt{\frac{\tau}{i}} \left(v - \frac{k}{\tau} \right) \\
&= \sqrt{y} v + \frac{ik}{\sqrt{y}}
\end{aligned}$$

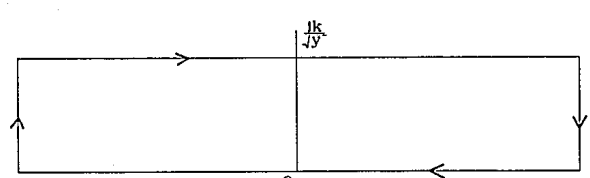
de donde

$$ds = \sqrt{y} dv$$

y entonces

$$\begin{aligned}
\alpha_k &= \frac{e^{-\pi i \frac{k^2}{\tau}}}{\sqrt{y}} \int_{-\infty + \frac{ik}{\sqrt{y}}}^{\infty + \frac{ik}{\sqrt{y}}} e^{\pi i \tau \cdot \frac{1}{\tau} s^2} \, ds \\
&= \frac{e^{-\pi i \frac{k^2}{\tau}}}{\sqrt{y}} \int_{-\infty + \frac{ik}{\sqrt{y}}}^{\infty + \frac{ik}{\sqrt{y}}} e^{-\pi s^2} \, ds
\end{aligned}$$

donde la integración es a lo largo de una línea paralela al eje real en el s-plano complejo.



Por el teorema de la integral de Cauchy tenemos que:

$$\int_{-r+\frac{i}{\sqrt{y}}}^{r+\frac{i}{\sqrt{y}}} e^{-\pi s^2}\,ds + \int_{\frac{i}{\sqrt{y}}}^{0} e^{-\pi(r+ix)^2}\,dx + \int_{r}^{-r} e^{-\pi x^2}\,dx + \int_{0}^{\frac{i}{\sqrt{y}}} e^{-\pi(-r+ix)^2}\,dx = 0$$

Pero

$$\int_{\frac{i}{\sqrt{y}}}^{0} e^{-\pi(r+ix)^2}\,dx + \int_{0}^{\frac{i}{\sqrt{y}}} e^{-\pi(-r+ix)^2}\,dx = \frac{e^{-2\pi ir\frac{i}{\sqrt{y}}}-1}{2\pi ir} + \frac{e^{2\pi ir\frac{i}{\sqrt{y}}}-1}{2\pi ir}$$

y como

$$\left|\frac{e^{-2\pi ir\frac{i}{\sqrt{y}}}-1}{2\pi ir} + \frac{e^{2\pi ir\frac{i}{\sqrt{y}}}-1}{2\pi ir}\right| \leq \left|\frac{e^{-2\pi ir\frac{i}{\sqrt{y}}}-1}{2\pi ir}\right| + \left|\frac{e^{2\pi ir\frac{i}{\sqrt{y}}}-1}{2\pi ir}\right|$$

$$\leq \frac{2}{\pi r} \to 0, \quad \text{cuando } r \to \infty$$

Por tanto

$$\int_{-\infty+\frac{iy}{\sqrt{y}}}^{\infty+\frac{iy}{\sqrt{y}}} e^{-\pi s^2}\,ds = \int_{-\infty}^{\infty} e^{-\pi x^2}\,dx \quad (\text{con } x \in \mathbf{R})$$

$$= \int_{-\infty}^{\infty} e^{-u^2}\frac{du}{\sqrt{\pi}} = 1$$

luego

$$\alpha_k = \frac{e^{-\pi i\frac{k^2}{\tau}}}{\sqrt{y}}$$

y así,

$$F(v) = \frac{1}{\sqrt{y}}\sum_{k=-\infty}^{\infty} e^{-\pi i\frac{k^2}{\tau}+2\pi ikv}$$

$$= \sqrt{\frac{i}{\tau}}\sum_{k=-\infty}^{\infty} e^{-\pi i\frac{k^2}{\tau}+2\pi ikv}$$

$$= \sqrt{\frac{i}{\tau}}\theta_3\left(v, -\frac{1}{\tau}\right).$$

de donde

$$\sqrt{\frac{\tau}{i}}\sum_{n=-\infty}^{\infty} e^{\pi i\tau(n+v)^2} = \theta_3\left(v, -\frac{1}{\tau}\right) \qquad (*)$$

para todo $v \in \mathbf{R}$ y $\tau = iy$ fijo, con $y \in \mathbf{R}^+$.

Ahora, dado que ambos miembros de (*) son funciones analíticas de v para τ fijo, se sigue por continuación analítica que:

$$\sqrt{\frac{\tau}{i}}\sum_{n=-\infty}^{\infty} e^{\pi i\tau(n+v)^2} = \theta_3\left(v, -\frac{1}{\tau}\right) \quad \forall v \in \mathbf{C}.$$

También (*) vista como función de τ para v fija, se cumple para $\tau = iy$ con $y > 0$, y nuevamente por continuación analítica (*) se cumple para todo $\tau \in \mathbf{C}$, con $Im\tau > 0$.

Así, la primera parte del teorema queda probada.

Ahora, si tomamos $-\frac{1}{\tau}$ en lugar de τ y dado que $Im(-\frac{1}{\tau}) > 0$, la primera parte del teorema nos dice que:

$$\begin{aligned}
\theta_3(\upsilon,\tau) &= \sqrt{\frac{-1}{i\tau}} \sum_{n=-\infty}^{\infty} e^{-\pi i \frac{1}{\tau}(n+\upsilon)^2} \\
&= \sqrt{\frac{i}{\tau}} e^{-\frac{\pi i \upsilon^2}{\tau}} \sum_{n=-\infty}^{\infty} e^{-\frac{2\pi i n\upsilon}{\tau} - \frac{\pi i n^2}{\tau}} \\
&= \sqrt{\frac{i}{\tau}} e^{-\frac{\pi i \upsilon^2}{\tau}} \sum_{n=-\infty}^{\infty} q^{n^2} e^{-2\pi i n \frac{\upsilon}{\tau}} \quad \text{(tomando } q = e^{-\frac{\pi i}{\tau}}\text{)} \\
&= \sqrt{\frac{i}{\tau}} e^{-\frac{\pi i \upsilon^2}{\tau}} \theta_3\left(-\frac{\upsilon}{\tau}, -\frac{1}{\tau}\right) \\
&= \sqrt{\frac{i}{\tau}} e^{-\frac{\pi i \upsilon^2}{\tau}} \theta_3\left(\frac{\upsilon}{\tau}, -\frac{1}{\tau}\right)
\end{aligned}$$

por tanto

$$\sqrt{\frac{\tau}{i}}\theta_3(\upsilon,\tau) = e^{-\pi i \frac{\upsilon^2}{\tau}} \theta_3\left(\frac{\upsilon}{\tau}, -\frac{1}{\tau}\right).$$

■

En este capítulo daremos una demostración de la "Ley de Reciprocidad Cuadrática". Esta ley fue descubierta empíricamente y en una forma más complicada por Euler, quien la publica en 1783. En 1785 Legendre la redescubre, pero en su elegante forma moderna con el uso de su símbolo y le da el nombre actual debido a la simetría en el papel que desempeñan los dos primos, y da una prueba basándose en una afirmación no probada en ese tiempo. Gauss la redescubre en 1795, de nuevo empíricamente, y la prueba un año después. Gauss la enuncia en la siguiente forma: "Un primo p es o no un residuo cuadrático de otro primo q de acuerdo con que $(-1)^{\frac{1}{2}(q-1)}q$ sea un residuo cuadrático o no de p". Más tarde da 6 pruebas totalmente diferentes, la más corta de las cuales es su quinta prueba que se basa en el llamado "Lema de Gauss".

En mayo de 1801 Gauss registra en su diario las fórmulas que ahora representamos como:

$$\sum_{\iota=0}^{n-1} e^{\frac{2\pi i}{n}\iota^2} = \frac{1+(-i)^n}{1-i}\sqrt{n}$$

y las designa con el nombre de sumas de Gauss. Con la ayuda de éstas fórmulas de sumación Gauss deriva en sus "Disquisitiones Arithmeticae"la Ley de Reciprocidad Cuadrática.

El arreglo de la demostración del teorema 4.1 es debido a C.L.Siegel junto con el truco de usar casos límites en la fórmula del teorema 3.8.

Kronecker recoge el principio común de las pruebas de Dirichlet y Cauchy, y usando integración compleja obtiene una fórmula de reciprocidad para sumas de Gauss a partir de la cual puede ser deducida la Ley de Reciprocidad Cuadrática.

La fórmula de reciprocidad para sumas generalizadas puede ser probada sin el uso de la fórmula de transformación de las funciones theta por medio del teorema del residuo de Cauchy como lo hicieron Kronecker y Landsberg.

TEOREMA 4.1 *(Cauchy-Kronecker).*
Sean $a,b \in \mathbf{Z}^+$ *y* $v \in \mathbf{Q}$ *tales que* $ab+2av \equiv 0 \pmod 2$. *Entonces se tiene:*

$$\frac{1}{\sqrt{b}}\sum_{h=1}^{b} e^{\pi i \frac{a}{b}(h+v)^2} = \frac{\rho}{\sqrt{a}}\sum_{h=1}^{a} e^{-\pi i \frac{b}{a}h^2+2\pi i h v}, \quad \textit{donde } \rho = e^{\frac{\pi i}{4}}.$$

Demostración: Para $z \in \mathbf{C}$ con $Imz > 0$ y $v \in \mathbf{C}$ el teorema 3.8 nos dice:

$$\sum_{n=-\infty}^{\infty} e^{\pi i z(n+v)^2} = \sqrt{\frac{i}{z}}\sum_{n=-\infty}^{\infty} e^{-\pi i \frac{n^2}{z}+2\pi i n v} \qquad (1)$$

donde $\sqrt{\frac{i}{z}} = 1$, para $z = i$.

Ahora sea $z = \frac{a}{b} + i\varepsilon$, con $\varepsilon > 0$, donde $a, b \in \mathbf{Z}^+$ y $v \in \mathbf{Q}$ es tal que $ab + 2av \equiv 0 \pmod 2$.

Consideremos el caso límite de la fórmula (1) para z cuando $\varepsilon \to 0^+$.

Primero examinaremos el lado izquierdo de (1) para el cual tenemos:

$$\begin{aligned}\sum_{n=-\infty}^{\infty} e^{\pi i z(n+v)^2} &= \sum_{n=-\infty}^{\infty} e^{\pi i\left(\frac{a}{b}+i\varepsilon\right)(n+v)^2} \\ &= \sum_{n=-\infty}^{\infty} e^{\pi i \frac{a}{b}(n+v)^2 - \pi\varepsilon(n+v)^2} \qquad (2)\end{aligned}$$

Por el algoritmo de la división tenemos que $n = mb + h$ con $1 \le h \le b$ y $m \in \mathbf{Z}$.

Dado que:

$$\begin{aligned}\frac{a}{b}\left\{(h+mb+v)^2 - (h+v)^2\right\} &= \frac{a}{b}\left\{2mb(h+v) + (mb)^2\right\} \\ &= 2amh + 2amv + abm^2 \\ &\equiv m2av + mabm \pmod 2 \\ &\equiv m2av + (m-1)abm + mab \pmod 2 \\ &\equiv m(2av + ab) + m(m-1)ab \pmod 2 \\ &\equiv 0 \pmod 2 \quad \text{(por hipótesis).}\end{aligned}$$

entonces

$$e^{\pi i \frac{a}{b}(mb+h+v)^2} = e^{(h+v)^2}$$

y (2) queda:

$$\begin{aligned}\sum_{n=-\infty}^{\infty} e^{\pi i \frac{a}{b}(n+v)^2 - \pi\varepsilon(n+v)^2} &= \sum_{h=1}^{b}\sum_{m=-\infty}^{\infty} e^{\pi i \frac{a}{b}(h+mb+v)^2 - \pi\varepsilon(h+mb+v)^2} \\ &= \sum_{h=1}^{b}\sum_{m=-\infty}^{\infty} e^{\pi i \frac{a}{b}(h+v)^2 - \pi\varepsilon(h+mb+v)^2} \\ &= \sum_{h=1}^{b}\left(e^{\pi i \frac{a}{b}(h+v)^2}\sum_{m=-\infty}^{\infty} e^{-\pi\varepsilon b^2\left(m+\frac{h+v}{b}\right)^2}\right)\end{aligned}$$

Ahora usando el teorema 3.8 en $\sum_{m=-\infty}^{\infty} e^{-\pi\varepsilon b^2\left(m+\frac{h+v}{b}\right)^2}$ para $\frac{v+h}{b}$ en lugar de v y $i\varepsilon b^2$ en lugar de z (lo cual es válido ya que $Im(i\varepsilon b^2) > 0$), obtenemos:

$$\begin{aligned}\sum_{m=-\infty}^{\infty} e^{-\pi\varepsilon b^2\left(m+\frac{h+v}{b}\right)^2} &= \sqrt{\frac{i}{i\varepsilon b^2}}\sum_{n=-\infty}^{\infty} e^{-\pi i\frac{n^2}{i\varepsilon b^2} + 2\pi i n\left(\frac{v+h}{b}\right)} \\ &= \frac{1}{b\sqrt{\varepsilon}}\sum_{n=-\infty}^{\infty} e^{-\pi\frac{n^2}{\varepsilon b^2} + 2\pi i\frac{n}{b}(v+h)}.\end{aligned}$$

Además se tiene que:

$$\left|\sum_{n=-\infty}^{\infty} e^{-\pi\frac{n^2}{\epsilon b^2}+2\pi i\frac{n}{b}(v+h)}-1\right| = \left|\sum_{\substack{n=-\infty\\ n\neq 0}}^{\infty} e^{-\pi\frac{n^2}{\epsilon b^2}+2\pi i\frac{n}{b}(v+h)}\right|$$

$$\leq \sum_{\substack{n=-\infty\\ n\neq 0}}^{\infty} e^{-\pi\frac{n^2}{\epsilon b^2}}$$

$$= 2\sum_{n=1}^{\infty} e^{-cn^2} \quad (\text{con } c=\tfrac{\pi}{b^2\epsilon}>0)$$

$$\leq 2\sum_{n=1}^{\infty} e^{-cn}$$

$$= 2\frac{e^{-c}}{1-e^{-c}} \to 0, \quad \text{cuando } c\to+\infty$$

por tanto

$$\lim_{\epsilon\to 0^+}\sum_{n=-\infty}^{\infty} e^{-\pi\frac{n^2}{\epsilon b^2}+2\pi i\frac{n}{b}(v+h)} = 1.$$

Así, para $z=\frac{a}{b}+i\epsilon$, con $a,b\in\mathbf{Z}^+$, $\epsilon>0$ y $v\in\mathbf{Q}$ tal que $ab+2av\equiv 0 \pmod 2$ se tiene:

$$\sum_{n=\infty}^{\infty} e^{\pi i z(n+v)^2} \sim \frac{1}{b\sqrt{\epsilon}}\sum_{h=1}^{b} e^{\pi i\frac{a}{b}(h+v)^2}, \quad \text{cuando } \epsilon\to 0^+ \qquad (A).$$

Por otra parte como

$$-\frac{1}{z} = -\frac{1}{\frac{a}{b}+i\epsilon}$$

$$= \frac{-\frac{b}{a}}{1+i\epsilon\frac{b}{a}}$$

$$= -\frac{b}{a}\left(1-\frac{\frac{ib\epsilon}{a}}{1+ib\frac{\epsilon}{a}}\right)$$

$$= -\frac{b}{a}+\frac{\frac{ib^2}{a^2}\epsilon}{1+ib\frac{\epsilon}{a}} \qquad (*).$$

entonces para el lado derecho de (1) tenemos:

$$\sum_{n=\infty}^{\infty} e^{-\pi i\frac{n^2}{\epsilon}+2\pi i n v} = \sum_{n=-\infty}^{\infty} e^{\pi i n^2\left(-\frac{b}{a}+\frac{i\epsilon\frac{b^2}{a^2}}{1+i\frac{b}{a}\epsilon}\right)+2\pi i n v} \qquad (\text{por}(*))$$

$$= \sum_{n=-\infty}^{\infty} e^{-\pi i n^2\frac{b}{a}+2\pi i n v-\frac{\pi\frac{b^2}{a^2}\epsilon}{1+i\frac{b}{a}\epsilon}n^2} \qquad (3)$$

Por el algoritmo de la división tenemos que $n = ma + h$ con $1 \leq h \leq a$ y $m \in \mathbf{Z}$.
Dado que:

$$\begin{aligned} -\frac{b}{a}(h+ma)^2 + 2(h+ma)v + \frac{b}{a}h^2 - 2hv &= -\frac{b}{a}(2hma) - \frac{b}{a}(ma)^2 + 2mav \\ &= -2hbm - bm^2a + 2mav \\ &\equiv m2av - mabm \pmod 2 \\ &\equiv m2av + mabm \pmod 2 \\ &\equiv m(2av + ab) \equiv 0 \pmod 2 \end{aligned}$$

por lo tanto (3) queda:

$$\begin{aligned} \sum_{h=1}^{a}\sum_{m=-\infty}^{\infty} e^{-\pi i(h+ma)^2\frac{b}{a}+2\pi i(h+ma)v-\frac{\pi\left(\frac{b}{a}\right)^2\epsilon}{1+i\frac{b}{a}\epsilon}(h+ma)^2} &= \sum_{h=1}^{a}\sum_{m=-\infty}^{\infty} e^{-\pi ih^2\frac{b}{a}+2\pi ihv-\frac{\pi b^2\epsilon}{1+i\frac{b}{a}\epsilon}\left(\frac{h}{a}+m\right)^2} \\ &= \sum_{h=1}^{a}\left(e^{-\pi ih^2\frac{b}{a}+2\pi ihv}\sum_{m=-\infty}^{\infty} e^{-\frac{\pi b^2\epsilon}{1+i\frac{b}{a}\epsilon}\left(\frac{h}{a}+m\right)^2}\right) \quad (4) \end{aligned}$$

Si nuevamente usamos el teorema 3.8 con $\frac{b}{a}$ en lugar de v y $\frac{ib^2\epsilon}{1+i\frac{b}{a}\epsilon}$ en lugar de z (lo cual es válido ya que $Im(\frac{ib^2\epsilon}{1+i\frac{b}{a}\epsilon}) = \frac{b^2\epsilon}{|1+i\frac{b}{a}\epsilon|^2} > 0$), obtenemos:

$$\begin{aligned} \sum_{m=-\infty}^{\infty} e^{-\frac{\pi b^2\epsilon}{1+i\frac{b}{a}\epsilon}\left(m+\frac{h}{a}\right)^2} &= \sqrt{\frac{i}{\frac{ib^2\epsilon}{1+i\frac{b}{a}\epsilon}}}\sum_{n=-\infty}^{\infty} e^{-\pi in^2\left(\frac{1+i\frac{b}{a}\epsilon}{ib^2\epsilon}\right)+2\pi in\left(\frac{h}{a}\right)} \\ &= \sqrt{\frac{1+i\frac{b}{a}\epsilon}{b^2\epsilon}}\sum_{n=-\infty}^{\infty} e^{-\frac{\pi in^2}{ib^2\epsilon}-\pi in^2\frac{i\frac{b}{a}\epsilon}{ib^2\epsilon}+2\pi in\frac{h}{a}} \\ &= \frac{\sqrt{1+i\frac{b}{a}\epsilon}}{b\sqrt{\epsilon}}\sum_{n=-\infty}^{\infty} e^{-\frac{\pi n^2}{b^2\epsilon}-\pi i\frac{n^2}{ab}+2\pi i\frac{h}{a}n} \quad (5) \end{aligned}$$

Pero

$$\begin{aligned} \left|\sum_{n=-\infty}^{\infty} e^{-\frac{\pi n^2}{b^2\epsilon}+\pi i\frac{n^2}{ab}+2\pi i\frac{h}{a}n} - 1\right| &= \left|\sum_{\substack{n=-\infty \\ n\neq 0}}^{\infty} e^{-\frac{\pi n^2}{b^2\epsilon}+\pi i\frac{n^2}{ab}+2\pi i\frac{h}{a}n}\right| \\ &\leq \sum_{\substack{n=-\infty \\ n\neq 0}}^{\infty} e^{-\frac{\pi n^2}{b^2\epsilon}} \\ &= 2\sum_{n=1}^{\infty} e^{-cn^2} \left(\text{con } c = \frac{\pi}{b^2\epsilon} > 0\right) \\ &\leq \sum_{n=1}^{\infty} e^{-cn} \\ &= 2\frac{e^{-c}}{1-e^{-c}} \to 0, \quad \text{cuando } c \to \infty \end{aligned}$$

por tanto

$$\lim_{\epsilon\to 0^+}\sum_{n=-\infty}^{\infty} e^{-\frac{\pi n^2}{b^2\epsilon}-\pi i\frac{n^2}{ab}+2\pi i\frac{h}{a}n}=1 \qquad (6)$$

También tenemos que:

$$\lim_{\epsilon\to 0+}\sqrt{\frac{i}{\frac{\epsilon}{b}+i\epsilon}}=\sqrt{\frac{ib}{a}}$$
$$=\sqrt{\frac{b}{a}}e^{\frac{\pi i}{4}} \qquad (**)$$

así de (**) y de (3)-(6) obtenemos para el lado derecho de (1):

$$\sqrt{\frac{i}{z}}\sum_{n=-\infty}^{\infty} e^{-\pi i\frac{n^2}{a}+2\pi i n v}\sim\left(\frac{1}{b\sqrt{\epsilon}}\sum_{h=1}^{a} e^{-\pi i\frac{h}{a}h^2+2\pi i h v}\right)\left(\sqrt{\frac{b}{a}}e^{\frac{\pi i}{4}}\right), \text{cuando } \epsilon\to 0^+ \qquad (B)$$

Finalmente de (1), (A) y (B) obtenemos:

$$\frac{1}{b\sqrt{\epsilon}}\sum_{h=1}^{b} e^{\pi i\frac{a}{b}(h+v)^2}\sim\left(\frac{1}{b\sqrt{\epsilon}}\sum_{h=1}^{a} e^{-\pi i\frac{h}{a}h^2+2\pi i h v}\right)\left(\sqrt{\frac{b}{a}}e^{\frac{\pi i}{4}}\right)$$

cuando $\epsilon\to 0^+$ y por tanto cuando $z\to\frac{a}{b}$. Es decir

$$\sum_{h=1}^{b} e^{\pi i\frac{a}{b}(h+v)^2}\sim\left(\sum_{h=1}^{a} e^{-\pi i\frac{h}{a}h^2+2\pi i h v}\right)\left(\sqrt{\frac{b}{a}}e^{\frac{\pi i}{4}}\right)$$

cuando $\epsilon\to 0^+$; pero aquí no interviene ϵ, de donde se tiene:

$$\frac{1}{\sqrt{b}}\sum_{h=1}^{b} e^{\pi i\frac{a}{b}(h+v)^2}=\frac{e^{\frac{\pi i}{4}}}{\sqrt{a}}\sum_{h=1}^{a} e^{-\pi i\frac{h}{a}h^2+2\pi i h v}.$$

■

COROLARIO 4.2 *Si* $a,b\in\mathbf{Z}^+$ *se tiene:*

$$\frac{1}{\sqrt{b}}\sum_{h=1}^{b} e^{\pi i\frac{a}{b}h^2+\pi i a h}=\frac{\rho^{1-ab}}{\sqrt{a}}\sum_{h=1}^{a} e^{-\pi i\frac{h}{a}h^2-\pi i b h},$$

con $\rho=e^{\frac{\pi i}{4}}$.

Demostración: Tomando $v=\frac{b}{2}$ en el teorema 4.1 y dado que $ab+2av=ab+ab\equiv 0 \pmod 2$, tenemos:

$$\frac{1}{\sqrt{b}}\sum_{h=1}^{b} e^{\pi i\frac{a}{b}\left(h+\frac{b}{2}\right)^2}=\frac{\rho}{\sqrt{a}}\sum_{h=1}^{a} e^{-\pi i\frac{h}{a}h^2+2\pi i h\frac{b}{2}}$$

es decir

$$\frac{1}{\sqrt{b}}\sum_{h=1}^{b} e^{\pi i \frac{a}{b}\left(h^2+hb+\frac{b^2}{4}\right)} = \frac{\rho}{\sqrt{a}}\sum_{h=1}^{a} e^{-\pi i \frac{b}{a}h^2+\pi i h b}$$

por tanto

$$\frac{e^{\pi i \frac{ab}{4}}}{\sqrt{b}}\sum_{h=1}^{b} e^{\pi i \frac{a}{b}h^2+\pi i a h} = \frac{\rho}{\sqrt{a}}\sum_{h=1}^{a} e^{-\pi i \frac{b}{a}h^2+\pi i h b}$$

$$= \frac{\rho}{\sqrt{a}}\sum_{h=1}^{a} e^{-\pi i \frac{b}{a}h^2-\pi i h b} \quad (\text{ya que } e^{\pi i b h} = e^{-\pi i b h}).$$

Por tanto

$$\frac{1}{\sqrt{b}}\sum_{h=1}^{b} e^{\pi i \frac{a}{b}h^2+\pi i a h} = \frac{\rho^{1-ab}}{\sqrt{a}}\sum_{h=1}^{a} e^{-\pi i \frac{b}{a}h^2-\pi i b h}.$$

■

DEFINICION 4.3 *Sean $m, n \in \mathbf{Z}$ con $n \neq 0$. Definimos:*

$$G(m,n) = \sum_{h=1}^{|n|} e^{\pi i \frac{m}{n}h^2+\pi i m h}$$

llamada suma generalizada de Gauss.

Con esta definición el corolario 4.2 se reescribe como:

COROLARIO 4.4 *Para $a, b \in \mathbf{Z}^+$ se tiene:*

$$\frac{1}{\sqrt{b}}G(a,b) = \frac{1}{\sqrt{a}}G(-b,a)\rho^{1-ab}.$$

Ahora pasaremos a algunas definiciones y teoremas de la Teoría de Números clásica.

DEFINICION 4.5 *Sea p un primo impar y $a \in \mathbf{Z}$ tal que $(a,p) = 1$. Si existe $x \in \mathbf{Z}$ tal que $x^2 \equiv a \pmod{p}$, llamamos a a un residuo cuadrático módulo p y escribimos ${}_aR_p$. Si no existe una tal x, entonces decimos que a no es residuo cuadrático módulo p y escribimos ${}_aN_p$.*

DEFINICION 4.6 *Definimos el símbolo de Legendre $\left(\frac{m}{p}\right)$ como sigue:*

$$\left(\frac{m}{p}\right) = \begin{cases} 1 & si\ {}_mR_p \\ -1 & si\ {}_mN_p \\ 0 & si\ p|m \end{cases}$$

donde p es primo impar y $m \in \mathbf{Z}$.

OBSERVACION: Resulta útil saber cuántos de los elementos de $\{1,2,\cdots,p-1\}$ son residuos cuadráticos. Observemos que si $1 \leq r \leq \frac{1}{2}(p-1)$ se tiene que $\frac{1}{2}(p+1) \leq p-r \leq p-1$ y como $r^2 \equiv (p-r)^2 \pmod{p}$, entonces cuando x en $x^2 \equiv a \pmod{p}$ recorre los valores $1,2,\cdots,p-1$, se tiene que a recorre exactamente los $\frac{1}{2}(p-1)$ valores $1^2, 2^2, \cdots, \left(\frac{1}{2}(p-1)\right)^2$.

Además si $1 \leq r,s \leq \frac{1}{2}(p-1)$ con $r \neq s$, entonces $r^2 \not\equiv s^2 \pmod{p}$. Ya que si $r^2 \equiv s^2 \pmod{p}$, entonces $r+s \equiv 0 \pmod{p}$ ó $r-s \equiv 0 \pmod{p}$. Pero como $1 \leq r,s \leq \frac{1}{2}(p-1)$ y $r \neq s$ no se puede dar ninguna de las dos congruencias. De lo anterior se sigue que hay exactamante $\frac{1}{2}(p-1)$ residuos cuadráticos y $\frac{1}{2}(p-1)$ no residuos cuadráticos módulo p y que $\sum_{m=0}^{p-1} \left(\frac{m}{p}\right) = 0$.

Es claro que si $m_1 \equiv m_2 \pmod{p}$, entonces $\left(\frac{m_1}{p}\right) = \left(\frac{m_2}{p}\right)$.

PROPOSICION 4.7 *(Lagrange). Sea p un primo, $a_0, a_1, \cdots, a_n \in \mathbf{Z}$, con $(a_0, p) = 1$. Entonces la congruencia:*

$$a_0x^n + a_1x^{n-1} + \cdots + a_n \equiv 0 \pmod{p},$$

tiene a lo más n soluciones.

Demostración: Al hablar de soluciones de la congruencia nos referimos a las distintas clases residuales cuyos elementos satisfacen la congruencia.

Si $n = 1$, entonces $a_0x + a_1 \equiv 0 \pmod{p}$, tiene sólo una solución ya que $(a_0, p) = 1$.

Ahora, supongamos que la proposición es cierta para congruencias de grado $n-1$ con $n > 1$. Tenemos que la proposición es verdad para n si la congruencia no posee soluciones, pero si ésta poseé una solución, digamos $x \equiv x_1 \pmod{p}$, entonces

$$a_0x_1^n + a_1x_1^{n-1} + \cdots + a_n \equiv 0 \pmod{p}$$

y restándola a la congruencia

$$a_0x^n + a_1x^{n-1} + \cdots + a_n \equiv 0 \pmod{p}$$

obtenemos:

$$a_0(x^n - x_1^n) + a_1(x^{n-1} - x_1^{n-1}) + \cdots + a_{n-1}(x - x_1) \equiv 0 \pmod{p}$$

por tanto

$$\begin{aligned}&(x-x_1)\left\{a_0(x^{n-1} + x^{n-2}x_1 + \cdots + x_1^{n-1}) + a_1(x^{n-2} + x^{n-3}x_1 + \cdots + x_1^{n-2}) + \cdots + a_{n-1}\right\}\\ &= (x-x_1)(a_0x^{n-1} + b_1x^{n-2} + \cdots + b_{n-1}) \equiv 0 \pmod{p} \qquad (I)\end{aligned}$$

donde las $b_i's$ dependen de x_1 y de las $a_i's$.

Hay que observar que x es solución de la congruencia original de grado n si, y sólo si, x es solución de (1). Pero si x es solución de (I), entonces

$$x - x_1 \equiv 0 \pmod{p}$$

(lo cual nos lleva a la solución $x \equiv x_1 \pmod{p}$ que ya teníamos)
ó

$$a_0 x^{n-1} + b_1 x^{n-2} + \cdots + b_{n-1} \equiv 0 \pmod{p}, \text{con } (a_0, p) = 1;$$

la cual por ser una congruencia de grado $n-1$ tiene, por hipótesis de inducción, a lo más $n-1$ soluciones y por tanto la congruencia original de grado n tiene a lo más n soluciones.

■

TEOREMA 4.8 *(Euler). Sea p un primo impar y $a \in \mathbf{Z}$ tal que $(a,p) = 1$. Se tiene:*

$$_aR_p \text{ si, y sólo si, } a^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p} \qquad (A)$$

Demostración: Supongamos que $_aR_p$, entonces existe $x \in \mathbf{Z}$ tal que $x^2 \equiv a \pmod{p}$. Ahora, como p es impar, se tiene que $\frac{1}{2}(p-1)$ es entero y por tanto:

$$x^{2\left(\frac{1}{2}(p-1)\right)} \equiv a^{\frac{1}{2}(p-1)} \pmod{p}$$

de donde

$$x^{p-1} \equiv a^{\frac{1}{2}(p-1)} \pmod{p}.$$

Dado que $(x,p) = 1$ (ya que $(a,p) = 1$), por el Teorema de Fermat tenemos:

$$x^{p-1} \equiv 1 \pmod{p}$$

por lo tanto

$$a^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}.$$

En el otro sentido, supongamos que $a^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}$.
Observemos que la congruencia $x^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}$ tiene a lo más $\frac{1}{2}(p-1)$ soluciones por la proposición 4.7; pero también sabemos que cada uno de los $\frac{1}{2}(p-1)$ residuos cuadráticos módulo p satisfacen esta congruencia (lo cual se observó en la primera parte de la demostración), de donde no hay más soluciones que los residuos cuadráticos y por consiguiente $_aR_p$.

■

TEOREMA 4.9 *Si p es un primo impar, entonces*

$$a^{\frac{1}{2}(p-1)} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

de aquí:

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Demostración: Si $(a,p) = 1$, el Teorema de Fermat nos dice que:

$$a^{p-1} - 1 \equiv 0 \pmod{p}$$

de donde

$$\left(a^{\frac{1}{2}(p-1)} + 1\right)\left(a^{\frac{1}{2}(p-1)} - 1\right) \equiv 0 \pmod{p},$$

es decir,

$$a^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}$$

ó

$$a^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}$$

Pero del teorema 4.8 tenemos que:

$$a^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}$$

si, y sólo si, ${}_aR_p$, es decir

$$a^{\frac{1}{2}(p-1)} \equiv \left(\frac{a}{p}\right) \pmod{p},$$

ya que $\left(\frac{a}{p}\right) = 1$.
Si ${}_aN_p$, entonces se debe satisfacer que:

$$a^{\frac{1}{2}(p-1)} \equiv -1 = \left(\frac{a}{p}\right) \pmod{p}.$$

Así, en ambos casos para $(a,p) = 1$ se tiene:

$$a^{\frac{1}{2}(p-1)} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Finalmente si $(a,p) = p$, entonces

$$a^{\frac{1}{2}(p-1)} \equiv 0 = \left(\frac{a}{p}\right) \pmod{p}.$$

De lo anterior tenemos que si $a, b \in \mathbf{Z}$, entonces

$$\begin{aligned}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) &\equiv a^{\frac{1}{2}(p-1)} b^{\frac{1}{2}(p-1)} \pmod{p} \\ &\equiv (ab)^{\frac{1}{2}(p-1)} \pmod{p} \\ &\equiv \left(\frac{ab}{p}\right) \pmod{p} \quad \text{(por la primera parte de la demostración)}\end{aligned}$$

Ahora $\left(\frac{a}{p}\right) = 0$ o $\left(\frac{b}{p}\right) = 0$ si, y sólo si, $\left(\frac{ab}{p}\right) = 0$ y por tanto

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

Si no se tiene el caso anterior, entonces $\left(\frac{a}{p}\right), \left(\frac{b}{p}\right), \left(\frac{ab}{p}\right) \in \{1, -1\}$. Pero como

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - \left(\frac{ab}{p}\right) \equiv 0 \pmod{p}$$

y p es un primo mayor que 2, se debe tener que:

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

■

TEOREMA 4.10 *Ley de Reciprocidad Cuadrática (Gauss).*
Sean p, q primos impares, $p \neq q$, entonces

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}.$$

Demostración: Evaluemos la correspondiente suma de Gauss para los primos p y q:

$$\begin{aligned}G(p,q) &= \sum_{h=1}^{q} e^{\pi i \frac{p}{q} h^2 + \pi i p h} \\ &= \sum_{h=1}^{q-1} e^{\pi i \frac{p}{q} h^2 + \pi i p h} + e^{2\pi i p q} \\ &= 1 + \sum_{h=1}^{q-1} e^{\pi i \frac{p}{q} h^2 + \pi i p h^2} \text{ (ya que } h^2 \equiv h \pmod{2}) \\ &= 1 + \sum_{h=1}^{q-1} e^{\pi i h^2 \frac{p}{q}(1+q)}.\end{aligned}$$

Sean λ y μ tales que λ recorre los residuos cuadráticos módulo q y μ recorre los no residuos cuadráticos módulo q.

Observemos que si $h^2 \equiv \lambda \pmod{q}$, entonces

$$\begin{aligned} e^{\pi i h^2 \frac{p}{q}(1+q)} &= e^{\pi i(kq+\lambda)\frac{p}{q}(1+q)} \\ &= e^{\pi i k p(1+q)} e^{\pi i \frac{p}{q}\lambda(1+q)} \\ &= e^{\pi i \frac{p}{q}\lambda(1+q)} \quad (\text{pues } 1+q \text{ es par}) \end{aligned}$$

pero $(q-h)^2 \equiv h^2 \equiv \lambda \pmod{q}$ para $1 \leq h \leq q-1$, luego entonces cuando h recorre el conjunto $\{1,2,\cdots,q-1\}$, se tiene que h^2 recorre el conjunto de residuos cuadráticos dos veces, de donde

$$1 + \sum_{h=1}^{q-1} e^{\pi i h^2 \frac{p}{q}(1+q)} = 1 + 2\sum_{\lambda} e^{\pi i \frac{p}{q}\lambda(1+q)}$$

Pero

$$1 + \sum_{\lambda} e^{\pi i \lambda \frac{p}{q}(1+q)} + \sum_{\mu} e^{\pi i \mu \frac{p}{q}(1+q)} = \sum_{h=0}^{q-1} e^{\pi i h \frac{p}{q}(1+q)} \qquad (*)$$

y como $q+1$ es par, entonces $e^{\pi i h \frac{p}{q}(1+q)}$ es la h-ésima potencia de una q-ésima raíz de la unidad, digamos $\xi \neq 1$ (ya que $q \neq p$), por lo que (*) queda:

$$\sum_{h=0}^{q-1} e^{\pi i h \frac{p}{q}(1+q)} = \sum_{h=0}^{q-1} \xi^h = \frac{1-\xi^q}{1-\xi} = 0$$

de donde para todo primo impar q y $p \in \mathbf{Z}$ tal que $(p,q) = 1$ se tiene:

$$G(p,q) = \sum_{\lambda} e^{\pi i \lambda \frac{p}{q}(1+q)} - \sum_{\mu} e^{\pi i \mu \frac{p}{q}(1+q)} \qquad (1)$$

Caso (i) Sea ${}_pR_q$. Dado que $(p,q) = 1$ el teorema 4.8 nos dice que cuando λ recorre el conjunto de residuos cuadráticos módulo q lo mismo hace λp. Similarmente μp recorre los no residuos cuadráticos cuando μ lo hace y por tanto

$$\begin{aligned} G(p,q) &= \sum_{\lambda} e^{\pi i \lambda \frac{p}{q}(1+q)} - \sum_{\mu} e^{\pi i \mu \frac{p}{q}(1+q)} \\ &= \sum_{\lambda} e^{\pi i \lambda \frac{1}{q}(1+q)} - \sum_{\mu} e^{\pi i \mu \frac{1}{q}(1+q)} \\ &= G(1,q) \quad (\text{usando (1) para } p=1) \\ &= \left(\frac{p}{q}\right) G(1,q) \quad (\text{ya que } {}_pR_q) \end{aligned}$$

Caso (ii) Sea ${}_pN_q$. Como en el caso (i) por el teorema 4.8 tenemos que si λ recorre los residuos cuadráticos módulo q, entonces λp recorre los no residuos y cuando μ recorre los no residuos cuadráticos, entonces μp recorre los residuos cuadráticos. Por tanto

$$\begin{aligned} G(p,q) &= \sum_{\lambda} e^{\pi i \lambda \frac{p}{q}(1+q)} - \sum_{\mu} e^{\pi i \mu \frac{p}{q}(1+q)} \\ &= \sum_{\mu} e^{\pi i \mu \frac{1}{q}(1+q)} - \sum_{\lambda} e^{\pi i \lambda \frac{1}{q}(1+q)} \\ &= -G(1,q) \quad \text{(usando (1) para } p=1) \\ &= \left(\frac{p}{q}\right) G(1,q) \quad \text{(ya que } {}_pN_q) \end{aligned}$$

Así, en ambos casos:

$$G(p,q) = \left(\frac{p}{q}\right) G(1,q)$$

Por el corolario 4.4 se tiene:

$$\begin{aligned} \frac{1}{\sqrt{q}} G(1,q) &= G(-q,1)\rho^{1-q} \quad (\text{con } \rho = e^{\frac{\pi i}{4}}) \\ &= e^{-2\pi i q} \rho^{1-q} \\ &= \rho^{1-q} \end{aligned}$$

de donde

$$\frac{1}{\sqrt{q}} G(p,q) = \left(\frac{p}{q}\right) \rho^{1-q} \tag{2}$$

para q un primo impar y $(p,q)=1$.

Si ahora consideramos $-q$ y p en lugar de p y q con p primo impar la fórmula (2) nos da:

$$\frac{1}{\sqrt{p}} G(-q,p) = \left(\frac{-q}{p}\right) \rho^{1-p} \tag{3}$$

Pero por el corolario 4.4 tenemos:

$$\begin{aligned} \frac{1}{\sqrt{q}} G(p,q) &= \frac{i}{\sqrt{p}} G(-q,p)\rho^{1-pq} \\ &= \left(\frac{-q}{p}\right) \rho^{1-p}\rho^{1-pq} \quad \text{(por (3))} \end{aligned}$$

sustituyendo en (2) obtenemos:

$$\left(\frac{p}{q}\right)\rho^{1-q} = \left(\frac{-q}{p}\right)\rho^{1-p}\rho^{1-pq}$$

por tanto

$$\rho^{1-q}\rho^{p-1}\rho^{pq-1} = \left(\frac{p}{q}\right)\left(\frac{-q}{p}\right) \quad (\text{pues } \left(\tfrac{p}{q}\right) = \pm 1)$$

pero

$$\begin{aligned} \rho^{p-q+pq-1} &= \rho^{(p-1)(q+1)} \\ &= e^{\pi i \frac{1}{2}(p-1)\cdot\frac{1}{2}(q+1)} \\ &= (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q+1)}. \end{aligned}$$

Además

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

y por el teorema 4.9:

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{1}{2}(p-1)} \pmod{p}$$

Pero dado que $\left(\frac{-1}{p}\right) = \pm 1$ y p es primo impar, se debe tener que $\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}$, luego

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)(-1)^{\frac{1}{2}(p-1)} = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q+1)}$$

y así:

$$\begin{aligned}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{\frac{1}{2}(p-1)(\frac{1}{2}(q+1)-1)} \\ &= (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}.\end{aligned}$$

■

OBSERVACION: La Ley de Reciprocidad Cuadrática se puede resumir así:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

salvo si $p, q \equiv 3 \pmod{4}$, en cuyo caso:

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

También observemos que de:

$$\begin{aligned}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)} \\ &= \left((-1)^{\frac{1}{2}(q-1)}\right)^{\frac{1}{2}(p-1)} \\ &= \left(\frac{(-1)^{\frac{1}{2}(q-1)}}{p}\right)\end{aligned}$$

se obtiene:

$$\left(\frac{p}{q}\right)\left(\frac{(-1)^{\frac{1}{2}(q-1)}q}{p}\right) = 1$$

lo cual es equivalente al enunciado que da Gauss para la Ley de Reciprocidad.

Una antigua conjetura dentro de la Teoría de los Números es la Conjetura de Godbach: "Cada entero par (> 2) es la suma de dos primos".

El siguiente corolario establece una equivalencia entre las sumas de Gauss y la Conjetura de Goldbach.

COROLARIO 4.11 *Sea n un entero positivo par (>2), p y q primos tales que $3 \le q \le \frac{n}{2}$ y $\frac{n}{2} \le p < n$. Se tiene:*

$$n = p + q \text{ si, y sólo si, } |G(n-q,p)| = p.$$

Demostración: Si $n = p+q$, entonces

$$\begin{aligned} G(n-q,p) &= G(p,p) \\ &= \sum_{h=1}^{p} e^{\pi i h^2 + \pi i p h} \\ &= \sum_{h=1}^{p} e^{\pi i h^2 + \pi i p h^2} \text{ (ya que } h^2 \equiv h \pmod 2) \\ &= \sum_{h=1}^{p} e^{\pi i h^2 (1+p)} \\ &= \sum_{h=1}^{p} 1 = p \text{(ya que } p \text{ es impar).} \end{aligned}$$

Inversamente, supongamos que $n \neq p+q$.
Luego debe ser $(n-q,p) = 1$ (pues en caso contrario $p|n-q$ y entonces $n-q = sp$, pero $n-q \le n-3 < 2p$ y por tanto $s = 1$!).
Así por (2) del teorema 4.10:

$$G(n-q,p) = \sqrt{p}\left(\frac{n-q}{p}\right) e^{\frac{\pi i}{4}(1-p)}$$

y entonces $|G(n-q,p)| = \sqrt{p}$!.

■

OBSERVACION: La proposición 4.7 nos asegura que el polinomio $f(x) = x^k + x^{k-1}n + \cdots + xn^{k-1} + n^k \equiv 0 \pmod p$ con $k = \frac{1}{2}(p-1)-1$, tiene a lo más k soluciones. El siguiente corolario nos da una equivalencia entre el símbolo de Legendre y la Conjetura de Goldbach.

COROLARIO 4.12 *Sea n un entero positivo par (>2), p y q ($p \neq q$) primos tales que $3 \le q \le \frac{n}{2}$ y $\frac{n}{2} \le p < n$. Se tiene:*

$$n = p + q \text{ si, y sólo si, } \left(\frac{n}{p}\right) = \left(\frac{q}{p}\right) \text{ y } p \nmid f(q).$$

Demostración: Si $n = p+q$, entonces $n \equiv q \pmod p$ y por tanto $\left(\frac{n}{p}\right) = \left(\frac{q}{p}\right)$.
Además como:

$$\begin{aligned} f(q) = f(n-p) &= (n-p)^k + (n-p)^{k-1}n + \cdots + (n-p)n^{k-1} + n^k \\ &\equiv n^k + n^{k-1}n + \cdots + nn^{k-1} + n^k = \frac{1}{2}(p-1)n^{\frac{1}{2}(p-1)} \pmod p \end{aligned}$$

y dado que $p \nmid \frac{1}{2}(p-1)$ y $p \nmid n$ (ya que si $p|n$, entonces $p|q$ y como q es primo, se debería tener que $p = q$!), entonces $p \nmid f(q)$.

Inversamente, si $\left(\frac{n}{p}\right) = \left(\frac{s}{p}\right)$ del teorema 4.9 tenemos:

$$\left(\frac{n}{p}\right) \equiv n^{\frac{1}{2}(p-1)} \pmod{p}$$

y

$$\left(\frac{q}{p}\right) \equiv q^{\frac{1}{2}(p-1)} \pmod{p}$$

por tanto

$$n^{\frac{1}{2}(p-1)} \equiv q^{\frac{1}{2}(p-1)} \pmod{p}$$

es decir, p divide a $n^{\frac{1}{2}(p-1)} - q^{\frac{1}{2}(p-1)}$.

Pero

$$n^{\frac{1}{2}(p-1)} - q^{\frac{1}{2}(p-1)} = (n-q)(n^k + n^{k-1}q + \cdots + nq^{k-1} + q^k) = (n-q)f(q)$$

y dado que $p \nmid f(q)$, entonces $p|n-q$.

Además como $0 < n - q \leq n - 3 < 2p$, debe ser $n - q = p$.

■

Observemos que si $n = k^2$ y $n > 4$, entonces $k < \frac{n}{2}$ y que para p y q primos existen $a, b \in \mathbf{Z}$ tales que $ap + bq = 1$.

Ahora damos una condición suficiente para que un cuadrado par sea la suma de dos primos.

COROLARIO 4.13 *Sean $n = k^2$ par, p y q primos tales que $3 \leq q$ y $n - k < p < n$. Si $p - kq = 1$, entonces $n = p + q$.*

Demostración: Sea $x \in \mathbf{Z}$ tal que $p + x = n$, entonces

$$k^2 = (p-1) + (x+1) = kq + (x+1)$$

por tanto $k|x+1$.

Pero $0 < x + 1 \leq k$ (ya que si $x + 1 > k$, entonces $k^2 = (p-1) + (x+1) > (p-1) + k$ y por tanto $p > k^2 - k > p - 1$!), por tanto debe ser $x + 1 = k$.

Luego $k^2 = kq + k = k(q+1)$ y $k = q + 1$, de donde se tiene que $x = q$ y $n = p + q$.

■

OBSERVACION: Dado que $n = k^2$ es par, se tiene que k es par y por tanto la expresión $p - kq$ es impar (ya que p y q lo son). Así tiene sentido afirmar que: $p - kq = 1$.

Finalmente, tenemos la contraparte de los corolarios 4.11 y 4.12 para la conjetura que dice:

"Cada entero par (>2) es la diferencia de dos primos".

COROLARIO 4.14 *Sea n un entero positivo par, p y q primos (≥ 3) tales que $n, q < p$. Se tiene:*

$$n = p - q \text{ si, y sólo si, } |G(n+q,p)| = p.$$

Demostración: Si $n = p - q$, entonces

$$G(n+q,p) = G(p,p) = p.$$

Inversamente, supongamos que $n \neq p-q$.

Luego debe ser $(n+q,p) = 1$ (pues si $p|n+q$, entonces como $n+q < 2p$ se tendría que $n+q = p$!).

Así por (2) del teorema 4.10:

$$G(n+q,p) = \sqrt{p}\left(\frac{n+q}{p}\right) e^{\frac{\pi i}{4}(1-p)}$$

y entonces $|G(n+q,p)| = \sqrt{p}$!.

■

COROLARIO 4.15 *Sea n un entero positivo par, p y q primos (≥ 3) tales que $n, q < p$ y $p \equiv 3 \pmod 4$. Se tiene:*

$$n = p - q \text{ si, y sólo si, } \left(\frac{n}{p}\right) = -\left(\frac{q}{p}\right) \text{ y } p \nmid f(-q).$$

Demostración: Si $n = p - q$, entonces $n \equiv -q \pmod p$ y por tanto

$$\begin{aligned}\left(\frac{n}{p}\right) &= \left(\frac{-q}{p}\right) \\ &= \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) \\ &= (-1)^{\frac{1}{2}(p-1)}\left(\frac{q}{p}\right) \text{ (por 4.9)} \\ &= -\left(\frac{q}{p}\right) \text{ (ya que } p \equiv 3 \pmod 4).\end{aligned}$$

Ahora

$$\begin{aligned}f(-q) = f(n-p) &= (n-p)^k + (n-p)^{k-1}n + \cdots + (n-p)n^{k-1} + n^k \\ &\equiv n^k + n^{k-1}n + \cdots + nn^{k-1} + n^k = \frac{1}{2}(p-1)n^{\frac{1}{2}(p-1)} \pmod p\end{aligned}$$

y como $p \nmid \frac{1}{2}(p-1)$ y $p \nmid n$ (ya que $p \neq q$), entonces $p \nmid f(-q)$.

Inversamente, por el teorema 4.9:

$$\left(\frac{n}{p}\right) \equiv n^{\frac{1}{2}(p-1)} \pmod{p}$$

y

$$\left(\frac{q}{p}\right) \equiv q^{\frac{1}{2}(p-1)} \pmod{p}$$

por tanto

$$n^{\frac{1}{2}(p-1)} \equiv -q^{\frac{1}{2}(p-1)} \pmod{p}$$

es decir, p divide a $n^{\frac{1}{2}(p-1)} + q^{\frac{1}{2}(p-1)}$.

Como $p \equiv 3 \pmod 4$ se tiene que $\frac{1}{2}(p-1)$ es impar, así

$$\begin{aligned} n^{\frac{1}{2}(p-1)} + q^{\frac{1}{2}(p-1)} &= (n+q)(n^k - n^{k-1}q + \cdots - nq^{k-1} + q^k) \\ &= (n+q)(n^k + n^{k-1}(-q) + \cdots + n(-q)^{k-1} + (-q)^k) \\ &= (n+q)f(-q) \end{aligned}$$

como $p \not| f(-q)$, entonces $p|n+q$. Pero $0 < n+q < 2p$. por lo tanto $n+q = p$. ∎

BIBLIOGRAFIA

1) Ahlfors L.V. *Complex Analysis.* Editorial McGraw-Hill.

2) Apostol T.M. *Análisis Matemático.* Editorial Reverté, S.A.

3) Apostol T.M. *Introducción a la Teoría Analítica de los Números.* Editorial Reverté, S.A.

4) Conway J.B. *Functions of one Complex Variable.* Editorial Springer-Verlag.

5) Chandrasekharan K. *Elliptic Functions.* Editorial Springer-Verlag.

6) Koblitz N. *Introduction to Elliptic Curves and Modular Forms.* Editorial Springer-Verlag.

7) Markushevich A. *Teoría de las Funciones Analíticas.* Tomos I y II. Editorial Mir.