FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Sumas de Cuadrados y Formas Modulares

Juan Carlos Regueiro García

Curso 2023/2024

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRADO DE MATEMÁTICAS

Traballo Fin de Grado

Sumas de Cuadrados y Formas Modulares

Juan Carlos Regueiro García

Julio, 2024

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Trabajo propuesto

Área de Conocimiento: Ánalise matemática
Título: Sumas de cadrados e formas modulares
Breve descripción del contenido
O obxectivo deste traballo é responder a algunhas preguntas clásicas da teoría de números desde o punto de vista da análise complexa: (1) Que enteiros positivos se poden escribir como suma de dous ou tres cadrados? (2) É todo enteiro positivo unha suma de catro cadrados? Para facermos iso, aproximarémonos a estas cuestións mediante a teoría de formas modulares, funcións definidas no semiplano superior e que admiten diferentes simetrías. Segundo o interese do/a alumno/a, poderán explorarse diferentes xeneralizacións desta cuestión tanto desde un punto de vista alxébrico como analítico.
Recomendaciones
Interese do alumno/a polas cuestións de teoría de números e as aplicacións das técnicas propias da análise matemática para darlles resposta, especialmente as vencelladas coa variable complexa.
Otras observaciones

Índice

Resumen

El objetivo de este Trabajo Fin de Grado es responder a algunas de las preguntas clásicas de la teoría de números, como qué enteros positivos se pueden escribir como la suma de dos cuadrados o si todo entero positivo se puede expresar como la suma de cuatro cuadrados. Estas preguntas se afrontan desde el punto de vista del análisis complejo utilizando la teoría de formas modulares. Estas son funciones definidas en el semiplano superior que admiten diferentes simetrías. En concreto, se emplea la función theta de Jacobi. Primero, se introducen definiciones que resultan de interés para la comprensión de los argumentos posteriores y una serie de resultados que se van a utilizar en las demostraciones presentadas al dar respuesta a las cuestiones. Luego, se define la función theta de Jacobi y se recogen algunas propiedades de esta que serán de interés en el desarrollo de las respuestas a las preguntas. A continuación, se desarrollan las demostraciones de los teoremas de los dos, los cuatro y los ocho cuadrados de acuerdo con los enunciados propuestos por Jacobi, empleando la teoría de formas modulares y la función theta de Jacobi para probar la equivalencia de las propiedades estructurales de esta última con las de otras funciones definidas para demostrar los teoremas. Además, se presenta una idea de la demostración del teorema de los tres cuadrados, cuyo tratamiento es más complejo.

Abstract

The aim of this Final Degree Project is to answer some of the classic questions in Number Theory, such as which positive integers can be written as the sum of two squares or whether all positive integers are the sum of four squares. These questions are addressed from the point of view of Complex Analysis by means of the theory of modular forms. These are functions defined in the upper half-plane that admit different symmetries. Specifically, the Jacobi theta function will be used. First, definitions that are of interest for the comprehension of subsequent arguments are introduced, together with a series of results that are used when answering these questions. Then, the Jacobi theta function is defined, together with its properties that will later be used. Then, the proofs of the sum of two squares theorem, the sum of four squares and the sum of eight squares theorem according to Jacobi are presented, using the theory of modular forms and Jacobi theta function to prove the equivalence of the structural properties of the latter with other functions defined specifically to prove each theorem. Furthermore, an idea of the proof of the sum of three squares theorem, the treatment of which is more complex, is presented.

Introducción

El objetivo de este trabajo es dar respuesta a algunas de las cuestiones clásicas de la teoría de números que surgieron en la Antigua Grecia. Se busca saber qué enteros positivos se pueden escribir como la suma de dos cuadrados y si todos los enteros positivos se pueden expresar como la suma de cuatro cuadrados. La respuesta a estas cuestiones aparece recogida por Diofanto de Alejandría en su *Arithmetica* [2], pero sin una demostración del resultado. De hecho, las primeras demostraciones no llegarían hasta quince siglos más tarde.

En el primer capítulo se presentan algunas definiciones que sirven para recordar al lector algunos de los conceptos básicos que se emplean en capítulos posteriores. Adicionalmente, en el capítulo figura una serie de resultados que se emplean en demostraciones de capítulos posteriores y no tienen una relación directa con la teoría de formas modulares. Algunos son resultados básicos del análisis complejo, mientras que otros tienen relación con las transformadas de Fourier y las sumas de Poisson o con las series de Eisenstein.

En el segundo capítulo, se define la función theta de Jacobi, que es una función de dos variables complejas, y se presentan algunas de sus propiedades. También se considera el caso en el que se fija una de sus variables, ya que es este el que se emplea al dar respuesta a las preguntas de teoría de números alrededor de las que gira este trabajo. Luego, se presentan algunos resultados que se emplean en las demostraciones de los teoremas de suma de cuadrados. Un tratamiento más genérico del problema se puede hallar en textos como [4] o [5].

En el tercer capítulo se presenta el teorema de los dos cuadrados por el enunciado dado por Jacobi: *Sea n un entero positivo y sean $d_1(n)$ y $d_3(n)$ los divisores de n de la forma $4k+1$ y $4k+3$, respectivamente. Entonces, el número de expresiones de n como suma de dos cuadrados es $4\,(d_1(n) - d_3(n))$. En particular, un número es suma de dos cuadrados si, y solamente si, todos sus divisores primos de la forma $4k+3$ aparecen con exponente par en su descomposición.* Por ejemplo, para $n = 5$, se tiene que $d_1(n) = 2$ y $d_3(n) = 0$, por lo que hay 8 descomposiciones posibles: $2^2 + 1^2$, $2^2 + (-1)^2$, $(-2)^2 + 1^2$, $(-2)^2 + (-1)^2$, $1^2 + 2^2$, $1^2 + (-2)^2$, $(-1)^2 + 2^2$, $(-1)^2 + (-2)^2$. Del mismo modo, para $n = 7$ se tiene que $d_1(n) = d_3(n) = 1$, por lo que el número de posibles representaciones es cero. Para su demostración se expresa el enunciado en términos de la función theta de Jacobi y se prueba que las propiedades estructurales del cuadrado de esta son equivalentes a la función dada por este nuevo enunciado del teorema de los dos cuadrados. Al final del capítulo se discute el comportamiento asintótico del número de posibles descomposiciones en suma de dos cuadrados. Se comprueba que existe una cantidad infinita de valores para las que se tiene un número concreto de descomposiciones, a la vez que el límite superior del número de descomposiciones diverge.

En el cuarto capítulo, se presenta el enunciado del teorema de los tres cuadrados: *Todo entero positivo puede expresarse como la suma de tres cuadrados si, y solo si, dicho entero no es de la forma* $4^r(8m+7)$, *con* $r, m \geq 0$. La complejidad de los cálculos necesarios para completar esta demostración llevan a solo presentar una idea de la demostración desde un punto de vista algebraico. La demostración de que los enteros de la forma $4^r(8m+7)$ no se pueden representar como la suma de tres cuadrados es sencilla, pero ver que los demás enteros sí se pueden representar como la suma de tres cuadrados es lo que presenta más dificultades.

En el quinto capítulo se presenta el teorema de los cuatro cuadrados, también por el enunciado dado por Jacobi: *Todo entero positivo se puede expresar como la suma de cuatro cuadrados y, además, el número de formas en las que esto se puede hacer es igual a ocho veces la suma de todos los divisores de dicho entero positivo que no son divisibles por cuatro.* Esta expresión de las formas en las que un entero positivo se puede expresar como la suma de cuatro cuadrados se expresa en términos de la función theta de Jacobi. Su prueba se basa en demostrar la equivalencia en las propiedades estructurales de la cuarta potencia de la función theta de Jacobi y una función definida como una variante de las series de Eisenstein. Al final del capítulo se discute el comportamiento asintótico del número de posibles descomposiciones como la suma de cuatro cuadrados de forma análoga al caso de los dos cuadrados. Se concluye con un resultado equivalente al teorema de los cuatro cuadrados, al que se llega evitando el uso de las formas modulares.

El último capítulo presenta el teorema de los ocho cuadrados, cuyo enunciado expresa lo siguiente: *Todo entero positivo se puede expresar como la suma de ocho cuadrados y, además, el número de formas en las que esto se puede hacer es igual a dieciséis veces la suma de la potencia tercera de todos los divisores de dicho entero positivo que no son divisibles por cuatro.* El tratamiento es muy similar al presentado en la prueba del teorema de los cuatro cuadrados e incluso algo más sencillo al trabajar con una serie convergente.

Capítulo 1

Definiciones y resultados previos

Primero se presenta una serie de definiciones y de teoremas que van a ser empleados en demostraciones de los siguientes capítulos y juegan un papel fundamental en la comprensión de estas. Las demostraciones detalladas de estos resultados, así como un tratamiento más exhaustivo de los diferentes temas, se puede ver por ejemplo en [1], [3], [6] o [7].

Se presentan unos conceptos básicos del análisis complejo como son el de función holomorfa y función entera. Estos conceptos aparecen a lo largo del trabajo en múltiples ocasiones y por ello se le recuerda al lector cómo se definen.

Definición 1.1. Sea U un abierto del plano complejo y $f : U \subset \mathbb{C} \to \mathbb{C}$ una función. Se dice que f es holomorfa en un punto z_0 de U si f es $\mathbb{C}$-diferenciable en todos los puntos de un entorno del punto z_0. Se dice que f es holomorfa en U si lo es en cada punto de U. Se dice que la función f es entera si $U = \mathbb{C}$.

Un resultado básico en análisis que se emplea en el capítulo 2 es el criterio mayorante de Weierstrass, que se presenta a continuación.

Teorema 1.2. ***(Criterio mayorante de Weierstrass)*** *Sea $\{f_n\}_{n=0}^{\infty}$ una sucesión de funciones definida en un subconjunto D de $\mathbb{R}$ con valores en $\mathbb{R}$ y sea $\{M_n\}_{n=0}^{\infty}$ una sucesión de números reales positivos tales que $|f_n(x)| \leq M_n$, para $x \in D$ y $n \in \mathbb{N}$. Si la serie $\sum M_n$ es convergente, entonces $\sum f_n$ converge uniformemente en D.*

En la demostración del Teorema 2.1 se emplea un resultado que se deduce del Teorema de Morera y por ello se presenta su enunciado.

Teorema 1.3. ***(de Morera)*** *Sean U un abierto del plano complejo y f una función continua en U tal que $\int_{\partial\Delta} f = 0$ para toda región triangular Δ contenida en U, donde $\partial\Delta$ denota la frontera de Δ. Entonces f es holomorfa en U.*

Corolario 1.4. *Sea* $\{f_n\}_{n=0}^{\infty}$ *una sucesión de funciones holomorfas definidas en un dominio* $D \subset \mathbb{C}$ *que convergen uniformemente a una función* f*. Entonces,* f *también es holomorfa.*

Se presentan las definiciones de algunas singularidades que aparecen a lo largo del trabajo. El concepto de polo cobra relevancia en el capítulo 2, mientras que el de singularidad evitable es relevante en las demostraciones de los dos teoremas de sumas de cuadrados que se tratan.

Definición 1.5. Sea $f \in \mathcal{H}(D(z_0; R) \setminus \{z_0\})$, con $\mathcal{H}$ el conjunto de las funciones holomorfas en una cierta región del plano complejo, y $\sum_{n=-\infty}^{\infty} a_n(z-z_0)^n$ su desarrollo en serie de Laurent en dicho entorno. Se dice que la función f presenta en z_0 un polo si la parte principal de la serie tiene un número finito de términos no nulos, esto es, si $a_{-n} = 0$ para casi todo $n \in \mathbb{N}$. En este caso, si n_0 es el mayor número natural que cumple que $a_{-n_0} \neq 0$, se dice que el polo es de orden n_0.

Se dice que la función f presenta en z_0 una singularidad evitable si la parte principal de la serie es nula, esto es, $a_{-n} = 0$ para todo $n \in \mathbb{N}$.

Las definiciones de función doblemente periódica y de función elíptica se usan en algunas de las demostraciones de propiedades asociadas con la función theta de Jacobi y por eso se le presentan al lector.

Definición 1.6. Una función $f(z)$ con $z \in \mathbb{C}$ se dice doblemente periódica si existen dos números no nulos ω_1 y ω_2, cuyo cociente no es real puro, tales que para $n, m \in \mathbb{Z}$ se cumple que $f(z + n\omega_1) = f(z)$ y $f(z + m\omega_2) = f(z)$, para todo valor de z para el que $f(z)$ existe.

Definición 1.7. Una función elíptica es una función doblemente periódica que es analítica (excepto en los polos) y no tiene más singularidades que polos en una región finita del plano complejo.

Se presenta la definición de la transformada de Fourier de una función, que juega un papel crucial en la demostración del teorema de los dos cuadrados [6,7] .

Definición 1.8. Sea $f : \mathbb{R} \longrightarrow \mathbb{C}$ una función integrable. La transformada de Fourier de f es la función $\hat{f} : \mathbb{R} \longrightarrow \mathbb{C}$ dada por:

$$\hat{f}(s) = \int_{\mathbb{R}} e^{-2\pi i s t}\, f(t)dt.$$

Esta integral converge bajo la hipótesis de que f es integrable, por lo que la transformada de Fourier está bien definida.

El teorema por el que se establece la fórmula de las sumas de Poisson se presenta a continuación. Esta fórmula permite obtener resultados que posteriormente se emplearán en los capítulos 2 y 3.

Teorema 1.9. ***(Fórmula de las sumas de Poisson)***

Sea $f : \mathbb{R} \longrightarrow \mathbb{C}$ una función de clase infinito que cumple que, para todo N, cuando $x \longrightarrow \infty$, $|f(x)| \ll |x|^{-N}$, donde $\ll$ denota que $|f(x)|$ es mucho menor que $|x|^{-N}$. Entonces,

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \hat{f}(n).$$

La siguiente proposición y su corolario son clave a la hora de demostrar el Teorema 2.6, que es necesario para la demostración del teorema de los dos cuadrados.

Proposición 1.10. *La función de Schwartz $g(t) = e^{-\pi x^2}$ es su propia transformada de Fourier.*

Corolario 1.11. *Para valores fijos de $t > 0$ y $a \in \mathbb{R}$, el cambio de variables $x^{1/2}(x + a)$ muestra que la transformada de Fourier de la función $f(x) = e^{-\pi t(n+a)^2}$ es $\hat{f}(\xi) = t^{-1/2}e^{-\pi\xi^2/t}e^{2\pi i a\xi}$. Además, considerando la fórmula de las sumas de Poisson se tiene la siguiente identidad:*

$$\sum_{n=-\infty}^{\infty} e^{-\pi t(n+a)^2} = \sum_{n=-\infty}^{\infty} t^{-1/2}e^{-\pi n^2/t}e^{2\pi i a n}. \tag{1.1}$$

Los dos resultados siguientes también son fundamentales a la hora de probar el teorema de los dos cuadrados.

Proposición 1.12. *La función de $g(t) = \frac{1}{\cosh(\pi x)}$ es su propia transformada de Fourier.*

Corolario 1.13. *Para valores fijos de $t > 0$ y $a \in \mathbb{R}$, la transformada de Fourier de la función $f(x) = \frac{e^{-2\pi i a x}}{\cosh(\pi x/t)}$ es $\hat{f}(\xi) = \frac{t}{\cosh(\pi(\xi+a)/t)}$. Además, considerando la fórmula de las sumas de Poisson, se tiene la siguiente identidad:*

$$\sum_{n=-\infty}^{\infty} \frac{e^{-2\pi i a n}}{\cosh(\pi n/t)} = \sum_{n=-\infty}^{\infty} \frac{t}{\cosh(\pi(n+a)/t)}. \tag{1.2}$$

La siguiente proposición y, en concreto, la equivalencia entre las dos primeras propiedades presentadas en esta, son indispensables para la prueba de uno de los resultados que permite demostrar el teorema de los dos cuadrados.

Proposición 1.14. *Sea $f \in \mathcal{H}(D(z_0; R) \setminus \{z_0\})$. Las siguientes propiedades son equivalentes:*

1. *f tiene en z_0 una singularidad evitable.*
2. *Existe $\lim_{z\to z_0} f(z) \in \mathbb{C}$.*
3. *Existe una función $g \in \mathcal{H}(D(z_0; R))$ tal que $g|_{D(z_0;R)\setminus\{z_0\}} = f$.*
4. *Existe un entorno W de z_0 tal que $f(W \setminus \{z_0\})$ es acotado.*

El principio del módulo máximo y la aplicación de su corolario son una de las claves para poder probar el último de los teoremas necesarios para la demostración del teorema de los dos cuadrados.

Teorema 1.15. ***(Principio del módulo máximo)*** *Si f es una función holomorfa no constante en un conjunto abierto Ω, entonces $|f|$ no puede alcanzar un máximo en Ω.*

Corolario 1.16. *Sea $\bar{\Omega}$ la clausura compacta de una región Ω. Si f es holomorfa en Ω y continua en $\bar{\Omega}$, entonces:*

$$\sup_{z\in\Omega} |f(z)| \leq \sup_{z\in\bar{\Omega}-\Omega} |f(z)| .$$

Al presentar la idea de la demostración del teorema de los tres cuadrados, se emplea el concepto de forma cuadrática ternaria. Su definición se presenta a continuación.

Definición 1.17. Una forma cuadrática ternaria es un polinomio

$$f(x_1, x_2, x_3) = \sum_{i,j=1}^{3} a_{ij} x_i x_j,$$

donde todo elemento a_{ij} es un número entero y $a_{ij} = a_{ji}$ para todo $i, j \in \{1, 2, 3\}$

En representación matricial, se tiene que:

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{21} & a_{31} \\ a_{12} & a_{22} & a_{32} \\ a_{13} & a_{23} & a_{33} \end{pmatrix}.$$

A continuación se presenta el conocido como teorema de Sylvester, que permite caracterizar cuándo una forma cuadrática es definida positiva mirando los menores principales.

Teorema 1.18. *Una forma cuadrática ternaria $f(x_1, x_2, x_3) = \sum_{i,j=1}^{3} a_{ij}x_i x_j$ es definida positiva si, y solo si $a_{11} > 0, \quad b = \begin{vmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{vmatrix} > 0, \quad d > 0$, donde d denota al determinante de la forma cuadrática.*

El siguiente resultado es clave para poder concluir la demostración del teorema de los tres cuadrados. Esto se extrae como consecuencia del teorema de clasificación de formas cuadráticas sobre los reales.

Teorema 1.19. *Toda forma cuadrática ternaria definida positiva y con determinante 1 es equivalente a la suma de tres cuadrados.*

En el cálculo técnico del que solo se da una idea en la demostración del teorema de los tres cuadrados, una de las claves son los símbolos de Jacobi, que se definen en función de los símbolos de Legendre. La definición de los símbolos de Legendre se presenta a continuación:

Definición 1.20. Los símbolos de Legendre $\left(\frac{a}{p_r}\right)$ se definen como 0 si a es múltiplo de p_r, 1 si a es un residuo cuadrático no nulo y -1 si a no es residuo cuadrático.

Las series de Eisenstein y el caso concreto de las *series prohibidas* de Eisenstein son la piedra angular sobre la que se apoya la demostración del teorema de los cuatro cuadrados y por ello se presentan sus definiciones.

Definición 1.21. Las series de Eisenstein de orden k están definidas por

$$E_k(\tau) = \sum_{(n,m)\neq(0,0)} \frac{1}{(n+m\tau)^k},$$

cuando k es un entero tal que $k \geq 3$ y τ es un número complejo con $\Im(\tau) > 0$.

Considerando que $\omega = n + m\tau$, si Λ es el retículo generado por 1 y τ, entonces otra expresión para la serie de Eisenstein es $\sum_{\omega\in\Lambda^*} 1/\omega^k$, donde $\omega \in \Lambda^*$ denota los punto del retículo diferentes de $(0,0)$.

Definición 1.22. La *serie prohibida* de Eisenstein se define, teniendo en cuenta que las sumas se hacen en el orden indicado con $(n,m) \neq (0,0)$, como:

$$F(\tau) = \sum_m \left(\sum_n \frac{1}{(m\tau+n)^2} \right).$$

Una de las proposiciones necesarias para probar el teorema de los cuatro cuadrados emplea el corolario del siguiente teorema en la demostración presentada en este trabajo.

Teorema 1.23. *Si $k \geq 4$ es par y se tiene que $\Im(\tau) > 0$, entonces:*

$$E_k(\tau) = 2\zeta(k) + \frac{2(-1)^{k/2}(2\pi)^k}{(k-1)!} \sum_{r=1}^{\infty} \sigma_{k-1}(r) e^{2\pi i\tau r},$$

donde ζ es la función zeta y $\sigma_n(r)$ es la función divisor, que se define como la suma de las n-ésimas potencias de los divisores de r.

Corolario 1.24. *La doble suma que define F converge en el orden indicado. Se tiene que*

$$F(\tau) = 2\zeta(2) - 8\pi^2 \sum_{r=1}^{\infty} \sigma(r) e^{2\pi i\tau r},$$

donde $\sigma(r) = \sum_{d|r} d$ es la suma de los divisores de r.

Para la derivación logarítmica que se hace en la demostración del teorema de los cuatro cuadrados se tiene en cuenta la siguiente proposición.

Proposición 1.25. *Se supone que $\{F_n\}$ es una sucesión de funciones holomorfas en un conjunto abierto Ω. Si existen constantes $c_n > 0$ tal que, para todo $z \in \Omega$,*

$$\sum c_n < \infty \quad y \quad |F_n(z) - 1| \leq c_n,$$

entonces:

1. *El producto $\prod_{n=1}^{\infty} F_n(z)$ converge uniformemente en Ω a una función holomorfa $F(z)$.*
2. *Si $F_n(z)$ no se anula para ningún n, entonces*

$$\frac{F'(z)}{F(z)} = \sum_{n=1}^{\infty} \frac{F_n'(z)}{F_n(z)}.$$

Capítulo 2

La función theta de Jacobi

De forma general, se define la función theta de Jacobi como:

$$\Theta\left(z|\,\tau\right) = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 \tau 2}, \quad z \in \mathbb{C}, \quad \tau \in \mathbb{H}, \tag{2.1}$$

donde $\mathbb{H}$ se define como $\mathbb{H} = \{z \in \mathbb{C} : \ \Im(z) > 0\}$, con $\Im(z)$ la parte imaginaria de $z \in \mathbb{C}$.

La función theta de Jacobi es una función de dos variables complejas. Sin embargo, va a resultar de especial interés en posteriores demostraciones el caso concreto en el que se fija el valor de z y, por tanto, solo es función de τ:

$$\theta\left(\tau\right) = \ \Theta\left(0|\,\tau\right) = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 \tau}, \quad \tau \in \mathbb{H}. \tag{2.2}$$

De todas formas, para caracterizar esta función se estudian primero las propiedades estructurales básicas de Θ como función de z, tomando un valor fijo de τ.

Proposición 2.1. *La función Θ cumple las siguientes propiedades:*

1. *Θ es entera en $z \in \mathbb{C}$ y holomorfa en $\tau \in \mathbb{H}$.*
2. $\Theta\left(z+1|\,\tau\right) = \ \Theta\left(z|\,\tau\right).$
3. $\Theta\left(z+\tau|\,\tau\right) = \ \Theta\left(z|\,\tau\right) e^{-\pi i \tau} e^{-2\pi i z}.$
4. $\Theta\left(z|\,\tau\right) = 0$ *si* $z = \frac{1}{2} + \frac{\tau}{2} + n + m\tau,$ *con* $n, m \in \mathbb{Z}$.

Demostración. Se considera que $\Im(\tau) = t \geq \ t_0 > 0$ y que $z \in \mathbb{C}$ pertenece a un conjunto acotado en $\mathbb{C}$ de tal forma que $|z| \leq \ M$, donde M es una constante real positiva. A partir de esto es posible acotar la serie funcional por una serie de números absolutamente convergente de la siguiente forma:

$$\sum_{n=-\infty}^{\infty} \left| e^{\pi i n^2 \tau} \cdot e^{2\pi i n z} \right| \leq 2 \cdot \sum_{n\geq 0} e^{-\pi n^2 t_0} \cdot e^{2\pi n M} < \infty.$$

El valor absoluto de la sucesión de funciones está acotado por un número real positivo para todo su dominio y la serie de la cota es absolutamente convergente en $\mathbb{R}$. A partir del Teorema de Morera se extrae como corolario que el límite localmente uniforme de funciones holomorfas es holomorfo. De esta forma, se tiene que $\Theta\left(\cdot|\,\tau\right)$ es entera para cada $\tau \in \mathbb{H}$ fijo y que $\Theta\left(z|\,\cdot\right)$ es holomorfa en el semiplano superior para cada $z \in \mathbb{C}$ fijo. Así el punto 1) queda demostrado.

$$e^{2\pi i n(z+1)} = e^{2\pi i n z} \cdot e^{2\pi i n} = e^{2\pi i n z} \cdot \left(e^{2\pi i}\right)^n = e^{2\pi i n z}.$$

Así, se tiene que $\Theta\left(z+1|\,\tau\right) = \Theta\left(z|\,\tau\right)$ y el punto 2) queda demostrado. Se toma la expresión de $\Theta\left(z+\tau|\,\tau\right)$ y se completan cuadrados.

$$\begin{aligned}
\Theta\left(z+\tau|\,\tau\right) &= \sum_{n=-\infty}^{\infty} e^{\pi i n^2 \tau} \cdot e^{2\pi i n(z+\tau)} = \sum_{n=-\infty}^{\infty} e^{\pi i\left(n^2+2n\right)\tau} \cdot e^{2\pi i n z} \cdot e^{\pi i \tau} \cdot e^{-\pi i \tau} \\
&= \sum_{n=-\infty}^{\infty} e^{\pi i\left(n^2+2n+1\right)\tau} \cdot e^{2\pi i n z} \cdot e^{-\pi i \tau} \\
&= \sum_{n=-\infty}^{\infty} e^{\pi i (n+1)^2\tau} \cdot e^{2\pi i n z} \cdot e^{-\pi i \tau} \cdot e^{2\pi i z} \cdot e^{-2\pi i z} \\
&= \sum_{n=-\infty}^{\infty} e^{\pi i (n+1)^2\tau} \cdot e^{2\pi i (n+1) z} \cdot e^{-\pi i \tau} \cdot e^{-2\pi i z} \\
&= \Theta\left(z|\,\tau\right) \cdot e^{-\pi i \tau} \cdot e^{-2\pi i z}.
\end{aligned}$$

Así, se tiene que $\Theta\left(z+\tau|\,\tau\right) = \Theta\left(z|\,\tau\right) e^{-\pi i \tau} e^{-2\pi i z}$ y el punto 3) queda demostrado.

Se quiere calcular $\Theta\left(\frac{1}{2} + \frac{\tau}{2} + n + m\tau\middle|\,\tau\right)$, con $n, m \in \mathbb{Z}$. Aplicando la propiedad 2) n veces, se tiene que es suficiente con calcular $\Theta\left(\frac{1}{2} + \frac{\tau}{2} + m\tau\middle|\,\tau\right)$. Aplicando ahora la propiedad 3) m veces, se tiene que basta con calcular $\Theta\left(\frac{1}{2} + \frac{\tau}{2}\middle|\,\tau\right)$.

$$\Theta\left(\frac{1}{2} + \frac{\tau}{2}\middle|\,\tau\right) = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 \tau} \cdot e^{2\pi i n\left(\frac{1}{2}+\frac{\tau}{2}\right)} = \sum_{n=-\infty}^{\infty} e^{\pi i (n^2+n)\tau} \cdot e^{\pi i n} = \sum_{n=-\infty}^{\infty} e^{\pi i (n^2+n)\tau} \cdot (-1)^n.$$

Es suficiente con encontrar dos términos para cada $n \geq 0$ que tengan la misma expresión de la exponencial presentada previamente, pero paridad opuesta. De esta forma se le asocia a cada término n el término $-n-1$, ya que $(-n-1)^2 + (-n-1) = n^2 + n$. Así, cada término del sumatorio se anula y la propiedad 4) queda demostrada. $\square$

A continuación, se considera un producto $\Pi(z|\,\tau)$, que comparte las mismas propiedades estructurales que $\Theta\,(z|\,\tau)$ como función de z:

$$\Pi\,(z|\,\tau) = \prod_{n=1}^{\infty}\left(1-q^{2n}\right)\left(1+q^{2n-1}e^{2\pi iz}\right)(1+q^{2n-1}e^{-2\pi iz}),\ \text{con}\ q = e^{\pi i\tau}. \tag{2.3}$$

Proposición 2.2. *La función* Π *cumple las siguientes propiedades:*

1. Π *es entera en* $z \in \mathbb{C}$ *y holomorfa en* $\tau \in \mathbb{H}$.
2. $\Pi\,(z+1|\,\tau) = \Pi\,(z|\,\tau)\,.$
3. $\Pi\,(z+\tau|\,\tau) = \Pi\,(z|\,\tau)\,e^{-\pi i\tau}e^{-2\pi iz}$.
4. $\Pi\,(z|\,\tau) = 0$ *si* $z = \frac{1}{2} + \frac{\tau}{2} + n + m\tau$, *con* $n,\ m \in \mathbb{Z}$. *Además, estos puntos son los únicos ceros simples de* $\Pi\,(\cdot|\,\tau)\,.$

Demostración. Se considera que $\Im(\tau) = t \geq t_0 > 0$ y que $z \in \mathbb{C}$. De esta forma, $|q| \leq e^{\pi t_0} < 1$ y $\left(1-q^{2n}\right)\left(1+q^{2n-1}e^{2\pi iz}\right)(1+q^{2n-1}e^{-2\pi iz}) = 1 + O(|q|^{2n-1}e^{2\pi|z|})$.

Como $\sum |q|^{2n-1}$ converge, se tiene que $\Pi\,(z|\,\tau)$ define una función entera en $z \in \mathbb{C}$ con $\tau \in \mathbb{H}$ fijo y una función holomorfa en $\tau \in \mathbb{H}$ con $z \in \mathbb{C}$ fijo. Así, queda demostrada la propiedad 1).

De manera análoga a la propiedad 2) de la Proposición 1.2, el 1 desaparece de la exponencial porque $e^{2\pi i} = 1$. Así, la propiedad 2) queda demostrada.

Se considera que $q^2 = e^{2\pi i\tau}$. De esta forma se tiene lo siguiente:

$$\begin{aligned}\Pi\,(z+\tau|\,\tau) &= \prod_{n=1}^{\infty}\left(1-q^{2n}\right)\left(1+q^{2n-1}e^{2\pi i(z+\tau)}\right)(1+q^{2n-1}e^{-2\pi i(z+\tau)})\\ &= \prod_{n=1}^{\infty}\left(1-q^{2n}\right)\left(1+q^{2n+1}e^{2\pi iz}\right)(1+q^{2n-3}e^{-2\pi iz}) = \Pi\,(z|\,\tau)\left(\frac{1+q^{-1}e^{-2\pi iz}}{1+qe^{2\pi iz}}\right).\end{aligned}$$

Como $\frac{1+x}{1+x^{-1}} = x$, para todo $x \neq -1$, se tiene que $\Pi\,(z+\tau|\,\tau) = \Pi\,(z|\,\tau)\,e^{-\pi i\tau}e^{-2\pi iz}$. Así, la propiedad 3) queda demostrada.

Para que $\Pi\,(z|\,\tau)$ se anule, hay que demostrar que uno de sus factores se iguala a cero para $z = \frac{1}{2} + \frac{\tau}{2} + n + m\tau$. Por un lado, el término $\left(1-q^{2n}\right)$ no se va a anular nunca, ya que $|q| < 1$. El término $\left(1+q^{2n-1}e^{2\pi i(z+\tau)}\right)$ se anula cuando:

$$1 + q^{2n-1}e^{2\pi iz} = 1 + e^{\pi i\tau(2n-1)}e^{2\pi iz} = 0.$$

El segundo término de la expresión anterior debe ser -1 para que la igualdad se verifique. Expresado en su forma exponencial y tomando los exponentes se tiene:

$$\pi i\tau\,(2n-1) + 2\pi iz = \pi i \ \leftrightarrow\ \pi i\ \left[\tau\,(2n-1) + 2z - 1\right] = 0.$$

Los exponentes de la forma anterior se anulan si el término $[\tau\,(2n-1)+2z-1]$ es múltiplo de 2, ya que la exponencial es $2\pi i$-periódica.

Dividiendo entre dos la expresión anterior se obtiene una expresión equivalente siendo múltiplo de 1, esto es, un entero. De ahí se puede obtener la forma de z para la que $\Pi\,(\,z|\,\tau)=0$.

$$z = \frac{1}{2}+\frac{\tau}{2}-m\tau, \quad m\in\mathbb{Z}. \tag{2.4}$$

Por la propiedad 2), lo anterior es equivalente a la siguiente expresión:

$$z = \frac{1}{2}+\frac{\tau}{2}-m\tau+n, \quad m\geq 1, \quad n\in\mathbb{Z}\,.$$

Para el tercer factor se opera de manera análoga y se obtiene que se debe de verificar:

$$\pi i\,[\tau\,(2n-1)-2z-1] = 0.$$

El procedimiento seguido antes lleva a que:

$$z = -\frac{1}{2}-\frac{\tau}{2}+m\tau.$$

Como se tiene que para que $\Pi\,(\,z|\,\tau)=0$ la igualdad se da en módulo 1 tras operar la expresión que era múltiplo de uno, esta es equivalente a la siguiente:

$$z = \frac{1}{2}+\frac{\tau}{2}-m'\tau, \quad m'\geq 0.$$

Así, combinando las expresiones halladas para el segundo y el tercer término se tiene:

$$z = \frac{1}{2}+\frac{\tau}{2}-m\tau+n, \quad m\in\mathbb{Z}, \quad n\in\mathbb{Z}.$$

Esto da todos los ceros de $\Pi\,(\,\cdot|\,\tau)$. Ahora se expresa un término como función de τ y se calcula se derivada para comprobar que los ceros son simples. Al evaluar ambas expresiones en $\tau=0$ se obtiene que ambas son cero. De esta forma se ve que los ceros son simples y además los únicos que existen para el producto. Así, la propiedad 4) queda demostrada. □

El hecho de que el producto $\Pi\,(\,z|\,\tau)$ y la función theta compartan propiedades similares indica que puede existir cierta relación entre ambas funciones. El siguiente teorema establece dicha relación.

Teorema 2.3. ***(Fórmula del producto para la función theta)***

Para todo $z\in\mathbb{C}$ y $\tau\in\mathbb{H}$, se tiene que $\Theta\,(\,z|\,\tau)=\Pi\,(\,z|\,\tau)$.

Demostración. Se fija $\tau \in \mathbb{H}$ y se supone que existe una constante $c(\tau)$ tal que $\Theta\left(z|\,\tau\right) = c\left(\tau\right)\ \Pi\left(z|\,\tau\right).$

Si se considera el cociente $F\left(z\right) = \frac{\Theta(z|\tau)}{\Pi(z|\tau)}$, como ambos elementos del cociente son funciones enteras, el cociente también lo es. Además, ambas son funciones doblemente periódicas con períodos 1 y τ, de acuerdo con las propiedades 2) y 3) de las proposiciones anteriores, por lo que el cociente también lo será. Teniendo en cuenta lo anterior, el cociente solo puede ser constante.

Entonces hay que probar que la constante $c\left(\tau\right) = 1$ y para esto se busca demostrar que $c\left(\tau\right) = c\left(4\tau\right).$

Por un lado, para obtener una expresión lo más simple posible se fija $z = \frac{1}{2}$, de manera que $e^{2\pi inz} = e^{-2\pi inz} = (-1)^n$. Así se tiene:

$$\begin{aligned}
\sum_{n=-\infty}^{\infty} q^{n^2} \cdot (-1)^n &= c\left(\tau\right) \prod_{n=1}^{\infty} \left(1 - q^{2n}\right)\left(1 - q^{2n-1}\right)(1{-}q^{2n-1}) \\
&= c\left(\tau\right) \prod_{n=1}^{\infty} \left(1 - q^{2n} - q^{2n-1} + q^{4n-1}\right)(1{-}q^{2n-1}) \\
&= c\left(\tau\right) \prod_{n=1}^{\infty} \left(1 - q^{2n} - e^{(2n-1)\pi i\tau} + e^{(4n-1)\pi i\tau}\right)(1{-}q^{2n-1}) \\
&= c\left(\tau\right) \prod_{n=1}^{\infty} \left(1 - q^{2n} - 1^{n\tau}\left(-1\right)^{\tau} + 1^{2n\tau}\left(-1\right)^{\tau}\right)(1{-}q^{2n-1}) \\
&= c\left(\tau\right) \prod_{n=1}^{\infty} \left(1 - q^{2n} - \left(-1\right)^{\tau} + \left(-1\right)^{\tau}\right)(1{-}q^{2n-1}) \\
&= c\left(\tau\right) \prod_{n=1}^{\infty} \left(1 - q^{2n}\right)(1{-}q^{2n-1}).
\end{aligned}$$

Así, se obtiene una expresión para la constante:

$$c\left(\tau\right) = \frac{\sum_{n=-\infty}^{\infty} q^{n^2}\left(-1\right)^n}{\prod_{n=1}^{\infty}\left(1 - q^n\right)(1{-}q^{2n-1})}.$$

Por otro lado, se obtiene otra expresión fijando $z = \frac{1}{4}$, de manera que $e^{2\pi iz} = i$. Así se tiene:

$$\Theta\left(\frac{1}{4}\middle|\,\tau\right) = \sum_{n=-\infty}^{\infty} q^{n^2} \cdot i^n.$$

En la serie anterior, los términos para n impar se van a anular con los términos para su opuesto, $-n$, puesto que $i^{-n} = \left(\frac{1}{i}\right)^n = (-i)^n = -i^n$.

$$\Theta\left(\frac{1}{4}\middle|\,\tau\right) = \sum_{n\ par} -2 \cdot q^{n^2} + \sum_{n\ impar} \left(i - i\right) q^{n^2} = -2 \sum_{n\ par} q^{n^2}.$$

Entonces, tomando $m = 2n$, la serie se puede expresar como:

$$\Theta\left(\frac{1}{4}\middle|\,\tau\right) = \sum_{n=-\infty}^{\infty} q^{4m^2} \cdot (-1)^m .$$

Para el producto se tiene:

$$\Pi\left(\frac{1}{4}\middle|\,\tau\right) = \prod_{m=1}^{\infty} \left(1 - q^{2m}\right)\left(1 + i\, q^{2m-1}\right)\left(1 - iq^{2m-1}\right) = \prod_{m=1}^{\infty} \left(1 - q^{2m}\right)(1{+}q^{4m-2}).$$

El factor $\left(1 - q^{2m}\right)$ se descompone dentro del productorio tras considerar que $m = 2n$ en los términos consecutivos $\left(1 + q^{4n-4}\right)\left(1 + q^{4n-2}\right)$. Los términos de la forma del segundo se pueden agrupar con los términos $\left(1 - q^{2m}\right)$ para dar lugar a términos $\left(1 - q^{4m}\right)$. Así se tiene:

$$\Pi\left(\frac{1}{4}\middle|\,\tau\right) = \prod_{m=1}^{\infty} \left(1 - q^{2m}\right)(1{+}q^{8m-4}).$$

De las dos expresiones calculadas se saca que la constante es:

$$c\,(\tau) = \frac{\sum_{n=-\infty}^{\infty} q^{4n^2}\,(-1)^n}{\prod_{n=1}^{\infty}\left(1 - q^{2n}\right)(1{-}q^{8n-4})}.$$

De las expresiones de la constante calculadas se ve que $c\,(\tau) = c\,(4\tau)$. Aplicando sucesivamente esta identidad se tiene que $c\,(\tau) = c\left(4^k\tau\right),\ k \in \mathbb{N}$. Así, como $\tau \in \mathbb{H}$, se tiene que $\lim_{k\to\infty} q^{4^k} = \lim_{k\to\infty} e^{i\pi 4^k\tau} = 0$. Entonces, en el límite en el que $k \to \infty$, el único término que no tiende a cero es el de $n = 0$, por lo que se concluye que $c\,(\tau)$, quedando el teorema demostrado. □

El siguiente corolario del teorema anterior presenta un resultado que permite concluir la demostración del teorema de los dos cuadrados.

Corolario 2.4. *Considerando que $\Im\,(\tau) > 0$ y que $q = e^{\pi i\tau}$, se tiene:*

$$\Theta\,(\tau) = \prod_{n=1}^{\infty}\left(1 - q^{2n}\right)\left(1 + q^{2n-1}\right)^2 .$$

Así, $\Theta\,(\tau) \neq 0$, para $\tau \in \mathbb{H}$.

Corolario 2.5. *Para cada $\tau \in \mathbb{H}$ fijo, el cociente $\frac{\partial^2 log\Theta(z|\tau)}{\partial z^2} = \frac{\Theta(z|\tau)\ \frac{\partial^2\Theta(z|\tau)}{\partial z^2} - \left(\frac{\partial\Theta(z|\tau)}{\partial z}\right)^2}{\Theta(z|\tau)^2}$ es una función elíptica de orden 2 con períodos 1 y τ; y con un polo doble en $z = \frac{1}{2} + \frac{\tau}{2}$.*

Demostración. Sea $F(z) = \frac{\partial log(\Theta(z|\tau))}{\partial z} = \frac{\frac{\partial\Theta(z|\tau)}{\partial z}}{\Theta(z|\tau)}$. Se considera que $\Theta\,(\,z+1|\,\tau) = \Theta\,(\,z|\,\tau)$ y diferenciando ambas expresiones respecto a z se obtiene que $\frac{\partial\Theta(z|\tau)}{\partial z} = \frac{\partial\Theta(z+1|\tau)}{\partial z}$, de donde se ve que $F(z) = F(z+1)$. También se considera que $\Theta\,(\,z+\tau|\,\tau) = \Theta\,(\,z|\,\tau)\ e^{-\pi i\tau}e^{-2\pi iz}$ y diferenciando nuevamente ambas expresiones respecto de z se obtiene que $\frac{\partial \Theta(z+\tau|\tau)}{\partial z} = (\frac{\partial \Theta(z|\tau)}{\partial z} - 2\pi i\ \Theta\left(z|\,\tau\right))\ e^{-\pi i\tau}e^{-2\pi iz}$, de donde se ve que $F(z+\tau) = F(z) - 2\pi i$. Se diferencia una vez más cada una de las expresiones obtenidas y se obtiene que $\frac{\partial^2 \Theta(z|\tau)}{\partial z^2} = \frac{\partial^2 \Theta(z+1|\tau)}{\partial z^2}$ y que $\frac{\partial^2 \Theta(z+\tau|\tau)}{\partial z^2} = (\frac{\partial^2 \Theta(z|\tau)}{\partial z^2} - 4\pi i\ \frac{\partial \Theta(z|\tau)}{\partial z} - 4\pi i\ \Theta\left(z|\,\tau\right))\ (e^{-\pi i\tau}e^{-2\pi iz})$. En el primero de los casos es directo que $\frac{\partial F(z)}{\partial z} = \frac{\partial F(z+1)}{\partial z}$. En el segundo de los casos, sin más que sustituir en la expresión de la derivada segunda se llega a que $\frac{\partial F(z)}{\partial z} = \frac{\partial F(z+\tau)}{\partial z}$. De esta forma, se ha llegado a que $\frac{\partial F(z)}{\partial z}$ es doblemente periódica. Como $\Theta\left(z|\,\tau\right)$ se anula solo en $z = \frac{1}{2} + \frac{\tau}{2}$ en el paralelogramo fundamental, la función $F(z)$ tiene un único polo y, por ello, $\frac{\partial F(z)}{\partial z}$ tiene un polo doble en ese punto. $\square$

De esta forma se concluye el estudio de las propiedades estructurales básicas de Θ como función de z. Ahora se procede al estudio del carácter modular de Θ. Para la función Θ se van a considerar las siguientes transformaciones:

$$T_2 :\ \tau\ \longmapsto\ \tau\ +\ 2,\quad S :\ \tau\ \longmapsto\ -\frac{1}{\tau},$$

puesto que $\Theta\left(z|\,\tau+2\right) = \ \Theta\left(z|\,\tau\right)$, pero $\Theta\left(z|\,\tau+1\right) \neq \Theta\left(z|\,\tau\right)$. Primero, se estudia la transformación de $\Theta\left(z|\,\tau\right)$ bajo S.

Teorema 2.6. *Si $\tau \in \mathbb{H}$, entonces $\Theta\left(z|-1/\tau\right) = \sqrt{\frac{\tau}{i}}\ e^{\pi i\tau z^2}\ \Theta\left(z\tau|\,\tau\right)$ para todo $z \in \mathbb{C}$. En esta expresión $\sqrt{\frac{\tau}{i}}$ denota la rama de la raíz cuadrada definida en la mitad superior del plano, que es positiva cuando $\tau = it,\ \ t > 0$.*

Demostración. Basta con probar la fórmula para $z = x$ real y para $\tau = it,\ \ t > 0$, ya que se tiene que para cada $x \in \mathbb{R}$, los dos lados de la fórmula son funciones holomorfas en la mitad superior del plano. Estas funciones coinciden en el eje imaginario positivo y, por ello, son iguales en todos los puntos. Para $\tau \in \mathbb{H}$ fijo, se vuelve a tener que las expresiones a los dos lados de la fórmula definen funciones holomorfas, esta vez respecto a z. Ambas coinciden en el eje real y, por ello, se tiene que coinciden en todo punto. Se considera un x real y $\tau = it$, de manera que se tiene:

$$\Theta\left(z|-1/\tau\right) = \sum_{n=-\infty}^{\infty} e^{-\pi n^2/t}\cdot e^{2\pi inx} = \sqrt{t}\ e^{-\pi \mathrm{t}x^2} \sum_{n=-\infty}^{\infty} e^{-2\pi nxt} = \sqrt{\frac{\tau}{i}}\ e^{\pi i\tau z^2}\ \Theta\left(z\tau|\,\tau\right).$$

La fórmula se puede reescribir como:

$$\sum_{n=-\infty}^{\infty} e^{-\pi t(n+x)^2} = \sqrt{t}\ e^{-\pi \mathrm{t}x^2} \sum_{n=-\infty}^{\infty} t^{-1/2}\ e^{-\pi n^2/t}\ e^{-2\pi inx}.$$

Esta expresión es la igualdad establecida en (1.1) a partir de las fórmula de las sumas de Poisson. De esta forma, la igualdad se verifica y el teorema queda probado. $\square$

Fijando $z = 0$ en el Teorema 2.6 se extrae el siguiente corolario:

Corolario 2.7. *Si* $\Im(\tau) > 0$, *entonces* $\theta\left(-1/\tau\right) = \sqrt{\frac{\tau}{i}}\,\theta\left(\tau\right).$

El siguiente corolario da información muy precisa acerca del comportamiento cuando $\tau \to 0$ y se empleará en la demostración del teorema de los dos cuadrados al determinar las propiedades estructurales de θ^2.

Corolario 2.8. *Si* $\tau \in \mathbb{H}$, *entonces* $\theta\left(1 - 1/\tau\right) = \sqrt{\frac{\tau}{i}} \cdot \sum_{n=-\infty}^{\infty} e^{\pi i (n+1/2)^2 \tau} = \sqrt{\frac{\tau}{i}}(2e^{\pi i \tau/4} + ...).$

La segunda identidad se interpreta como que $\theta\left(1 - 1/\tau\right) \sim 2\sqrt{\frac{\tau}{i}}\, e^{\pi i \tau/4}$ *cuando* $\Im\left(\tau\right) \to \infty.$

Demostración. Se tiene que n y n^2 tienen la misma paridad. Esto lleva a que se cumpla la siguiente igualdad:

$$\theta\left(1+\tau\right) = \sum_{n=-\infty}^{\infty} (-1)^n e^{\pi i n^2 \tau} = \Theta\left(1/2 |\, \tau\right).$$

De esta igualdad está claro que $\theta\left(1 - 1/\tau\right) = \Theta\left(1/2 | -1/\tau\right).$ Ahora se considera que $z = \frac{1}{2}$ y se aplica el Teorema 2.6 a la expresión de la derecha.

$$\begin{aligned}\theta\left(1 - 1/\tau\right) &= \sqrt{\frac{\tau}{i}}\; e^{\pi i \tau/4}\; \Theta\left(\tau/2 |\, \tau\right) = \sqrt{\frac{\tau}{i}}\; e^{\pi i \tau/4} \sum_{n=-\infty}^{\infty} e^{\pi i n^2 \tau} \cdot e^{\pi i n \tau} \\ &= \sqrt{\frac{\tau}{i}} \sum_{n=-\infty}^{\infty} e^{\pi i (n+1/2)^2 \tau}.\end{aligned}$$

Los términos asociados a $n = 0$ y a $n = -1$ contribuyen al sumatorio en $2 \cdot e^{\pi i \tau/4}$, que tiene un valor absoluto, considerando $\tau = \sigma + it$, de $2 \cdot e^{-\pi t/4}$. El sumatorio de los términos distintos a los dos valores de n mencionados es de orden:

$$O\left(\sum_{n=-\infty}^{\infty} e^{-(k+1/2)^2 \pi t}\right) = O\left(e^{-9\pi t/4}\right)$$

□

La última de las proposiciones se relaciona con la función eta de Dedekind, la cual se define para $\Im(\tau) > 0$ como:

$$\eta(\tau) = e^{\frac{\pi i \tau}{12}} \prod_{n=1}^{\infty} (1 - e^{2\pi i n \tau}).$$

Proposición 2.9. *Si* $\Im(\tau) > 0$, *entonces se tiene que* $\eta(-1/\tau) = \sqrt{\frac{\tau}{i}}\, \eta(\tau).$

Demostración. Se considera la fórmula del producto para la función theta como ya se ha hecho previamente, considerando de nuevo que $q = \ e^{\pi i \tau}$. Esta se reescribe extrayendo el primer término del último de los factores del productorio:

$$\Theta\left(z \middle| \tau \right) = \left(1 + qe^{-2\pi i z}\right) \prod_{n=1}^{\infty} \left(1 - q^{2n}\right) \left(1 + q^{2n-1} e^{2\pi i z}\right) \left(1 + q^{2n+1} e^{-2\pi i z}\right).$$

Como el primer factor se anula en $z_0 = \frac{1}{2} \ + \frac{\tau}{2}$, se tiene la siguiente igualdad:

$$\Theta'\left(z_0 \middle| \tau \right) = 2\pi i \ \prod_{n=1}^{\infty} \left(1 - e^{2\pi i n \tau}\right)^3 = 2\pi i \ H(\tau).$$

Se considera la expresión dada por el Teorema 2.4 sin más que sustituir $-1/\tau$ por τ:

$$\Theta\left(z \middle| \tau \right) = \sqrt{\frac{i}{\tau}} \ e^{-\pi i z^2/\tau} \ \Theta\left(-z/\tau \middle| -1/\tau \right).$$

Esta expresión se diferencia respecto a z y se evalúa nuevamente en el punto z_0, teniendo en cuenta que $\Theta\left(z_0 \middle| \tau \right) = 0$. Así, se tiene la siguiente expresión:

$$2\pi i H\left(\tau\right) = \sqrt{\frac{i}{\tau}} \, e^{-\pi i {z_0}^2/\tau} \cdot \Theta'\left(- z_0/\tau \middle| \tau \right) = \sqrt{\frac{i}{\tau}} \, e^{-\frac{\pi i}{4\tau}} e^{-\frac{\pi i}{2}} e^{-\frac{\pi i \tau}{4}} \left(\frac{-2\pi i}{\tau}\right) H\left(-1/\tau\right).$$

De la expresión anterior se tiene la siguiente expresión equivalente:

$$e^{\frac{\pi i \tau}{4}} \ H(\tau) \ = \ \left(\frac{i}{\tau}\right)^{3/2} e^{-\frac{\pi i}{4\tau}} \ H(-1/\tau).$$

Se tiene que tomando $\tau = it$, con $t > 0$, la función $\eta(\tau)$ es positiva. Esto permite tomar la raíz cúbica de la expresión anterior e introducir la función $\eta(\tau)$ en la igualdad. Tras tomar la raíz cúbica se obtiene lo siguiente:

$$e^{\frac{\pi i \tau}{12}} \ \prod_{n=1}^{\infty} \left(1 - e^{2\pi i n \tau}\right) = \sqrt{\frac{i}{\tau}} \ e^{-\frac{\pi i}{12\tau}} \ \prod_{n=1}^{\infty} \left(1 - e^{-2\pi i n/\tau}\right).$$

Por la definición de $\eta(\tau)$ se tiene que $\eta(\tau) = \sqrt{\frac{i}{\tau}} \ \eta(-1/\tau)$ y de esta forma la identidad se da para cada $\tau \in \mathbb{H}$. $\square$

Capítulo 3

El Teorema de los dos cuadrados

Los resultados del capítulo anterior sirven de base sobre la que se van a cimentar las demostraciones de los teoremas de las sumas de cuadrados. Primero se va a buscar respuesta a la pregunta de: ¿Qué enteros se pueden escribir como la suma de dos o tres cuadrados?

En la Antigua Grecia había gran interés por las ternas pitagóricas (a, b, c), números enteros vistos como lados de un triángulo que satisfacen que $a^2 = b^2 + c^2$. De acuerdo con Diofanto de Alejandría, si c es un entero de una terna pitagórica y los otros dos miembros de la terna no tienen factores en común, entonces c es la suma de dos cuadrados. Además, dicho c sería la hipotenusa de un triángulo cuyos lados estarían dados por la terna pitagórica (a, b, c). Ante esto surge de manera natural la pregunta de qué enteros se pueden escribir como la suma de dos cuadrados.

Los enteros de la forma $4k + 3$ no pueden escribirse como suma de dos cuadrados. Esto se puede comprobar de manera sencilla considerando que el entero se puede escribir como $n^2 + m^2$, con $n, m \in \mathbb{Z}$. Con esta condición, la única posibilidad que se puede dar es que uno de enteros elevados al cuadrado sea par y el otro impar. Por un lado, el cuadrado de un número par es múltiplo de 4. Por otro lado, el cuadrado de un número impar siempre da de resto 1 al ser dividido entre 4. De esta forma, está claro que un entero de la forma $4k + 3$ no podrá ser escrito como suma de cuadrados. Además, surge la cuestión de si un entero de la forma $4k + 1$ podría ser escrito como suma de cuadrados. Este no siempre será el caso, ya que, por ejemplo, 21 es un número de la forma $4k + 1$ que no puede ser expresado como la suma de dos cuadrados.

Para expresar esta pregunta de forma matemática, se define como $r_2(n)$ el número de formas en las que un número n se puede escribir como suma de dos cuadrados, esto es, la cantidad de pares (x, y), $x, y \in \mathbb{Z}$ tal que $n = x^2 + y^2$. Así, la pregunta se puede reducir a encontrar una expresión para $r_2(n)$.

Este problema es de naturaleza aditiva, pero también cuenta con un aspecto multiplicativo, ya que si dos enteros n y m se pueden escribir como suma de dos cuadrados, entonces su producto también se puede escribir como suma de dos cuadrados.

Se consideran los enteros $a, b, c, d \in \mathbb{Z}$ y dos números enteros que se pueden escribir como suma de los cuadrados de estos enteros:

$$n = a^2 + b^2, \quad m = c^2 + d^2.$$

Se considera también el número complejo:

$$x + iy = (a + ib)(c + id). \tag{3.1}$$

Está claro que tanto x como y son enteros, pues sus expresiones son sumas y productos de otros enteros.

$$x = ac - bd, \quad y = ad + bc$$

Se toma el módulo a ambos lados de la igualdad de la expresión (3.1). Por un lado, el módulo al cuadrado de $x + iy$ es $x^2 + y^2$. Por el otro, de las dos expresiones anteriores se tiene que el módulo al cuadrado de $(a + ib)(c + id)$ es:

$$\begin{aligned}
|(a + ib)(c + id)|^2 &= |(ac - bd) + i(ad + bc)|^2 = (ac - bd)^2 + (ad + bc)^2 \\
&= a^2c^2 - abcd \ + b^2d^2 + a^2d^2 + abcd + b^2c^2 \\
&= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\
&= a^2\ (c^2 + d^2) + b^2(c^2 + d^2) \\
&= (a^2 + b^2)(c^2 + d^2) = n \cdot m.
\end{aligned}$$

Así, queda demostrado que $n \cdot m = x^2 + y^2$, por lo que el producto de dos enteros que se pueden escribir como suma de dos cuadrados se puede escribir también como suma de dos cuadrados.

Por esto, las propiedades de divisibilidad de n tienen relevancia a la hora de determinar $r_2(n)$.

Se define $d_1(n)$ como el número de divisores de n de la forma $4k + 1$ y $d_3(n)$ como el número de divisores de n de la forma $4k + 3$. Así, se enuncia el siguiente Teorema como enunciado matemático que da respuesta a la pregunta del principio.

Teorema 3.1. ***(de los dos cuadrados)***

Si $n \geq 1$, *entonces* $r_2(n) = 4(d_1(n) - d_3(n))$.

Para estar en condiciones de probar el teorema, se emplea la función theta de Jacobi elevada a la segunda potencia. Las potencias pares de esta función son sencillas de manejar y, en este caso, van a permitir establecer la relación entre $r_2(n)$ y las funciones que contabilizan la cantidad de divisores de las formas $4k+1$ y $4k+3$.

Primero, se ve que la función generatriz de la sucesión $\{r_2(n)\}_{n=1}^{\infty}$ se corresponde con el cuadrado de la función θ.

$$\theta(\tau)^2 = \sum_{n=0}^{\infty} r_2(n)\; q^n, \text{ con } q = e^{\pi i \tau}, \tau \in \mathbb{H}. \tag{3.2}$$

En términos de q, la función theta de Jacobi se puede escribir de la siguiente forma:

$$\theta\left(\tau\right) = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 \tau} = \sum_{n=-\infty}^{\infty} q^{n^2}.$$

Así, teniendo en cuenta que $r_2(n)$ cuenta el número de pares (n_1, n_2) tales que $n_1^2 + n_2^2 = n$, se desarrolla el cuadrado de la función θ de la siguiente manera:

$$\theta(\tau)^2 = \left(\sum_{n_1=-\infty}^{\infty} q^{n_1^2}\right)\left(\sum_{n_2=-\infty}^{\infty} q^{n_2^2}\right) = \sum_{(n_1,n_2)\in\mathbb{Z}\times\mathbb{Z}} q^{n_1^2+n_2^2} = \sum_{n=0}^{\infty} r_2(n)\; q^n.$$

De esta forma, se ha relacionado la función generatriz de $r_2(n)$ con el cuadrado de la función theta de Jacobi. Ahora se busca escribir las funciones generatrices de $d_1(n)$ y de $d_3(n)$ como una expresión con la que se pueda operar. Esto daría una igualdad equivalente a la proporcionada por el Teorema 3.1, que sería la que se buscaría probar para demostrar el teorema de los dos cuadrados.

En la siguiente proposición se presenta una relación derivada de (3.2) y de las funciones generatrices de $d_1(n)$ y $d_3(n)$.

Proposición 3.2. *La identidad* $r_2(n) = 4(d_1(n) - d_3(n))$, $n \geq 1$, *es equivalente a las identidades:*

$$\theta(\tau)^2 = 2\sum_{n=-\infty}^{\infty} \frac{1}{q^n + q^{-n}} = 1 + 4\sum_{n=1}^{\infty} \frac{q^n}{1+q^{2n}}, \; \textit{con } q = e^{\pi i \tau}, \tau \in \mathbb{H}. \tag{3.3}$$

Demostración. Primero, se verifica que la igualdad a la derecha de la expresión (3.3) se cumple. Se consideran las siguientes relaciones, que no son más que el resultado de multiplicar el término de la primera serie por q^n o por q^{-n}.

$$\frac{1}{q^n + q^{-n}} = \frac{q^n}{1+q^{2n}} = \frac{q^{-n}}{1+q^{-2n}} = \frac{q^{|n|}}{1+q^{2|n|}}$$

Teniendo esto en cuenta, los términos de la serie para $n = k$ y para $n = -k$ son los mismos para todo $k \in \mathbb{N}$. Entonces, basta con tomar el término para $n = 0$, que es 1, y el doble de la serie desde $n = 1$ hasta el infinito.

Además, como $|q| < 1$, los términos $q^{|n|}$ convergen y, por tanto, las dos series son convergentes.

Multiplicando y dividiendo por el conjugado se tiene la siguiente igualdad:

$$\frac{1}{1+q^{2n}} = \frac{1-q^{2n}}{1+q^{4n}}.$$

Así, la expresión de la derecha de (3.3) se podría escribir de la siguiente forma:

$$1 + 4\sum_{n=1}^{\infty} \frac{q^n}{1+q^{2n}} = 1 + 4\sum_{n=1}^{\infty} \left(\frac{q^n}{1+q^{4n}} - \frac{q^{3n}}{1+q^{4n}} \right). \tag{3.4}$$

Los términos $1/(1-q^{4n})$ se pueden considerar como aquellos a los que converge una serie geométrica $\sum_{m=0}^{\infty} q^{4nm}$. Así, se tiene que:

$$\sum_{n=1}^{\infty} \frac{q^n}{1-q^{4n}} = \sum_{n=1}^{\infty}\sum_{m=0}^{\infty} q^n\, q^{4nm} = \sum_{n=1}^{\infty}\sum_{m=0}^{\infty} q^{n(4m+1)} = \sum_{k=1}^{\infty} d_1\left(k\right) q^k.$$

La última de las igualdades anteriores se tiene al considerar que $d_1\left(k\right)$ cuenta el número de divisores de k que son de la forma $4m + 1$. Adicionalmente, la serie resultante es convergente, puesto que $d_1\left(k\right) \leq\ k$.

Se procede de manera análoga con el otro término de la expresión (3.4). Así, se tiene que:

$$\sum_{n=1}^{\infty} \frac{q^{3n}}{1-q^{4n}} = \sum_{n=1}^{\infty}\sum_{m=0}^{\infty} q^{3n}\, q^{4nm} = \sum_{n=1}^{\infty}\sum_{m=0}^{\infty} q^{n(4m+3)} = \sum_{k=1}^{\infty} d_3\left(k\right) q^k.$$

La serie es de nuevo convergente debido a que $d_3\left(k\right) \leq\ k$.

Entonces, la expresión (3.4) se puede escribir así:

$$1 + 4\sum_{n=1}^{\infty} \left(\frac{q^n}{1+q^{2n}} - \frac{q^{3n}}{1+q^{2n}} \right) = 1 + 4\sum_{k=1}^{\infty} \left(d_1\left(k\right) - d_3\left(k\right)\right) q^k.$$

De esta forma, se puede expresar el cuadrado de la función θ de la siguiente forma:

$$\theta(\tau)^2 = 1 + 4\sum_{n=1}^{\infty} \frac{q^n}{1+q^{2n}} = 1 + 4\sum_{k=1}^{\infty} \left(d_1\left(k\right) - d_3\left(k\right)\right) q^k. \tag{3.5}$$

De las expresiones del cuadrado de la función θ, (3.2) y (3.5), se ve que la expresión (3.3) es equivalente a que $r_2(n) = 4(d_1(n) - d_3(n))$, $n \geq 1$. De esta forma, la proposición queda probada. $\square$

Ahora se emplea $C(\tau)$ para denotar la función a la que se ha igualado θ^2:

$$C(\tau) = 2\sum_{n=-\infty}^{\infty} \frac{1}{q^n + q^{-n}} = \sum_{n=-\infty}^{\infty} \frac{1}{\cos(n\pi\tau)}, \ \textit{con } q = e^{\pi i \tau}, \tau \in \mathbb{H}. \tag{3.6}$$

El objetivo ahora es probar que se verifica la identidad $\theta(\tau)^2 = C(\tau)$, ya que esto equivale a probar el teorema de los dos cuadrados. Para ello, primero hay que comprobar que ambas cumplen las mismas propiedades estructurales. La siguiente proposición recoge las cuatro propiedades que se prueban a continuación.

Proposición 3.3. *La función $C(\tau) = \sum_{n=-\infty}^{\infty} \frac{1}{\cos(n\pi\tau)}$, con $\tau \in \mathbb{H}$ cumple:*

1. $C(\tau+2) = C(\tau)$.
2. $C(\tau) = \frac{i}{\tau}\, C(-1/\tau)$.
3. $C(\tau) \longrightarrow 1$ *cuando* $\Im(\tau) \longrightarrow \infty$.
4. $C(1-1/\tau) \sim\ 4\left(\frac{\tau}{i}\right)\ e^{\pi i \tau/2}$ *cuando* $\Im(\tau) \longrightarrow \infty$.

Además, $\theta(\tau)^2$ cumple las mismas propiedades.

Demostración. La periodicidad de θ^2 es sencilla de ver a partir de la propia definición de la función.

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

De esta forma, la periodicidad queda probada para θ^2. Falta ver que también se cumple para C.

$$C(\tau+2) = \sum_{n=-\infty}^{\infty} \frac{1}{\cos\left[n\pi(\tau+2)\right]} = \sum_{n=-\infty}^{\infty} \frac{1}{\cos(n\pi\tau + 2n\pi)} = \sum_{n=-\infty}^{\infty} \frac{1}{\cos(n\pi\tau)} = C(\tau)$$

Así, la periodicidad de ambas funciones queda probada.

Respecto a la segunda propiedad de la proposición, se vio en el Corolario 2.7 que para θ^2 se verifica la ley de transformación $\theta(-1/\tau)^2 = \frac{\tau}{i}\theta(\tau)$. Para demostrar que esta misma propiedad se cumple para C, se tiene en cuenta que la transformada de Fourier de la función $1/\cosh(\pi x)$ es su propia transformada de Fourier (Proposición 1.12).

$$\int_{-\infty}^{\infty} \frac{e^{-2\pi i x\xi}}{\cosh(\pi x)}\, dx = \frac{1}{\cosh(\pi\xi)}.$$

Esto implica que,

si $t > 0$ y $a \in \mathbb{R}$, entonces por el Corolario 1.13, la transformada de Fourier de la función $f(x) = \frac{e^{-2\pi ian}}{\cosh(\pi n/t)}$ es $\hat{f}(\xi) = \frac{t}{\cosh(\pi(\xi+a)t)}$ y la fórmula de las sumas de Poisson da la expresión (1.2):

$$\sum_{n=-\infty}^{\infty} \frac{e^{-2\pi ian}}{\cosh(\pi n/t)} = \sum_{n=-\infty}^{\infty} \frac{t}{\cosh[\pi(n+a)t]}$$

Tomando en esta expresión $a = 0$ se tiene la siguiente relación:

$$\frac{1}{t} \sum_{n=-\infty}^{\infty} \frac{1}{\cosh(\pi n/t)} = \sum_{n=-\infty}^{\infty} \frac{1}{\cosh(\pi nt)}.$$

Para $\tau = it$, $t > 0$, esta identidad se corresponde con la siguiente expresión:

$$\frac{i}{\tau}\, C(-1/\tau) = C(\tau).$$

Esta identidad se verifica para todo $\tau \in \mathbb{H}$ sin más que considerar una función con la misma expresión, pero definida para todo $\tau \in \mathbb{H}$. Esta función se expresa como una serie de potencias convergente, como ya se estableció en la Proposición 3.2, y, por lo tanto, es analítica en $\mathbb{H}$. Así, por continuidad analítica, la identidad (3.7) se cumple para todo $\tau \in \mathbb{H}$.

La tercera propiedad estructural que se comprueba que es igual para θ^2 y para C es el comportamiento para valores muy grandes de la parte imaginaria de τ. De la expresión (3.2) se ve que si $\Im(\tau) \longrightarrow \infty$, entonces todos los términos del sumatorio tienden a cero a excepción del término correspondiente a $n = 0$. De esta forma, $\theta(\tau)^2$ tiende a 1, que es el valor de su término para $n = 0$.

De la expresión (3.6) se ve que al tomar el límite $\Im(\tau) \longrightarrow \infty$, todos los términos vuelven a tender a 0 a excepción del término para $n = 0$. Así, $C(\tau)$ tiende a 1.

Ambas funciones muestran el mismo comportamiento en el límite $\Im(\tau) \longrightarrow \infty$. Ahora solo falta comprobar la tendencia de ambas funciones en $\tau = 1$. La importancia de este punto de $\mathbb{H}$ reside en que, posteriormente, se va a emplear una función restringida a un subconjunto $\mathcal{F} = \{\tau \in \overline{\mathbb{H}} : |\Re(\tau)| \leq 1 \ y \ \ |\tau| \geq 1\}$, para el que $\tau = -1$ y $\tau = 1$ son cúspides.

Para θ^2 se tiene en cuenta el Corolario 2.8 para ver que:

$$\theta(1 - 1/\tau)^2 \sim \ 4\left(\frac{\tau}{i}\right)\, e^{\pi i\tau/2}, \text{ cuando } \Im(\tau) \longrightarrow \infty.$$

Para comprobar que la función C tiene el mismo comportamiento que θ^2, se usa la expresión obtenida de la fórmula de las sumas de Poisson de nuevo, (1.2). Tomando en esta el valor $a = \frac{1}{2}$, se obtiene lo siguiente:

$$\sum_{n=-\infty}^{\infty} \frac{(-1)^n}{\cosh(\pi n/t)} = \sum_{n=-\infty}^{\infty} \frac{t}{\cosh(\pi(n+1/2)t)}$$

Para $\tau = it$, $t > 0$, se tiene que $\cosh(\pi n/t) = \cosh\left(\frac{i\pi n}{\tau}\right)$.

Se tiene en cuenta que $\cosh(it) = \cos(t)$, por lo que $\cosh\left(\frac{i\pi n}{\tau}\right) = \cos\left(\frac{\pi n}{\tau}\right)$. De esta forma, se cumple lo siguiente:

$$\sum_{n=-\infty}^{\infty} \frac{(-1)^n}{\cosh(\pi n/t)} = \sum_{n=-\infty}^{\infty} \frac{(-1)^n}{\cos(\pi n/\tau)} = \frac{\tau}{i} \sum_{n=-\infty}^{\infty} \frac{1}{\cos(\pi(n+1/2)\tau)} .$$

Por otro lado, se tiene que:

$$C(1-1/\tau) = \sum_{n=-\infty}^{\infty} \frac{1}{\cos\left(\pi n \left(1 - \frac{1}{\tau}\right)\right)} .$$

Teniendo en consideración la expresión del coseno de la resta de ángulos se tiene:

$$\begin{aligned} \cos\left(n\pi - \frac{n\pi}{\tau}\right) &= \cos(n\pi) \cdot \cos\left(\frac{n\pi}{\tau}\right) + \operatorname{sen}(n\pi) \cdot \operatorname{sen}\left(\frac{n\pi}{\tau}\right) \\ &= \cos(n\pi) \cdot \cos\left(\frac{n\pi}{\tau}\right) = (-1)^n \cdot \cos\left(\frac{n\pi}{\tau}\right). \end{aligned}$$

De esto, se tiene la siguiente igualdad:

$$C(1-1/\tau) = \sum_{n=-\infty}^{\infty} \frac{(-1)^n}{\cos\left(\frac{\pi n}{\tau}\right)} = \frac{\tau}{i} \sum_{n=-\infty}^{\infty} \frac{1}{\cos\left(\pi\left(n+\frac{1}{2}\right)\tau\right)}.$$

Los principales términos de este último sumatorio son los correspondientes a $n = -1$ y $n = 0$. Como el coseno es una función par, estos términos son el mismo, y al considerar su límite cuando $\Im(\tau) \longrightarrow \infty$, el módulo de estos términos será mayor que el de $\frac{1}{\cos\left(\frac{3\pi\tau}{2}\right)}$ o el de cualquiera de los términos para otros n. Considerando que $\tau = \sigma + it$ y la expresión exponencial del coseno para los mayores términos, se tiene que cuando $t \longrightarrow \infty$:

$$C(1-1/\tau) = 4\left(\frac{\tau}{i}\right) e^{\pi i \tau/2} + O\left(|\tau|\, e^{-3\pi t/2}\right).$$

El comportamiento de la función C es el mismo que el de la función θ^2. $\square$

Esta proposición prueba que θ^2 y C tienen las mismas propiedades estructurales. Ahora solo faltaría ver que $\theta(\tau)^2 = C(\tau)$, esto es, que el valor de ambas funciones en cada punto de $\mathbb{H}$ es el mismo. Para esto, se considera la función $f = \frac{C}{\theta^2}$.

Teorema 3.4. *Se considera que f es una función holomorfa en el semiplano superior que verifica:*

1. $f(\tau + 2) = f(\tau)$,
2. $f(-1/\tau) = f(\tau)$,
3. $f(\tau)$ *está acotada.*

Entonces, f es constante.

Se considera el semiplano superior cerrado, $\overline{\mathbb{H}} = \{z \in \mathbb{C} : \Im(z) \geq 0\}$. Para la demostración de este teorema se introduce el subconjunto de $\overline{\mathbb{H}}$ definido de la siguiente forma:

$$\mathcal{F} = \{\tau \in \overline{\mathbb{H}} : \ |\Re(\tau)| \leq 1 \ y \ \ |\tau| \geq 1\}. \tag{3.7}$$

Los puntos correspondientes a $\tau = -1$ y a $\tau = 1$ son cúspides y son equivalentes bajo la aplicación $\tau \ \mapsto \ \tau + 2$.

Antes de proceder con la demostración del Teorema 3.4, se presenta un lema

Lema 3.5. *Cada punto del semiplano superior puede conectarse por medio de una aplicación con $\mathcal{F}$ usando repetidamente las siguientes transformaciones lineales fraccionarias o sus inversas:*

$$T_2 : \ \tau \ \mapsto \ \tau + 2, \quad S : \mapsto \ \tau \mapsto \ -1/\tau.$$

Demostración. Sea G el grupo generado por T_2 y S. Como T_2 y S son transformaciones lineales fraccionarias, es posible representar un elemento $g \in G$ por la matriz:

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

teniéndose que

$$g(\tau) = \frac{a\tau + b}{c\tau + d}.$$

Como las matrices representando a T_2 y S tienen coeficientes enteros y sus determinantes son la unidad, estas mismas características se extienden para todas las matrices de elementos en G. En particular, si $\tau \in \mathbb{H}$, entonces

$$\Im(g(\tau)) \ = \frac{\Im(\tau)}{|c\tau + d|^2}. \tag{3.8}$$

Sea $\tau \in \mathbb{H}$. Si $g \in G$ con $g(\tau) = \frac{a\tau+b}{c\tau+d}$, entonces c y d son enteros por ser G el grupo generado por T_2 y S. Esto permite definir una acción de G en el semiplano superior. Teniendo en cuenta la expresión (3.8), es posible escoger una acción $g_0 \in G$ tal que $\Im(g_0(\tau))$ es maximal, esto es, tal que no sea posible escoger ninguna otra acción $g \in G$ con una parte imaginaria estrictamente superior a la de g_0. Como las traslaciones T_2 y sus inversas no cambian las partes imaginarias, es posible aplicar una cantidad finita de estas para ver que existe un $g_1 \in G$ verificando que $|\Re(g_1(\tau))| \leq 1$, donde $\Re(b)$ denota la parte real de b, y que $\Im(g_1(\tau))$ sea maximal. Entonces, basta con probar que $|g_1(\tau)| \geq 1$ para concluir que $g_1(\tau) \in \mathcal{F}$.

Si se supone que esto no se cumple, se tiene que $|g_1(\tau)| < 1$. A partir de esta condición, se busca probar por reducción al absurdo que $g_1(\tau) \in \mathcal{F}$. Entonces, se toma la parte imaginaria de la acción g_1 bajo la transformación S:

$$\Im\left(Sg_1\left(\tau\right)\right) = \Im\left(-1/g_1\left(\tau\right)\right) = -\frac{\Im\left(\overline{g_1\left(\tau\right)}\right)}{\left|g_1\left(\tau\right)\right|^2} > \Im\left(g_1\left(\tau\right)\right).$$

De esta forma, se tiene $\Im\left(Sg_1\left(\tau\right)\right)$ es mayor que $\Im\left(g_1\left(\tau\right)\right)$, y esto supone una contradicción, pues se había elegido la acción g_1 de tal forma que su parte imaginaria fuese maximal. No se cumple la maximalidad de $\Im\left(g_1\left(\tau\right)\right)$, por lo que queda demostrado por reducción al absurdo que $|g_1(\tau)| \geq 1$ y, así, que $g_1(\tau) \in \mathcal{F}$. El lema ha sido demostrado. □

Ahora, tras enunciar y demostrar este lema, se procede con la demostración del Teorema 3.4, para la que se hace uso de dicho lema.

Demostración. (Teorema 3.4) Sea f una función no constante y sea $g(z) = f(\tau)$, donde $z = e^{\pi i \tau}$. Como por la primera hipótesis del teorema se tiene que f es periódica de periodo 2, la función g estará bien definida en z en el disco unidad perforado, pues su diámetro es precisamente de dos unidades. Además, como por la tercera hipótesis, $f(\tau)$ está acotada, g estará acotada en un entorno del origen. De esta forma, 0 es una singularidad evitable de g y, por la Proposición 1.14 se tiene que $\lim_{z\longrightarrow 0} g(z) = \lim_{\Im(\tau)\longrightarrow\infty} f(\tau)$ existe. Por el principio del módulo máximo se tiene que:

$$\lim_{\Im(\tau)\longrightarrow\infty} |f(\tau)| < \sup_{\tau\in\mathcal{F}} |f(\tau)|.$$

Ahora, se estudia el comportamiento de f en las cúspides, esto es, en los puntos $\tau = \pm 1$. Como se tiene que $f\left(\tau+2\right) = f\left(\tau\right)$, basta con estudiar el comportamiento de f en el punto $\tau = 1$, pues en $\tau = -1$ la función se comportará de la misma forma. Si se asume la existencia de $\lim_{\Im(\tau)\longrightarrow\infty} f(1-1/\tau)$, por el principio del módulo máximo se tiene que:

$$\lim_{\Im(\tau)\longrightarrow\infty} |f(1-1/\tau)| < \sup_{\tau\in\mathcal{F}} |f(\tau)|. \tag{3.9}$$

Para estudiar el comportamiento de f en $\tau = 1$ se estudia el comportamiento de $F(\tau) = f(1 - 1/\tau)$ en el límite en el que $\Im(\tau) \longrightarrow \infty$. Para ello, primero hay que ver que F es periódica. Para ello, se considera la transformación lineal fraccionaria asociada a la matriz:

$$U_n = \begin{pmatrix} 1-n & n \\ -n & 1+n \end{pmatrix}.$$

Equivalentemente, se está considerando la aplicación:

$$\tau \longmapsto \frac{(1-n)\,\tau + n}{-n\tau + (1+n)},$$

que lleva 1 a 1. Ahora, sea $\mu(\tau) = 1/(1-\tau)$ una función que lleva 1 a ∞ y cuya inversa es $\mu(\tau)^{-1} = 1 - 1/\tau$, que lleva ∞ a 1.

Así, teniendo en cuenta que T_n es la traslación $T_n = \tau + n$, se ve que U_n es la traslación asociada a la función μ:

$$U_n = \mu^{-1} T_n \mu.$$

Está claro que de esta forma se tendrá que $U_n U_m = U_{n+m}$:

$$U_n U_m = \mu^{-1} T_n \mu \cdot \mu^{-1} T_m \mu = \mu^{-1} T_n T_m \mu = U_{n+m}.$$

Además, se tendrá que:

$$U_{-1} = \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix} = T_2 S.$$

De esta forma, cualquier U_n se podrá obtener en un número finito de aplicaciones de T_2, de S o de sus inversas. Se toma un U_n inicial arbitrario y se aplica U_{-1} o su inversa las veces que haga falta para alcanzar el valor de $n + m$ deseado. Esto es posible gracias al Lema 3.5, por el que cada punto de $\mathbb{H}$ se puede conectar con $\mathcal{F}$ por medio del uso repetido de las transformaciones lineales T_2 y S. Además, como f es invariante bajo T_2 y S, también es invariante bajo U_m. Así, se tiene que:

$$f\left(\mu^{-1} T_n \mu(\tau)\right) = f\left(\tau\right).$$

Entonces, considerando que $F(\tau) = f\left(\mu^{-1}(\tau)\right) = f(1 - 1/\tau)$, se tiene que para todo entero n:

$$F(\tau) = f\left(\mu^{-1}(\tau)\right) = f\left(\mu^{-1} T_n \mu \cdot \mu^{-1}(\tau)\right) = f\left(\mu^{-1} T_n \tau\right) = F(T_n \tau).$$

Esto es equivalente a que la función F sea periódica de periodo 1, que es lo que se quería probar. De esta forma, tomando $h(z) = F(\tau)$, con $z = e^{2\pi i\tau}$, se tiene que h tiene una singularidad evitable en $z = 0$. Entonces, por la Proposición 1.14 se tiene que la existencia de esta singularidad evitable es equivalente a que $\lim_{z\longrightarrow 0} h(z) = \lim_{\Im(\tau)\longrightarrow\infty} F(\tau)$ y, así, la relación (3.9) se cumple.

De lo anterior, se concluye que f no alcanza su máximo en los puntos $\tau = \pm 1$, que son los únicos dos puntos de $\mathcal{F}$ que no pertenecen al semiplano superior. Así, f ha de alcanzar su máximo en el interior de $\mathbb{H}$. Sin embargo, esto supone una contradicción al principio del máximo, por lo que se ha llegado a un absurdo. Así, el teorema queda probado por reducción al absurdo tras suponer que f no era constante. □

Ya se tienen todos los resultados necesarios para probar que $\theta(\tau)^2 = C(\tau)$. Demostrando esto, se tendría que la identidad (3.3) se cumple y, enotonces, como la Proposición 3.2 establece que esta identidad es equivalente al enunciado del teorema de los dos cuadrados, este quedaría demostrado.

Se considera la función $f(\tau) = \frac{C(\tau)}{\theta(\tau)^2}$. Se sabe por el Corolario 2.4 que la función $\theta(\tau)$ no se anula en el semiplano superior, por lo que f es holomorfa al existir en todo punto de $\mathbb{H}$ y ser el cociente de dos funciones holomorfas en $\mathbb{H}$.

Por la Proposición 3.3 se tiene que tanto C como θ^2 cumplen que $C(\tau+2) = C(\tau)$ y que $C(\tau) = \frac{i}{\tau}\, C(-1/\tau)$, por lo que se va a tener que $f(\tau+2) = f(\tau)$ y que $f(\tau) = f(-1/\tau)$. Esto es, f es invariante bajo las transformaciones T_2 y S.

Finalmente, la función f cumple que $f(\tau) \longrightarrow 1$ cuando $\Im(\tau) \longrightarrow \infty$, puesto que sus dos elementos cumplen esta propiedad de acuerdo con la Proposición 3.3.

La Proposición 3.3 también afirma que tanto C como θ^2 cumplen que $C(1-1/\tau) \sim\ 4\left(\frac{\tau}{i}\right)\ e^{\pi i\tau/2}$ cuando $\Im(\tau) \longrightarrow \infty$. Así, la función f tiende a 1 cuando τ tiende a las cúspides.

De esta forma, f no solo está acotada en $\mathcal{F}$, sino que también lo está en $\mathbb{H}$.

Ahora, por el Teorema 3.4 se tiene que f es constante y, a la vista de los límites considerados antes, esta debe ser igual a la unidad. De esta forma, queda probado que $\theta(\tau)^2 = C(\tau)$, que era lo necesario para demostrar el teorema de los dos cuadrados.

Entonces, se tiene el siguiente enunciado para determinar el número de formas en las que un número entero positivo n se puede expresar como la suma de dos cuadrados: si $n \geq 1$, entonces $r_2(n) = 4(d_1(n) - d_3(n))$.

Esta fórmula se puede interpretar como que, si $n = p_1^{a_1} \cdots p_r^{a_r}$ es la factorización en primos de n en la que $p_1, ..., p_r$ son distintos, entonces el entero positivo n puede ser representado como la suma de dos cuadrados si, y solo si, todo primo p_j de la forma $4k+3$ que aparece en la factorización de n tiene un exponente a_j par.

Si $n = p$, donde p es un primo de la forma $4k + 1$, se tiene que $r_2(n) = 4(2 - 0) = 8$. Esto implica que un n de la forma $4k + 1$ se podría escribir de una única forma como $n = n_1^2 + n_2^2$, excepto por los signos y cambios de orden de n_1 y de n_2.

Si $n = q^a$, donde q es un primo de la forma $4k + 3$ y a es un entero positivo, se tiene que:

$$r_2(q^a) = 4\left[\left(\left\lfloor \frac{a}{2} \right\rfloor + 1\right) - \left(\left\lfloor \frac{a-1}{2} \right\rfloor + 1\right)\right],$$

donde $\lfloor b \rfloor$ representa el mayor entero menor o igual que b. Si a es impar, se tiene que $\left\lfloor \frac{a}{2} \right\rfloor = \left\lfloor \frac{a-1}{2} \right\rfloor$ y, por lo tanto, $r_2(q^a) = 0$. De esta forma se tiene que $r_2(n) > 0$ si, y solo si, a es par.

Como el producto de dos números que se pueden escribir como sumas de cuadrados se puede escribir como suma de cuadrados, de los dos resultados anteriores se deduce el resultado.

3.1. Comportamiento asintótico

Para complementar el estudio del teorema de los dos cuadrados, se destaca que hay ciertas irregularidades en el comportamiento de las funciones $r_2(n)$ para valores de n muy grandes.

Primero se estudia el comportamiento asintótico de $r_2(n)$. En este caso, se cumple que $r_2(n) = 0$ para una cantidad infinita de valores de n, mientras que, por otro lado, se cumple que $\limsup_{n \longrightarrow \infty} r_2(n) = \infty$.

Como ya se dijo con anterioridad, ningún entero de la forma $4k + 3$ puede ser escrito como la suma de dos cuadrados. Teniendo en cuenta que $r_2(n)$ es el número de formas en las que un entero positivo se puede escribir como la suma de dos cuadrados, está claro que para todo entero positivo de la forma $4k + 3$ se va a cumplir que $r_2(n) = 0$. Así, hay infinitos valores de n para los que $r_2(n) = 0$.

Se consideran los enteros positivos de la forma $n = 5^k$. Los divisores de cualquier posible valor de n van a ser potencias de 5 y, a su vez, cualquier potencia de 5 es de la forma $4k + 1$. Entonces, siempre se va a tener que $d_1(n) = k+1$ y que $d_3(n) = 0$ y, en estas condiciones, $r_2(n) = 4(d_1(n) - d_3(n)) = 4\,(k + 1 - 0) = 4(k + 1)$. Así, al considerar los enteros positivos de la forma $n = 5^k$, $\lim_{k \longrightarrow \infty} r_2(5^k) = \lim_{k \longrightarrow \infty} 4k = \infty$. De esta forma, se tiene que $\limsup_{n \longrightarrow \infty} r_2(n) = \infty$.

Capítulo 4

El teorema de los tres cuadrados

Después de ver que no todos los enteros se pueden expresar como la suma de dos cuadrados y de hallar cuáles sí pueden, es lógico plantear antes la cuestión de cuáles se pueden expresar como la suma de tres cuadrados o si todo entero positivo se puede expresar como la suma de tres cuadrados. La respuesta a esto la da el Teorema de los tres cuadrados, planteado por Legendre en 1797 y generalizado por Gauss en 1801. El enunciado que todo entero positivo puede expresarse como la suma de tres cuadrados si, y solo si, dicho entero no es de la forma $4^r(8m+7)$, con $r, m \geq 0$.

Por ejemplo, todos los números que son 7 en módulo 8 no son suma de tres cuadrados, como se puede ver con el 7, el 15 o el 23; pero estos no son los únicos, ya que, por ejemplo, el $4 \cdot 7 = 28$ tampoco lo es. Si, por el contrario, se consideran todos los enteros entre el 16 y el 22, estos se pueden expresar como la suma de tres cuadrados: $16 = 4^2 + 0^2 + 0^2$, $17 = 3^2 + 2^2 + 2^2$, $18 = 4^2 + 1^2 + 1^2$, $19 = 3^2 + 3^2 + 1^2$, $20 = 4^2 + 2^2 + 0^2$, $21 = 4^2 + 2^2 + 1^2$ y $22 = 3^2 + 3^2 + 2^2$. Esto se debe a que ninguno de los enteros entre 15 y 23 se puede expresar como una potencia de 4 por un entrero que sea 7 en módulo 8. Además del ya mencionado 28, los enteros más pequeños que no son 7 en módulo 8 y no se pueden escribir como la suma de tres cuadrados son $4 \cdot 15 = 60$, $4 \cdot 23 = 92$, $4^2 \cdot 7 = 112$ y $4 \cdot 31 = 124$.

La demostración del teorema de los tres cuadrados no se trata desde el punto de vista de la teoría de formas modulares debido a la dificultad que supone su planteamiento. Es mucho más complejo tratar con potencias impares de la función theta de Jacobi que con las potencias pares que se usaron para la demostración del teorema de los dos cuadrados y se usarán para la del teorema de los cuatro y los ocho cuadrados. Adicionalmente, en el teorema de los dos cuadrados se emplea una función de peso $2/2 = 1$. En el teorema de los cuatro cuadrados se utiliza la serie de Eisenstein de peso $4/2 = 2$ y en el teorema de los ocho cuadrados la de peso $8/2 = 4$. Sin embargo, en el caso de los tres cuadrados, la función sería de peso $3/2$. Las formas modulares de peso semientero son más complicadas que las de peso entero y por ello se evita utilizarlas.

Se presenta ahora el teorema de los tres cuadrados, así como su demostración. En ella, se ha omitido un cálculo técnico y que es el que permite concluir, aunque se detalla la estructura del resto de la demostración.

Teorema 4.1. *Todo entero positivo puede expresarse como la suma de tres cuadrados si, y solo si, dicho entero no es de la forma:*

$$4^r(8m+7), \qquad \text{con } r, m \geq 0.$$

Demostración. Lo primero que se prueba es que si todo entero positivo se puede expresar como la suma de tres cuadrados, entonces dicho entero no es de la forma $4^r(8m+7)$. Esto es equivalente a probar que si $n = 4^r(8m+7)$, entonces n no puede ser expresado como la suma de tres cuadrados.

Se comprueban los valores que pueden tener los cuadrados perfectos de todo entero positivo en módulo 8. A continuación se representa cada uno de manera individual:

$$\begin{aligned} 0^2 &\equiv 0 \pmod 8, & 1^2 &\equiv 1 \pmod 8, \\ 2^2 &\equiv 4 \pmod 8, & 3^2 &\equiv 1 \pmod 8, \\ 4^2 &\equiv 0 \pmod 8, & 5^2 &\equiv 1 \pmod 8, \\ 6^2 &\equiv 4 \pmod 8, & 7^2 &\equiv 1 \pmod 8. \end{aligned}$$

Esto evidencia que los cuadrados en módulo 8 son 0, 1 ó 4. De esta forma, se consideran las posibles combinaciones de estos tres valores para ver los enteros que se pueden representar como la suma de tres cuadrados en módulo 8.

$$\begin{aligned} 0+0+0 &\equiv 0 \pmod 8, \\ 0+4+4 &\equiv 0 \pmod 8, \\ 0+0+1 &\equiv 1 \pmod 8, \\ 1+4+4 &\equiv 1 \pmod 8, \\ 0+1+1 &\equiv 2 \pmod 8, \\ 1+1+1 &\equiv 3 \pmod 8, \\ 0+0+4 &\equiv 4 \pmod 8, \\ 4+4+4 &\equiv 4 \pmod 8, \\ 0+1+4 &\equiv 5 \pmod 8, \\ 1+1+4 &\equiv 6 \pmod 8. \end{aligned}$$

De esta forma, queda en evidencia que ningún entero que sea 7 en módulo 8 se puede expresar como la suma de tres cuadrados.

Se tiene el comportamiento para ciertos valores, que se denotan por k. Entonces, se supone que $n = 4k$. El objetivo es probar que n es la suma de tres cuadrados si, y solamente si, k es la suma de tres cuadrados

Si se supone que k puede ser escrito como la suma de tres cuadrados, $k = x^2 + y^2 + z^2$. A partir de esto, n se puede expresar como $n = (2x)^2 + (2y)^2 + (2z)^2$, que es la suma de tres cuadrados. Sin embargo, por hipótesis se tiene que $k = 8m + 7$. De esta forma, $k \equiv 7$ y, de acuerdo con lo mostrado previamente, k no se puede expresar como la suma de tres cuadrados. Esto prueba la primera implicación del teorema.

Por otro lado, se pretende demostrar que si n es la suma de tres cuadrados, k es la suma de tres cuadrados. Se supone que k no se puede escribir como la suma de tres cuadrados y se tiene que $n = 4k = x^2 + y^2 + z^2$. Como n es par, no puede pasar que entre x,y y z, solo uno o los tres sean impares, puesto que su suma resulta en un valor impar. En el caso en el que dos de los cuadrados sean impares, la suma sería 2 en módulo 4, por lo que son todos pares. De esta forma, se definen $x = 2a$, $y = 2b$ y $z = 2c$. Entonces, $4k = 4a^2 + 4b^2 + 4c^2$ y, como consecuencia, $k = a^2 + b^2 + c^2$. Sin emabargo, se había supuesto que k no era la suma de tres cuadrados, por lo que se da una contradicción. Se concluye por reducción al absurdo que si n es la suma de tres cuadrados, entonces k es la suma de tres cuadrados.

Esto concluye la prueba de que n es la suma de tres cuadrados si, y solo si, k es la suma de tres cuadrados.

Ahora, el objetivo es probar que todos los enteros positivos que no son de la forma $n = 4^r(8m+7)$ se pueden escribir como la suma de tres cuadrados. Como ya se comentó, la demostración tiene cálculos complejos y por este motivo solo se proporciona una idea de cómo se plantea la prueba.

El objetivo es construir una forma cuadrática definida positiva con determinante unidad que sirva para representar un entero n de la forma $n = 4^r(8m + 7)$. Si esto se cumple, la forma cuadrática equivale a la representación de n como la suma de tres cuadrados.

La notación que se emplea es la recogida en la Definición 1.17 y en el Teorema 1.18, esto es:

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{21} & a_{31} \\ a_{12} & a_{22} & a_{32} \\ a_{13} & a_{23} & a_{33} \end{pmatrix}, \quad b = \begin{vmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{vmatrix}.$$

La construcción de una forma cuadrática ternaria definida positiva, de acuerdo con el Teorema 1.18, se centra en encontrar un $b > 0$ tal que $-b$ sea un cuadrado perfecto en módulo $bn-1$. Una vez se tiene este b, se escoge un a_{12} que verifique que $-b$ sea congruente con a_{12}^2 en módulo $bn-1$. Adicionalmente, se determinan los siguientes valores para los coeficientes de la representación matricial de una forma cuadrática:

$$\begin{aligned} a_{22} &= bn - 1, \\ a_{11} &= \frac{b + a_{12}^2}{a_{22}}, \\ a_{13} &= 1, \\ a_{23} &= 0, \\ a_{33} &= n. \end{aligned}$$

Además, por la Definición 1.17, se tiene que $a_{12} = a_{21}$, $a_{13} = a_{31}$ y $a_{23} = a_{32}$. De esta forma, todos los elementos de la representación matricial quedan determinados para un cierto b.

Con todos los coeficientes determinados, se establece que $f(x_1, x_2, x_3) = \sum_{i,j=1}^{3} a_{ij} x_i x_j$. De esta forma, se tiene una forma cuadrática ternaria definida positiva, f, verificando que su determinante es 1 y que $f(0, 0, 1) = n$

La cuestión de la elección de b cumpliendo que $-b$ sea un cuadrado perfecto en módulo $bn - 1$ es más compleja. Un procedimiento por el que se podría determinar incluye el uso de los símbolos de Jacobi. Estos consisten en una generalización de los símbolos de Legendre. Si se considera un entero impar $b = \prod_{r=1}^{k} p_r$ y una constante a entera, se define un símbolo de Jacobi $\left(\frac{a}{b}\right)$ como

$$\left(\frac{a}{b}\right) = \prod_{r=1}^{k} \left(\frac{a}{p_r}\right),$$

donde $\left(\frac{a}{p_r}\right)$ denota el símbolo de Legendre habitual.

Otro resultado a tener en cuenta es el Teorema de Dirichlet para números primos en progresiones aritméticas. Este dice que si a y d son enteros positivos coprimos, entonces hay una cantidad infinita de números primos congruentes con a en módulo d.

De esta forma, a partir de los símbolos de Jacobi y el teorema de Dirichlet para números primos en progresiones aritméticas se puede desarrollar un cálculo complejo con el que se encuentra un valor de b que cumple que $-b$ es un cuadrado perfecto de módulo $bn - 1$. A partir de este b se define una forma cuadrática ternaria definida positiva y de determinante 1. En estas condiciones, aplicando el Teorema 1.19 se tiene que dicha forma cuadrática ternaria es equivalente a la suma de tres cuadrados, por lo que el teorema queda probado. $\square$

Capítulo 5

El teorema de los cuatro cuadrados

En este capítulo se prueba el teorema de los cuatro cuadrados, esto es, se demuestra que todo entero positivo se puede expresar como la suma de cuatro cuadrados y se encuentra una expresión para $r_4(n)$, que da el número de formas en las que se puede expresar el número como suma de cuatro cuadrados.

El teorema de los cuatro cuadrados fue propuesto por primera vez por el matemático griego Diofanto de Alejandría, el mismo al que se atribuyen los primeros escritos conservados que hacen referencia al teorema de los dos cuadrados. Sin embargo, este solo era conocedor del resultado y no proporcionó una prueba. Este resultado está recogido en *Arithmetica*, que era un tratado de 13 libros de los que solo se conservan los seis primeros. La primera demostración no llegaría hasta el siglo XVII, de la mano del matemático Pierre de Fermat. Sin embargo, este no llegó a publicar su demostración y no sería hasta 1770 que se publicaría por primera vez la prueba de este teorema. La demostración la conseguiría hacer Joseph-Louis Lagrange y por ello a este teorema también se lo conoce como el teorema de los cuatro cuadrados de Lagrange. Sin embargo, la prueba que se da en este capítulo es la proporcionada por Carl Gustav Jakob Jacobi en 1834, que añadía la expresión del número de formas en las que un entero positivo podía ser expresado como la suma de cuatro cuadrados.

Para enunciar el teorema se denota por $\sigma_1^*(n)$ al número de divisores de n que no son divisibles por cuatro. Así, el teorema de los cuatro cuadrados es el siguiente:

Teorema 5.1. ***(de los cuatro cuadrados)*** *Cada entero positivo es la suma de cuatro cuadrados y, además, para todo $n \geq 1$:*

$$r_4(n) = 8\sigma_1^*(n). \tag{5.1}$$

De manera análoga a como se hizo para el teorema de los dos cuadrados, se establece una relación que identifica la función generatriz de la sucesión $\{r_4(n)\}_{n=1}^{\infty}$ con la cuarta potencia de la función θ.

$$\theta(\tau)^4 = \sum_{n=0}^{\infty} r_4(n)\ q^n, \qquad \text{con } q = e^{\pi i \tau}, \tau \in \mathbb{H}.$$

Teniendo esto en cuenta, se busca encontrar la función modular cuya igualdad con $\theta(\tau)^4$ exprese la identidad $r_4(n) = 8\sigma_1^*(n)$. Sin embargo, este caso no es tan sencillo como el del teorema de los dos cuadrados y no sirve con simplemente definir una función como $C(\tau)$. Esta vez, es necesario construir una función que supone una ligera variación de las series de Eisenstein consideradas en la Definición 1.21. De esta forma, se define, para $\tau \in \mathbb{H}$:

$$E_2^*(\tau) = \sum_m \sum_n \frac{1}{\left(\frac{m\tau}{2} + n\right)^2} - \sum_m \sum_n \frac{1}{\left(m\tau + \frac{n}{2}\right)^2}. \tag{5.2}$$

Las series representadas no convergen absolutamente, por lo que es indispensable mantener el orden de suma, ya que la reordenación de los términos de la serie altera el valor de la suma.

Con la siguiente proposición se reduce el teorema de los cuatro cuadrados a las propiedades modulares de E_2^* al establecer una relación entre θ^4 y E_2^* que es equivalente al propio teorema de los cuatro cuadrados.

Proposición 5.2. *La igualdad $r_4(n) = 8\sigma_1^*(n)$ es equivalente a la identidad*

$$\theta(\tau)^4 = -\frac{1}{\pi^2}\ E_2^*\left(\tau\right), \ \textit{donde } \tau \in \mathbb{H}.$$

Demostración. Primero, se considera que $\theta(\tau)^4 = \sum_{n=0}^{\infty} r_4(n)\ q^n$. De esta forma, al sustituir en esta expresión que $r_4(n) = 8\sigma_1^*(n)$ y separar del sumatorio el término para $k = 0$, se llega que basta con probar que, si $q = e^{\pi i \tau}$, entonces

$$-\frac{1}{\pi^2}\ E_2^*\left(\tau\right) = 1 + \sum_{k=1}^{\infty} 8\sigma_1^*(k) q^k.$$

Ahora, se consideran las *series prohibidas* de Eisenstein que se establecieron en la Definición 1.22, omitiendo el término para el que $n = m = 0$:

$$F\left(\tau\right) = \sum_m \left(\sum_n \frac{1}{\left(m\tau + n\right)^2} \right). \tag{5.3}$$

Una vez más, la serie no es absolutamente convergente y, por ello, las sumas deben darse en n y, posterioremnte, en m, sin alterar en ningún caso este orden. Primero se hace el sumatorio en n y, posteriormente, en m. Teniendo esto en cuenta, es posible expresar (5.2) en términos de las *series prohibidas* de Eisenstein (5.3), que se definen de la siguiente manera:

$$E_2^*(\tau) = F\left(\frac{\tau}{2}\right) - 4F\left(2\tau\right). \tag{5.4}$$

Por el Corolario 1.24 se tiene que, siendo $\sigma_1(k)$ la suma de los divisores de k:

$$F(\tau) = \frac{\pi^2}{3} - 8\pi^2 \sum_{k=1}^{\infty} \sigma_1(k) e^{2\pi i \tau k}. \tag{5.5}$$

Ahora, se tiene en cuenta que se había denotado por $\sigma_1^*(n)$ al número de divisores de n que no son divisibles por cuatro. Si n no es divisible por 4, entonces ninguno de los divisores de n será divisible por 4. Si $n = 4\widetilde{n}$ y d es un divisor de n que es divisible por 4 que se denota como $d = 4\widetilde{d}$, entonces $\widetilde{d}$ divide a $\widetilde{n}$. Así, los divisores de $\widetilde{n}$ que son divisibles por 4 son $\sigma_1(\widetilde{n}) = \widetilde{d} = \frac{d}{4}$ y, de esta forma, los divisores de n que son divisibles por 4 son $d = 4\widetilde{d} = 4\sigma_1(\widetilde{n}) = 4\sigma_1\left(\frac{n}{4}\right)$. Teniendo esto en cuenta, se define $\sigma_1^*(n)$ como:

$$\sigma_1^*(n) = \begin{cases} \sigma_1(n) & \text{si } n \text{ no es divisible por 4.} \\ \sigma_1(n) - 4\sigma_1\left(\frac{n}{4}\right) & \text{si } n \text{ es divisible por 4.} \end{cases} \tag{5.6}$$

Combinando las expresiones (5.4) y (5.5) se tiene que

$$\begin{aligned} E_2^*(\tau) &= \frac{\pi^2}{3} - 8\pi^2 \sum_{k=1}^{\infty} \sigma_1(k) e^{\pi i \tau k} - \frac{4\pi^2}{3} + 32\pi^2 \sum_{k=1}^{\infty} \sigma_1(k) e^{4\pi i \tau k} \\ &= -\pi^2 - 8\pi^2 \sum_{k=1}^{\infty} \sigma_1(k) e^{\pi i \tau k} + 8\pi^2 \sum_{k=1}^{\infty} 4\sigma_1(k) e^{4\pi i \tau k}. \end{aligned}$$

Se tiene en cuenta esta expresión y (5.6). El caso en el que n es divisible por 4 se deduce fácilmente de la expresión (5.6). El caso en el que n no es divisible por 4 se obtiene debido a que $\sum_{k=1}^{\infty} 4\sigma_1(k) e^{4\pi i \tau k}$ se anula por la simetría de los términos del sumatorio en el plano complejo. Así, se llega a que

$$E_2^*(\tau) = -\pi^2 - 8\pi^2 \sum_{k=1}^{\infty} \sigma_1^*(k) e^{\pi i \tau k}.$$

De esta forma, la proposición queda probada. □

Así, el Teorema 5.1 se ha reducido a la identidad $\theta^4 = -\frac{1}{\pi^2} E_2^*$. Para probar esto hay que demostrar que E_2^* satisface las mismas propiedades modulares que θ^4. Con este objetivo, se introduce un lema que posteriormente se empleará en la demostración de las propiedades modulares de E_2^*.

Antes de presentar el lema, se consideran las *series prohibidas* de Eisenstein, F, y las series que se obtienen invirtiendo el orden de las sumas de estas, $\widetilde{F}$, teniendo en cuenta que en ambos casos se omite el término que corresponde con $n = m = 0$:

$$F(\tau) = \sum_m \left(\sum_n \frac{1}{(m\tau + n)^2} \right) \quad \text{y} \quad \widetilde{F}(\tau) = \sum_n \left(\sum_m \frac{1}{(m\tau + n)^2} \right).$$

Lema 5.3. *Las funciones F y $\widetilde{F}$ satisfacen que:*

1. $F\left(-1/\tau\right) = \tau^2 \widetilde{F}\left(\tau\right)$,
2. $F\left(\tau\right) - \widetilde{F}\left(\tau\right) = \frac{2\pi i}{\tau}$,
3. $F\left(-1/\tau\right) = \tau^2 F\left(\tau\right) - 2\pi i\tau$.

Demostración. Para demostrar la primera igualdad, basta con considerar la siguiente identidad:

$$\left(n + m\left(-1/\tau\right)\right)^2 = \tau^{-2}\left(-m + n\tau\right)^2.$$

El término de la izquierda representa cada uno de los elementos de las series $F\left(-1/\tau\right)$, mientras que el término de la derecha representa cada uno de los elementos de las series $\tau^2\widetilde{F}\left(\tau\right)$. Así, la primera igualdad está probada.

Para probar la segunda igualdad se recurre a la función eta de Dedekind, que se define como:

$$\eta(\tau) = e^{\frac{\pi i\tau}{12}} \prod_{n=1}^{\infty} (1 - e^{2\pi i n\tau}).$$

Se considera el logaritmo neperiano de la función eta de Dedekind:

$$\ln\left(\eta(\tau)\right) = \frac{\pi i\tau}{12} + \sum_{n=1}^{\infty} \ln\left(1 - e^{2\pi i n\tau}\right).$$

Así, se calcula la derivada de η por derivación logarítmica y se obtiene que:

$$\frac{\eta'}{\eta}\left(\tau\right) = \frac{\pi i}{12} - \sum_{n=1}^{\infty} \frac{n e^{2\pi i n\tau}}{1 - e^{2\pi i n\tau}}.$$

Sin embargo, si $\sigma_1\left(k\right)$ denota la suma de los divisores de k y se considera que para una serie geométrica se tiene que $\sum_{l=0}^{\infty} e^{2\pi i n\tau l} = \frac{1}{1-e^{2\pi i n\tau}}$, entonces se cumple que:

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{n e^{2\pi i n\tau}}{1 - e^{2\pi i n\tau}} &= \sum_{n=1}^{\infty}\sum_{l=0}^{\infty} n e^{2\pi i n\tau} e^{2\pi i n\tau l} = \sum_{n=1}^{\infty}\sum_{l=0}^{\infty} n e^{2\pi i n\tau(l+1)} \\ &= \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} n e^{2\pi i n\tau m} = \sum_{k=1}^{\infty} \sigma_1\left(k\right) e^{2\pi i\tau k}.\end{aligned}$$

Así, la derivada de η se puede expresar de la siguiente forma:

$$\frac{\eta'}{\eta}\left(\tau\right) = \frac{\pi i}{12} - \sum_{k=1}^{\infty} \sigma_1\left(k\right) e^{2\pi i\tau k}.$$

Teniendo en cuenta la expresión (5.5), esto se puede escribir como

$$\frac{\eta'}{\eta}(\tau) = \frac{i}{4\pi} F(\tau). \tag{5.7}$$

Aplicando la regla de la cadena, es posible hallar de manera sencilla que la derivada logarítmica de $\eta(-1/\tau)$ es $\tau^{-2}\left(\frac{\eta'}{\eta}\right)(-1/\tau) = \tau^{-2}\frac{i}{4\pi}F(-1/\tau)$.

De la primera propiedad de este lema se obtiene que la derivada logarítmica de $\eta(-1/\tau)$ se puede expresar como

$$\frac{\eta'}{\eta}(\tau) = \frac{i}{4\pi}\widetilde{F}(\tau). \tag{5.8}$$

Ahora se considera el Corolario 2.9, por el que se tiene que

$$\eta(-1/\tau) = \sqrt{\frac{\tau}{i}}\,\eta(\tau).$$

Por derivación logarítmica de esta expresión se obtiene que

$$\frac{\eta'}{\eta}(-1/\tau) = \frac{1}{2\tau} + \frac{\eta'}{\eta}(\tau) \tag{5.9}$$

Teniendo en cuenta la expresión (5.7), esto es equivalente a:

$$\frac{\eta'}{\eta}(-1/\tau) = \frac{1}{2\tau} + \frac{i}{4\pi}F(\tau).$$

Combinando las expresiones (5.8) y (5.9) se tiene la siguiente relación:

$$\frac{i}{4\pi}\widetilde{F}(\tau) = \frac{1}{2\tau} + \frac{i}{4\pi}F(\tau).$$

Sin más que multiplicar a ambos lados de la expresión por $\frac{4\pi}{i}$ se tiene que

$$\widetilde{F}(\tau) = -\frac{2\pi i}{\tau} + F(\tau).$$

Esta se trata precisamente de la segunda igualdad que se quería probar, por lo que queda demostrada.

Para demostrar la última igualdad se consideran las dos igualdades anteriores del lema. De esta forma se tiene que

$$\widetilde{F}(\tau) = \tau^{-2}F(-1/\tau) = -\frac{2\pi i}{\tau} + F(\tau) \Leftrightarrow F(-1/\tau) = \tau^2 F(\tau) - 2\pi i\tau.$$

Esta es la tercera igualdad, por lo que queda probada. $\square$

Ahora, se presenta la proposición que establece que las propiedades modulares de $-\pi^2\theta^4$ y las de E_2^* son las mismas. El resultado es análogo al presentado para la función C y θ^2 en la demostración del teorema de los dos cuadrados.

Proposición 5.4. *La función $E_2^*(\tau)$ definida en el semiplano superior tiene las siguientes propiedades:*

1. $E_2^*(\tau+2) = E_2^*(\tau)$.
2. $E_2^*(\tau) = -\tau^{-2}E_2^*(-1/\tau)$.
3. $E_2^*(\tau) \longrightarrow -\pi^2$, *cuando* $\Im(\tau) \longrightarrow \infty$.
4. $|E_2^*(1-1/\tau)| = O\left(\left|\tau^2 e^{\pi i\tau}\right|\right)$, *cuando* $\Im(\tau) \longrightarrow \infty$.

Además, $-\pi^2\theta^4$ cumple las mismas propiedades.

Demostración. La primera propiedad se prueba de manera sencilla teniendo en cuenta el siguiente cálculo:

$$\begin{aligned}
E_2^*(\tau+2) &= -\pi^2 - 8\pi^2\sum_{k=1}^{\infty}\sigma_1^*(k)\,e^{\pi i(\tau+2)k}\\
&= -\pi^2 - 8\pi^2\sum_{k=1}^{\infty}\sigma_1^*(k)\,e^{\pi i\tau k}\left(e^{2\pi i}\right)^k\\
&= -\pi^2 - 8\pi^2\sum_{k=1}^{\infty}\sigma_1^*(k)\,e^{\pi i\tau k}\\
&= E_2^*(\tau).
\end{aligned}$$

Así, la periodicidad de E_2^* queda probada.

Para probar la fórmula de transformación de E_2^* bajo $\tau \longmapsto -1/\tau$ recogida en la propiedad 2 de la proposición, se parte de la expresión (5.4):

$$E_2^*(\tau) = F\left(\frac{\tau}{2}\right) - 4F(2\tau).$$

Al tener E_2^* expresado en función de F, es posible usar el Lema 5.3 para demostrar la segunda propiedad de la proposición.

$$\begin{aligned}
E_2^*(-1/\tau) &= F(-1/(2\tau)) - 4F(-2/\tau)\\
&= \left[4\tau^2F(2\tau) - 4\pi i\tau\right] - 4\left[(\tau/2)^2F(\tau/2) - \pi i\tau\right]\\
&= 4\tau^2F(2\tau) - 4(\tau/2)^2F(\tau/2)\\
&= -\tau^2(F(\tau/2) - 4F(2\tau))\\
&= -\tau^2E_2^*(\tau).
\end{aligned}$$

Así, la segunda propiedad queda demostrada.

La tercera propiedad se prueba partiendo de la expresión (5.5):

$$F\left(\tau\right)=\frac{\pi^2}{3}-8\pi^2\sum_{k=1}^{\infty}\sigma_1(k)e^{2\pi i\tau k},$$

donde el sumatorio tiende a 0 cuando $\Im(\tau)\longrightarrow\infty$.

A la vista de la tendencia de la serie, se tiene que cuando $\Im(\tau)\longrightarrow\infty, F\left(\tau\right)\longrightarrow\frac{\pi^2}{3}$.

Entonces, teniendo en cuenta una vez más la expresión (5.4), $E_2^*(\tau)=F\left(\frac{\tau}{2}\right)-4F\left(2\tau\right)$, se tiene que cuando $\Im(\tau)\longrightarrow\infty$, $E_2^*(\tau)\longrightarrow\frac{\pi^2}{3}-\frac{4\pi^2}{3}=-\pi^2$. Así, la tercera propiedad queda probada.

Para probar la última propiedad, se aplica la tercera propiedad del Lema 5.3.

$$F(1/2-1/2\tau)=F\left(\frac{\tau-1}{2\tau}\right)=\left(\frac{2\tau}{\tau-1}\right)^2F\left(\frac{2\tau}{1-\tau}\right)-2\pi i\cdot\frac{2\tau}{1-\tau}.$$

Ahora, para conocer el valor de $F\left(\frac{2\tau}{1-\tau}\right)$, se aplican dos de las propiedades del Lema 5.3. Primero se considera la periodicidad de F y finalmente se emplea la tercera propiedad.

$$F\left(\frac{2\tau}{1-\tau}\right)=F\left(-2+2/(1-\tau)\right)=F(2/\left(1-\tau\right))=\left(\frac{1-\tau}{2}\right)^2F\left(\frac{\tau-1}{2}\right)-2\pi i\left(\frac{\tau-1}{2}\right).$$

Conociendo esto, se sustituye el valor de $F\left(\frac{2\tau}{1-\tau}\right)$ en la identidad hallada previamente. Operando, se obtiene lo que se muestra a continuación:

$$\begin{aligned}F(1/2-1/2\tau)&=\left(\frac{2\tau}{\tau-1}\right)^2F\left(\frac{2\tau}{1-\tau}\right)-2\pi i\frac{2\tau}{1-\tau}\\&=\left(\frac{2\tau}{\tau-1}\right)^2\left[\left(\frac{\tau-1}{2}\right)^2F\left(\frac{\tau-1}{2}\right)-2\pi i\left(\frac{\tau-1}{2}\right)\right]-2\pi i\frac{2\tau}{1-\tau}\\&=\tau^2F\left(\frac{\tau-1}{2}\right)-2\pi i\left(\frac{2\tau}{\tau-1}\right)^2\left(\frac{\tau-1}{2}\right)-2\pi i\left(\frac{2\tau}{1-\tau}\right)\\&=\tau^2F\left(\frac{\tau-1}{2}\right)-2\pi i\left(\frac{2\tau^2}{\tau-1}\right)-2\pi i\left(\frac{2\tau}{1-\tau}\right).\end{aligned}$$

Aplicando el Lema 5.3 también se tiene que $F\left(2-2/\tau\right)=F\left(-2/\tau\right)=\left(\frac{\tau^2}{4}\right)F\left(\tau/2\right)-2\pi i\tau/2$. Entonces, empleando la expresión (5.4) y aplicando sobre esta la identidad anterior, se llega a lo siguiente:

$$\begin{aligned}
E_2^*(1-1/\tau) &= F(1/2-1/2\tau) - 4F(2-2/\tau) \\
&= \tau^2 F\left(\frac{\tau-1}{2}\right) - 2\pi i\left(\frac{2\tau}{1-\tau}\right) - 2\pi i\left(\frac{2\tau^2}{\tau-1}\right) - 4\left[\left(\frac{\tau^2}{4}\right) F\left(\tau/2\right) - \pi i\tau\right] \\
&= \tau^2\left[F\left(\frac{\tau-1}{2}\right) - F\left(\tau/2\right)\right] - 2\pi i\left(\frac{2\tau}{1-\tau} + \frac{2\tau^2}{\tau-1}\right) + 4\pi i\tau \\
&= \tau^2\left[F\left(\frac{\tau-1}{2}\right) - F\left(\tau/2\right)\right] - 4\pi i\tau\left(\frac{1-\tau}{1-\tau}\right) + 4\pi i\tau \\
&= \tau^2\left[F\left(\frac{\tau-1}{2}\right) - F\left(\tau/2\right)\right].
\end{aligned}$$

Considerando la expresión (5.5) y que $E_2^*\left(1-1/\tau\right) = \tau^2\left[F\left(\frac{\tau-1}{2}\right) - F\left(\tau/2\right)\right]$, se tiene la siguiente igualdad:

$$E_2^*(1-1/\tau) = \tau^2\left[8\pi^2\sum_{k=1}^{\infty}\sigma_1\left(k\right)e^{\pi ik\tau}\left(1-e^{\pi ik\tau}\right)\right].$$

De esto se tiene que, cuando $\Im(\tau)\longrightarrow\infty$:

$$\left|E_2^*\left(1-1/\tau\right)\right| = O\left(\left|\tau^2 e^{\pi i\tau}\right|\right).$$

Así, la última propiedad queda probada y, con ella, la proposición para E_2^*.

La comprobación de las mismas propiedades para θ^4 se lleva a cabo de forma parecida a la demostración de las propiedades análogas del teorema de los dos cuadrados. Para la primera propiedad, simplemente se considera el siguiente cálculo:

$$\theta\left(\tau+2\right)^4 = \sum_{n=-\infty}^{\infty} e^{2\pi in^2(\tau+2)} = \sum_{n=-\infty}^{\infty} e^{2\pi in^2\tau}e^{4\pi in^2} = \sum_{n=-\infty}^{\infty} e^{2\pi in^2\tau} = \theta(\tau)^4.$$

Para la segunda propiedad, no hace falta más que considerar que $\theta(\tau)^2 = i\tau^{-1}\theta(-1/\tau)^2$, como se había visto en la Proposición 3.3. Al elevar al cuadrado los dos términos de la identidad anterior, se ollega a que $\theta(\tau)^4 = -\tau^{-2}\theta(-1/\tau)^4$.

En la tercera propiedad, se parte de que $\theta(\tau)^4 = \sum_{n=0}^{\infty} r_4(n)e^{\pi i\tau n}$ y se observa como si $\Im(\tau)\longrightarrow\infty$, entonces los términos del sumatorio tienden a cero, excepto el término que se corresponde con $n=0$. De esta forma, $\theta(\tau)^4$ tiende al valor del término para $n=0$, que es la unidad.

Para la última propiedad, se tiene en cuenta de nuevo la Proposición 3.3. Así, se tiene que cuando $\Im(\tau)\longrightarrow\infty$, $\left|\theta\left(1-1/\tau\right)^2\right| = O\left(\left|\tau e^{\frac{1}{2}\pi i\tau}\right|\right)$. Esto permite deducir que $\left|\theta\left(1-1/\tau\right)^4\right| = O\left(\left|\tau^2 e^{\pi i\tau}\right|\right)$. □

Ahora, para probar el teorema de los cuatro cuadrados, se considera el cociente $f(\tau) = E_2^*(\tau)/\theta(\tau)^4$.

Por la Proposición 5.4 se tiene que tanto E_2^* como $-\pi^2\theta^4$ cumplen que $E_2^*(\tau+2) = E_2^*(\tau)$ y que $E_2^*(\tau) = -\tau^{-2}E_2^*(-1/\tau)$, por lo que está claro que $f(\tau+2) = f(\tau)$ y que $f(\tau) = f(-1/\tau)$.

De acuerdo con la Proposición 5.4, se tiene que cuando $\Im(\tau) \longrightarrow \infty$, $\theta(\tau)^4 \longrightarrow 1$. Además, considerando la Proposición 3.3 y el cuadrado de θ^2, se tiene que cuando $\Im(\tau) \longrightarrow \infty$, $\theta(1-1/\tau)^4 \sim 16\tau^2\, e^{\pi i\tau}$.

Se tiene que $f(\tau+2) = f(\tau)$, $f(\tau) = f(-1/\tau)$ y que f está acotada, por lo que se cumplen las condiciones que permiten emplear el Teorema 3.4 para ver que $f(\tau)$ es constante. Por lo establecido en la Proposición 5.4, se tiene que E_2^* y $-\pi^2\theta^4$ tienen las mismas propiedades, por lo que $f(\tau) = \frac{E_2^*(\tau)}{\theta(\tau)^4} = \frac{-\pi^2 E_2^*(\tau)}{-\pi^2\theta(\tau)^4} = -\pi^2$. Así, está claro que la constante va a ser igual a $-\pi^2$. De esta forma se ha visto que θ^4 y E_2^* cumplen las mismas propiedades estructurales y por tanto la igualdad $\theta^4 = -\frac{1}{\pi^2}\, E_2^*$ se cumple. Por la Proposición 5.2, esta identidad es equivalente al teorema de los cuatro cuadrados, por lo que esto quedaría probado.

5.1. Comportamiento asintótico

Ahora, para complementar el estudio del teorema de los cuatro cuadrados, se considera $r_4(n)$ y se estudia su comportamiento asintótico. Se tiene que $r_4(n) = 24$ para una cantidad infinita de valores de n, mientras que, por otro lado, se cumple que $\limsup_{n\longrightarrow\infty} r_4(n)/n = \infty$.

Se consideran los enteros positivos de la forma $n = 2^k$. Se tiene que si $k = 1$, n no es divisor de 4 y, por la expresión (5.6), $r_4(n) = 8\sigma_1^*(n) = 8\sigma_1(n) = 8\cdot(1+2) = 24$. Para $k > 1$, n será divisor de 4 y, por lo tanto, la expresión (5.6) establece que

$$\begin{aligned} r_4(n) = 8\sigma_1^*(n) &= 8\left(\sigma_1(n) - 4\sigma_1(n/4)\right) \\ &= 8\left(\sum_{l=0}^{k} 2^l - 4\cdot\sum_{l=2}^{k} 2^{l-2}\right) \\ &= 8\left(\sum_{l=0}^{k} 2^l - \sum_{l=2}^{k} 2^l\right) \\ &= 8\cdot(1+2) = 24. \end{aligned}$$

Así, está claro que $r_4(n) = 24$ para una cantidad infinita de valores de n.

Se consideran ahora los enteros positivos de la forma $n = q^k$, donde q es impar y arbitrariamente grande. Como q es impar, está claro que n no va a ser divisible por 4 y, por lo tanto, de acuerdo con la expresión (5.6), $r_4(n) = 8\sigma_1^*(n) = 8\sigma_1(n)$.

Sea $\{p_1, ..., p_k\}$ una numeración de los números primos impares que conforman n. Si n es un número primo p_1, entonces los divisores de n son 1 y p_1, por lo que $\sigma_1(n) = 1 + p_1$. Se supone de esta forma que, si n es el producto de $k-1$ números primos, se cumple que $\sigma_1(n) = (1+p_1)\cdots(1+p_{k-1})$. Enotonces, hay que probar que si n es el producto de k primos, $\sigma_1(n) = (1+p_1)\cdots(1+p_k)$. Se sabe por hipótesis que los divisores de $n_{k-1} = p_1\cdots p_{k-1}$ suman $(1+p_1)\cdots(1+p_{k-1})$. Al multiplicar dicho n_{k-1} por p_k, se tienen todos los divisores que ya se tenían para n_{k-1} y se añade cada uno de estos multiplicado por p_k. Esto es equivalente a que $\sigma_1(n) = (1+p_1)\cdots(1+p_{k-1})(1+p_k)$. En el nuevo término $(1+p_k)$, el 1 recoge los divisores que ya lo eran sin p_k y el propio p_k recoge los nuevos. De esta forma, queda probado por inducción que $\sigma_1(n) = (1+p_1)\cdots(1+p_k)$.

Ahora, falta comprobar la divergencia del límite.

$$\begin{aligned}
\lim_{k\longrightarrow\infty} \frac{r_4(q^k)}{q^k} &= 8 \lim_{k\longrightarrow\infty} \frac{\sigma_1(q^k)}{q^k} \\
&= 8 \lim_{k\longrightarrow\infty} \frac{(1+p_1)\cdots(1+p_k)}{p_1\cdots p_k} \\
&= 8 \lim_{k\longrightarrow\infty} \left(\frac{1}{p_1}+1\right)\cdots\left(\frac{1}{p_k}+1\right) \\
&= 8 \lim_{k\longrightarrow\infty} \sum_{i=1}^{k} \left(\frac{1}{p_i}+1\right) = \infty.
\end{aligned}$$

Así, queda claro que $\limsup_{n\longrightarrow\infty} r_4(n)/n = \infty$. De esta forma, existe una cantidad infinita de valores para la que el número de posibles descomposiciones como la suma de cuatro cuadrados es 24, pero también se tiene que en el límite para números enteros muy grandes, la cantidad de posibles representaciones como la suma de cuatro cuadrados tiende al infinito.

5.2. Reinterpretación del teorema

Para complementar el estudio de los teoremas de las sumas de cuadrados todavía más, se presenta una identidad relacionada con θ^4, que es equivalente al teorema de los cuatro cuadrados. Con el objetivo de estudiar de nuevo este teorema, se establece una identidad relativa a la función theta sin hacer uso de las propiedades modulares que se emplearon previamente en el capítulo en el proceso por el que se llega a esta. Teniendo en cuenta que $q = e^{\pi i\tau}$, la identidad en cuestión es:

$$\theta(\tau)^4 = 1 + 8\sum_{n=1}^{\infty} \frac{q^n}{\left(1+(-1)^n q^n\right)^2}. \tag{5.10}$$

El primer paso para probar la identidad anterior es demostrar la siguiente relación general:

$$\sum_{n=1}^{\infty} \sigma_l(n)\, q^n = \sum_{n=1}^{\infty} \frac{n^l q^n}{1-q^n}, \quad |q| < 1, \tag{5.11}$$

donde $\sigma_l(n)$ es la suma de las l-ésimas potencias de los divisores de n.

Esta expresión solo es necesaria durante el desarrollo de la demostración en el caso $l = 1$, pero aún así se prueba la fórmula general para llevar a cabo un estudio más completo.

Se tiene en cuenta que $\sigma_l(n) = \sum_{d|n} d^l$. Así, la expresión a la izquierda de (5.11) se puede escribir de la siguiente forma:

$$\sum_{n=1}^{\infty} \sigma_l(n)\, q^n = \sum_{n=1}^{\infty} \left(\sum_{d|n} d^l \right) q^n.$$

Todo entero n se puede expresar como el producto de un divisor d y un entero m. De esta forma, se tiene la siguiente igualdad:

$$\sum_{n=1}^{\infty} \sigma_l(n) q^n = \sum_{m=1}^{\infty} \sum_{d=1}^{\infty} d^l q^{md} = \sum_{m=0}^{\infty} \sum_{d=1}^{\infty} d^l q^{(m+1)d}.$$

Las series que se tienen deben ser convergentes, ya que cada elemento que las constituye es finito y, para $|q| < 1$, q^{md} es convergente. Además, los términos q^{md} decaen exponencialmente y dominan sobre los términos d^l. Así, en los elementos de la forma $d^l q^{md}$, el término q^{md} hace que los elementos de la serie tiendan a cero para valores de m y d altos. Como todos los elementos son finitos, está claro que las series deven ser convergentes. Esto permite cambiar el orden de los sumatorios sin que el valor al que convergen las series se vea alterado. Entonces, la serie se reescribe como

$$\sum_{n=1}^{\infty} \sigma_l(n) q^n = \sum_{d=1}^{\infty} \sum_{m=0}^{\infty} d^l q^{(m+1)d} = \sum_{d=1}^{\infty} d^l q^d \sum_{m=0}^{\infty} q^{md}.$$

Ahora, como $|q| < 1$, la serie en m es una serie geométrica convergente que cumple que $\sum_{m=1}^{\infty} q^{md} = \frac{1}{1-q^d}$. En base a esto, se tiene que:

$$\sum_{n=0}^{\infty} \sigma_l(n) q^n = \sum_{d=1}^{\infty} d^l q^d \frac{1}{1-q^d} = \sum_{n=1}^{\infty} \frac{n^l q^n}{1-q^n}.$$

El siguiente paso consiste en considerar el caso en el que $l = 1$ y demostrar la siguiente igualdad:

$$\sum_{n=1}^{\infty} \frac{n q^n}{1-q^n} = \sum_{n=1}^{\infty} \frac{q^n}{(1-q^n)^2}. \tag{5.12}$$

Se vuelve a expresar $\frac{1}{1-q^n}$ como una serie geométrica, de tal forma que $\frac{1}{1-q^n} = \sum_{m=0}^{\infty} q^{nm}$. Esto permite que se establezca la siguiente identidad:

$$\sum_{n=1}^{\infty} \frac{nq^n}{1-q^n} = \sum_{n=1}^{\infty} nq^n \sum_{m=0}^{\infty} q^{nm}.$$

Como las series son convergentes, es posible cambiar el orden de los sumatorios, de forma que se obtenga la siguiente relación:

$$\sum_{n=1}^{\infty} \frac{nq^n}{1-q^n} = \sum_{m=0}^{\infty} \sum_{n=1}^{\infty} nq^n q^{nm} = \sum_{m=0}^{\infty} \sum_{n=1}^{\infty} nq^{n(m+1)}.$$

Ahora, se considera que la serie $\sum_{n=1}^{\infty} nx^n$ converge a $\frac{x}{(1-x)^2}$. Esto permite expresar las series presentadas previamente como:

$$\sum_{n=1}^{\infty} \frac{nq^n}{1-q^n} = \sum_{m=0}^{\infty} \frac{q^{m+1}}{(1-q^{m+1})^2} = \sum_{k=1}^{\infty} \frac{q^k}{(1-q^k)^2}.$$

El objetivo de la demostración pasa a ser el de probar el siguiente resultado:

$$\sum_{n=1}^{\infty} \frac{nq^n}{1-q^n} - \sum_{n=1}^{\infty} \frac{4nq^{4n}}{1-q^{4n}} = \sum_{n=1}^{\infty} \frac{q^n}{(1-q^n)^2} - 4\sum_{n=1}^{\infty} \frac{q^{4n}}{(1-q^{4n})^2} = \sum_{n=1}^{\infty} \sigma_1^*(n) q^n. \tag{5.13}$$

La primera igualdad es inmediata, sin más que considerar la expresión (5.12), que se acaba de probar. Para la segunda igualdad, primero hay que considerar la expresión (5.11), que permite obtener la siguiente igualdad:

$$\sum_{n=1}^{\infty} \frac{nq^n}{1-q^n} - \sum_{n=1}^{\infty} \frac{4nq^{4n}}{1-q^{4n}} = \sum_{n=1}^{\infty} \sigma_1(n) q^n - \sum_{n=1}^{\infty} \sigma_1\left(\frac{n}{4}\right) q^n.$$

Ahora, basta con considerar la expresión (5.6), con la que se define $\sigma_1^*(n)$.

$$\sum_{n=1}^{\infty} \sigma_1(n) q^n - \sum_{n=1}^{\infty} \sigma_1\left(\frac{n}{4}\right) q^n = \sum_{n=1}^{\infty} \sigma_1^*(n) q^n.$$

Con la prueba de la identidad (5.13), ya se tienen todos los resultados previos necesarios para probar el enunciado equivalente al teorema de los cuatro cuadrados recogido en (5.10). Lo primero que se considera es el enunciado del teorema de los cuatro cuadrados, que se reduce a $r_4(n) = 8\sigma_1^*(n)$. Al tener en cuenta que también se cumple la relación $\theta(\tau)^4 = \sum_{n=0}^{\infty} r_4(n)\, q^n$, se cumplen las siguientes igualdades:

$$\theta(\tau)^4 = \sum_{n=0}^{\infty} r_4(n) q^n = 8\sum_{n=0}^{\infty} \sigma_1^*(n) q^n = 1 + 8\sum_{n=1}^{\infty} \sigma_1^*(n) q^n.$$

De esta forma, solo es necesario probar que $\sum_{n=1}^{\infty}\sigma_1^*(n)q^n = \sum_{n=1}^{\infty}\frac{q^n}{\left(1+(-1)^n q^n\right)^2}$. A la vista de la expresión (5.13), esta igualdad es equivalente a probar que

$$\sum_{n=1}^{\infty}\frac{q^n}{\left(1+(-1)^n q^n\right)^2} = \sum_{n=1}^{\infty}\frac{q^n}{(1-q^n)^2} - 4\sum_{n=1}^{\infty}\frac{q^{4n}}{(1-q^{4n})^2}.$$

Solo el primer sumatorio del término a la derecha de la expresión anterior proporciona elementos con valores de n impares. Por otro lado, el término a la izquierda es $\sum_{n=1}^{\infty}\frac{q^n}{(1-q^n)^2}$ para valores de n impares. Las expresiones de ambos sumatorios son las mismas, por lo que el caso en el que n es impar queda probado.

Para el caso en el que n es par, el término a la izquierda de la igualdad es $\sum_{n=1}^{\infty}\frac{q^n}{(1+q^n)^2}$. Por otro lado, los sumatorios a la derecha de la igualdad se desarrollan de la siguiente forma:

$$\begin{aligned}
\sum_{n=1}^{\infty}\frac{q^{2n}}{(1+q^{2n})^2} &= \sum_{n=1}^{\infty}\left(\frac{q^{2n}}{(1-q^{2n})^2} - \frac{2q^{2n}}{(1-q^{2n})^2}\cdot\frac{2q^{2n}}{(1+q^{2n})^2}\right)\\
&= \sum_{n=1}^{\infty}\left[\frac{q^{2n}}{(1-q^{2n})^2}\cdot\left(1-\frac{4q^{2n}}{(1+q^{2n})^2}\right)\right]\\
&= \sum_{n=1}^{\infty}\left[\frac{q^{2n}}{(1-q^{2n})^2}\cdot\left(\frac{\left(1-q^{2n}\right)^2}{(1+q^{2n})^2}\right)\right]\\
&= \sum_{n=1}^{\infty}\frac{q^{2n}}{(1+q^{2n})^2}.
\end{aligned}$$

La igualdad también se cumple para los términos pares, por lo que la expresión (5.10) se verifica. De esta forma, se ha encontrado un enunciado equivalente al teorema de los cuatro cuadrados.

Capítulo 6

Teorema de los ocho cuadrados

De igual manera que cualquier entero positivo puede ser expresado como la suma de cuatro cuadrados, también se puede escribir como la suma de ocho cuadrados. De esta forma, la cuestión que surge vuelve a ser el número de formas en las que se puede representar un entero n como la suma de ocho cuadrados.

Primero, se denota por $\sigma_3^*(n)$ a la suma de la potencia tercera de los divisores de n que no son divisibles por cuatro y por $\sigma_3(n)$ a la suma de la potencia tercera de los divisores de n. Además, $\sigma_3^p(n)$ y $\sigma_3^i(n)$ denotan la suma de la tercera potencia de los divisores de n que son pares e impares, respectivamente.

$$\sigma_3^*(n) = \begin{cases} \sigma_3(n) & \text{si } n \text{ es impar.} \\ \sigma_3^p(n) - \sigma_3^i(n) & \text{si } n \text{ es par.} \end{cases} \tag{6.1}$$

Con σ_3^* definida, se presenta el siguiente teorema, que da respuesta a la cuestión de la cantidad de formas en las que se puede expresar un entero positivo como la suma de .

Teorema 6.1. *Todo entero positivo es la suma de ocho cuadrados y, además, para todo $n \geq 1$:*

$$r_8(n) = 16\sigma_3^*(n). \tag{6.2}$$

Ahora, se establece una relación que identifica la función generatriz de la sucesión $\{r_8(n)\}_{n=1}^{\infty}$ con la potencia octava de la función θ, tal y como se hizo en los teoremas de los dos y los cuatro cuaadrados con sus respectivas potencias.

$$\theta(\tau)^8 = \sum_{n=0}^{\infty} r_8(n)q^n, \quad \text{con } q = e^{\pi i\tau},\ \tau \in \mathbb{H}. \tag{6.3}$$

Para poder demostrar el teorema, se pretende encontrar la función modular cuya igualdad con $\theta(\tau)^8$ exprese la identidad $r_8(n) = 16\sigma_3^*(n)$ de una forma alternativa. Una vez más, se considera una función que supone una ligera variación de las series de Eisenstein, aunque en esta ocasión el valor del exponente es de $n = 4$. Entonces, para $\tau \in \mathbb{H}$ y para valores de n y m de distinta paridad, se define E_4^* de la siguiente manera:

$$E_4^*(\tau) = \sum_{(n,m)} \frac{1}{(m\tau + n)^4}, \text{ con } n \text{ y } m \text{ de distinta paridad.} \tag{6.4}$$

Las series representadas convergen absolutamente, al contrario de lo que pasaba con las E_2^* consideradas en la demostración del teorema de los cuatro cuadrados. Esto facilita la manipulación de las series y evita la imposición de un orden sobre las sumas.

La siguiente proposición es equivalente al Teorema 6.1 y reduce el teorema de los ocho cuadrados a las propiedades modulares de E_4^*.

Proposición 6.2. *La igualdad $r_8(n) = 16\sigma_3^*(n)$ es equivalente a la identidad*

$$\theta(\tau)^8 = -\frac{48}{\pi^4}\, E_4^*(\tau)\,, \text{ donde } \tau \in \mathbb{H}.$$

Demostración. Se consideran las series de Eisenstein de orden $k = 4$, cuya expresión es la que se muestra a continuación:

$$E_4(\tau) = \sum_{(n,m)\neq(0,0)} \frac{1}{(n + m\tau)^4}. \tag{6.5}$$

Se considera la expresión que relaciona la función E_4^* con las series de Eisenstein. Esta considera que E_4^* es la serie de Eisenstein de orden $k = 4$, representada por el primer sumatorio, restando de esta los elementos con la misma paridad, que se recogen en el segundo sumatorio.

$$E_4^*(\tau) = E_4(\tau) - \frac{E_4\left(\frac{\tau-1}{2}\right)}{2^4}. \tag{6.6}$$

Se tiene en cuenta la siguiente expresión, que viene dada por la aplicación del Teorema 1.23 al caso en el que $k = 4$ y relaciona las series de Eisenstein de orden $k = 4$ con σ_3:

$$E_4(\tau) = 2\zeta(4) + \frac{(2\pi)^4}{3} \sum_{k=1}^{\infty} \sigma_3(k)\, e^{2\pi i k\tau}, \tag{6.7}$$

donde $\zeta(4)$ se corresonde con el valor de la función zeta de Riemann evaluada en $k = 4$, esto es, $\zeta(4) = \frac{\pi^4}{90}$.

Para probar la proposición se tienen en cuenta (6.2) y (6.3), de manera que basta con demostrar que

$$-\frac{48}{\pi^4}\, E_4^*(\tau) = 1 + \sum_{k=1}^{\infty} 16\sigma_3^*(k) q^k.$$

Se consideran las expresiones (6.6) y (6.7), que dan lugar a la siguiente igualdad:

$$
\begin{aligned}
E_4^*(\tau) &= E_4(\tau) - \frac{E_4\left(\frac{\tau-1}{2}\right)}{2^4} \\
&= 2\zeta(4) + \frac{(2\pi)^4}{3}\sum_{k=1}^{\infty}\sigma_3(k)\,e^{2\pi i\tau k} - \frac{\zeta(4)}{8} - \frac{\pi^4}{3}\sum_{k=1}^{\infty}\sigma_3(k)\,e^{\pi i(\tau-1)k} \\
&= \frac{15}{8}\zeta(4) + \frac{(2\pi)^4}{3}\sum_{k=1}^{\infty}\sigma_3(k)\,e^{2\pi i\tau k} - \frac{\pi^4}{3}\sum_{k=1}^{\infty}\sigma_3(k)\,e^{\pi i\tau k}e^{-\pi ik} \\
&= \frac{15}{8}\cdot\frac{\pi^4}{90} + \frac{(2\pi)^4}{3}\sum_{k=1}^{\infty}\sigma_3(k)\,e^{2\pi i\tau k} - \frac{\pi^4}{3}\sum_{k=1}^{\infty}\sigma_3(k)\,e^{\pi i\tau k}(-1)^k \\
&= \frac{\pi^4}{48}\left(1 + 16^2\sum_{k=1}^{\infty}\sigma_3(k)\,e^{2\pi i\tau k} - 16\sum_{k=1}^{\infty}\sigma_3(k)\,e^{\pi i\tau k}(-1)^k\right).
\end{aligned}
$$

Primero, se consideran los casos en los que se tengan valores de k impares. En estas condiciones, $(-1)^k = -1$ y $\sigma_3(k) = \sigma_3^*(k)$ para cualquier valor de k. Además, también se tiene en cuenta que no existen divisores pares para ningún valor de k. Así, denotando $q = e^{\pi i\tau}$, la expresión anterior se desarrolla de la siguiente manera:

$$
\begin{aligned}
E_4^*(\tau) &= \frac{\pi^4}{48}\left[1 + 16^2\sum_{k=1}^{\infty}\left(\sum_{d|k}d^3e^{2\pi i\tau k}\right) + 16\sum_{k=1}^{\infty}\sigma_3(k)\,e^{\pi i\tau k}\right] \\
&= \frac{\pi^4}{48}\left[1 + 2\cdot 16\sum_{k=1}^{\infty}\left(\sum_{2d|k}(2d)^3\,e^{2\pi i\tau k}\right) + 16\sum_{k=1}^{\infty}\sigma_3^*(k)\,e^{\pi i\tau k}\right] \\
&= \frac{\pi^4}{48}\left(1 + \sum_{k=1}^{\infty}16\sigma_3^*(k)\,e^{\pi i\tau k}\right),
\end{aligned}
$$

donde la última igualdad es consecuencia de que $\sum_{k=1}^{\infty}\left(\sum_{2d|k}(2d)^3\,e^{2\pi i\tau}\right)$ se anule. Esto se debe a que el sumatorio es sobre los valores pares de d(de la forma $2d$) que dividen a k. Sin embargo, k es un entero impar, por lo que ningún entero de la forma $2d$ será divisor de k. Entonces, la serie no tiene ningún elemento no nulo y por esto se anula.

Ahora, se consideran los casos en los que se tienen valore de k pares. En estas condiciones, $(-1)^k = 1$ y $\sigma_3^*(k) = \sigma_3^p(k) - \sigma_3^i(k)$ para cualquier valor de k. De esta forma, se considera un entero k_1 de la forma $k_1 = 2^{r-1}m$ y otro entero k_2 de la forma $k_2 = 2^r m$, donde m es el producto de todos los factores impares de k_1 y de k_2, respectivamente. Esto permite que se obtenga la siguiente expresión de $E_4^*(\tau)$:

$$\begin{aligned}
E_4^*(\tau) &= \frac{\pi^4}{48}\left[1+16^2\sum_{k_1=1}^{\infty}\left(\sum_{d|k_1} d^3 e^{2\pi i\tau k_1}\right) - 16\sum_{k_2=1}^{\infty}\left(\sum_{d|k_2} d^3 e^{\pi i\tau k_2}\right)\right]\\
&= \frac{\pi^4}{48}\left[1+2\cdot 16\sum_{k_1=1}^{\infty}\left(\sum_{2d|k_1}(2d)^3 e^{2\pi i\tau k_1}\right) - 16\sum_{k_2=1}^{\infty}\left(\sum_{d|k_2} d^3 e^{\pi i\tau k_2}\right)\right]\\
&= \frac{\pi^4}{48} + 2\cdot\frac{\pi^4}{3}\sum_{k=1}^{\infty}\left[\sum_{d|m}\left((2d)^3+(4d)^3+\cdots+(2^r d)^3\right)e^{2\pi i\tau k}\right]\\
&- \frac{\pi^4}{3}\sum_{k=1}^{\infty}\left[\sum_{d|m}\left(d^3+(2d)^3+\cdots+(2^m d)^3\right)e^{\pi i\tau k}\right]\\
&= \frac{\pi^4}{48}\cdot\left[1+16\sum_{k=1}^{\infty}\sum_{d|m}(-1)^d d^3 e^{\pi i\tau k}\right]\\
&= \frac{\pi^4}{48}\cdot\left[1+16\sum_{k=1}^{\infty}\sum_{d|m}\left(\sigma_3^p(k)-\sigma_3^p(k)\right)e^{\pi i\tau k}\right].
\end{aligned}$$

Si ahora se considera la expresión (6.1), la forma general de $E_4^*(\tau)$ es la que se muestra a continuación:

$$E_4^*(\tau) = \frac{\pi^4}{48}\cdot\left[1+\sum_{k=1}^{\infty}16\sigma_3^* e^{\pi i\tau k}\right].$$

De esta forma, la proposición queda probada. □

Ahora, el teorema de los ocho cuadrados se ha reducido a la identidad $\theta^8(\tau) = -\frac{48}{\pi^4}\, E_4^*$. Para demostrar esto hay que probar que E_4^* satisface las mismas propiedades modulares que θ^8. La siguiente proposición recoge lo necesario para que esto se dé y poder probar el Teorema 6.1.

Proposición 6.3. *La función $E_4^*(\tau)$ definida en el semiplano superior tiene las siguientes propiedades:*

1. $E_4^*(\tau+2) = E_4^*(\tau)$.
2. $E_4^*(\tau) = \tau^{-4}E_4^*(-1/\tau)$.
3. $\frac{48}{\pi^4}E_4^*(\tau) \longrightarrow 1$, *cuando* $\Im(\tau)\longrightarrow\infty$.
4. $|E_4^*(1-1/\tau)| \approx |\tau|^4\left|e^{2\pi i\tau}\right|$, *cuando* $\Im(\tau)\longrightarrow\infty$.

Además, θ^8 cumple las mismas propiedades.

Demostración. La primera propiedad de la proposición se prueba de manera sencilla de la siguiente forma:

$$\begin{aligned}
E_4^*(\tau+2) &= \frac{\pi^4}{48}\left[1+\sum_{k=1}^{\infty}16\sigma_3^*(k)\,e^{\pi i(\tau+2)k}\right]\\
&= \frac{\pi^4}{48}\left[1+\sum_{k=1}^{\infty}16\sigma_3^*(k)\,e^{\pi i\tau k}\left(e^{2\pi i}\right)^k\right]\\
&= \frac{\pi^4}{48}\left[1+\sum_{k=1}^{\infty}16\sigma_3^*(k)\,e^{\pi i\tau k}\right]\\
&= E_4^*(\tau).
\end{aligned}$$

Esto prueba la periodicidad de E_4^*.

Ahora, se busca demostrar la fórmula de transformación de E_4^* bajo $\tau \longmapsto -1/\tau$. Primero, se considera la expresión (6.6):

$$E_4^*(\tau) = E_4(\tau) - \frac{E_4\left(\frac{\tau-1}{2}\right)}{2^4}.$$

Se ha expresado E_4^* en función de las series de Eisenstein E_4, que son convergentes. En esta situación, el orden de los sumatorios no modifica el valor de la serie, por lo que no hay necesidad de introducir un lema análogo al presentado en la demostración del teorema de los cuatro cuadrados para demostrar la segunda propiedad de la proposición. Con esto en consideración, se busca relacionar $E_4^*(\tau)$ con $E_4^*(-1/\tau)$ a partir de lo siguiente:

$$(n+m(-1/\tau))^4 = \tau^{-4}(-m+n\tau)^4.$$

El término a la izquierda en la igualdad anterior representa cada uno de los elementos de $E_4(-1/\tau)$, mientras que el término a la derecha representa cada uno de los elementos de $\tau^4 E_4(\tau)$, por lo que se cumple que $E_4(-1/\tau) = \tau^4 E_4(\tau)$.

Se repite el cálculo anterior para relacionar $E_4\left(\frac{-1/\tau-1}{2}\right)$ con $E_4\left(\frac{\tau-1}{2}\right)$. El primero de los términos se expresa como $E_4\left(-\frac{1+\tau}{2\tau}\right)$.

$$\left[n+m\left(-\frac{1+\tau}{2\tau}\right)\right]^4 = \tau^{-4}\left(-m\cdot\frac{1+\tau}{2}+n\tau\right)^4 = \tau^{-4}\left[-\frac{m}{2}+\left(n-\frac{m}{2}\right)\tau\right]^4.$$

De esto se concluye que $E_4\left(-\frac{1+\tau}{2\tau}\right) = (2\tau)^{-4}E_4\left(\frac{\tau-1}{2}\right)$. Así, teniendo en cuenta la expresión

(6.6) se tiene lo siguiente:

$$\begin{aligned}
E_4^*(-1/\tau) &= E_4(-1/\tau) - 2^{-4} E_4\left(-\frac{1+\tau}{2\tau}\right) \\
&= \tau^4 E_4(\tau) - 2^{-4} \cdot (\tau)^4 \, E_4\left(\frac{\tau-1}{2}\right) \\
&= \tau^4 \left[E_4(\tau) - 2^{-4} E_4\left(\frac{\tau-1}{2}\right)\right] \\
&= \tau^4 E_4^*(\tau).
\end{aligned}$$

Así, la segunda propiedad queda demostrada.

Para demostrar la tercera propiedad se parte de la expresión (6.7):

$$E_4(\tau) = 2\zeta(4) + \frac{(2\pi)^2}{3} \sum_{k=1}^{\infty} \sigma_3(k) \, e^{2\pi i k \tau},$$

donde el sumatorio tiende a 0 cuando $\Im(\tau) \longrightarrow \infty$.

Así, se tiene que cuando $\Im(\tau) \longrightarrow \infty, E_4^*(\tau) \longrightarrow 2\zeta(4)$.

Entonces, al tener en cuenta una vez más la expresión (6.6), $E_4^*(\tau) = E_4(\tau) - \frac{E_4\left(\frac{\tau-1}{2}\right)}{2^4}$, se tiene que cuando $\Im(\tau) \longrightarrow \infty$:

$$E_4^*(\tau) \longrightarrow 2\zeta(4) - \frac{2\zeta(4)}{2^4} = 2 \cdot \frac{\pi^4}{90} - \frac{1}{2^4} \cdot 2 \cdot \frac{\pi^4}{90} = \frac{\pi^4}{45} - \frac{\pi^4}{720} = \frac{\pi^4}{48}.$$

Así, la tercera propiedad queda probada.

Para probar la última propiedad, se opera de la siguinete forma:

$$E_4(1-1/\tau) = E_4\left(\frac{\tau-1}{\tau}\right) = \tau^4 E_4(\tau).$$

Por otro lado, también se desarrolla este otro término:

$$E_4\left(\frac{1-\frac{1}{\tau}-1}{2}\right) = E_4\left(-\frac{1}{2\tau}\right) = 16\tau^4 E_4(2\tau).$$

Con estas dos expresiones, se tiene la siguiente relación:

$$E_4^*(1-1/\tau) = E_4(1-1/\tau) - \frac{E_4\left(\frac{1-\frac{1}{\tau}-1}{2}\right)}{16} = \tau^4 \left(E_4(\tau) - E_4(\tau)\right).$$

Considerando la expresión (6.7, se tiene la siguiente expresión:

$$E_4^*(1-1/\tau) = \tau^4 \left[\frac{(2\pi)^4}{3} \sum_{k=1}^{\infty} \sigma_3(k) \, e^{2\pi i k \tau} \left(1 - e^{2\pi i k \tau}\right)\right].$$

De esto se tiene que, cuando $\Im(\tau) \longrightarrow \infty$:

$$|E_4^* (1 - 1/\tau)| = O\left(|\tau|^4 \left|e^{2\pi i\tau}\right|\right).$$

Así, se cumple que $|E_4^* (1 - 1/\tau)| \approx |\tau|^4 \left|e^{2\pi i\tau}\right|$. Esto se debe a que este es el término dominante en la expresión de $|E_4^* (1 - 1/\tau)|$ y el otro término es despreciable en comparación con este. Esto permite que la última propiedad quede probada y, de esta forma, la proposición quede demostrada.

La comprobación de estas propiedades para θ^8 se realiza de forma similar a las demostraciones análogas de los teoremas de los dos y los cuatro cuadrados. Para la primera propiedad se considera el cálculo siguiente:

$$\theta(\tau + 2)^8 = \sum_{n=-\infty}^{\infty} e^{4\pi i n^2(\tau+2)} = \sum_{n=-\infty}^{\infty} e^{4\pi i n^2\tau} e^{8\pi i n^2} = \sum_{n=-\infty}^{\infty} e^{4\pi i n^2\tau} = \theta(\tau)^8.$$

Para la segunda propiedad, basta con considerar que $\theta(\tau)^4 = -\tau^{-2}\theta(-1/\tau)^4$, como se había visto en la Proposición 5.4. Si se elevan al cuadrado ambos términos de la igualdad anterior, se obtiene que $\theta(\tau)^8 = \tau^{-4}\theta(-1/\tau)^8$.

En la tercera propiedad, al considerar que $\theta(\tau)^8 = \sum_{n=0}^{\infty} r_8(n)e^{\pi i\tau n}$, se ve que si $\Im(\tau) \longrightarrow \infty$, entonces todos los términos del sumatorio tienden a cero a excepción del término correspondiente a $n = 0$. De esta forma, $\theta(\tau)^8$ tiende a 1, que es el valor del término para $n = 0$.

Para la última de las propiedades, se vuelve a tener en cuenta la Proposición 5.4. Así, se tiene que cuando $\Im(\tau) \longrightarrow \infty$, $\left|\theta(1 - 1/\tau)^4\right| = O\left(\left|\tau^2 e^{\pi i\tau}\right|\right)$. Esto permite deducir que $\left|\theta(1 - 1/\tau)^8\right| = O\left(\left|\tau^4 e^{2\pi i\tau}\right|\right)$. □

Ahora, se considera el cociente $f(\tau) = \frac{48}{\pi^4} \cdot E_4^*(\tau)/\theta(\tau)^8$ y se busca comprobar que se cumplen las condiciones de Teorema 3.4.

Está claro que se verifica que $f(\tau + 2) = f(\tau)$ y que $f(-1/\tau) = f(\tau)$, ya que tanto E_4^* como θ^8 las cumplen de manera individual.

De acuerdo con la Proposición 6.3, se tiene que cuando $\Im(\tau) \longrightarrow \infty$, $\theta(\tau)^8 \longrightarrow 1$. Además, considerando la Proposición 5.4 y el cuadrado de θ^4, se tiene que cuando $\Im(\tau) \longrightarrow \infty$, $\theta(1 - 1/\tau)^8 \sim 256\tau^4 e^{2\pi i\tau}$. Esto, junto a las dos últimas propiedades de la Proposición 6.3, permiten ver que la función f está acotada.

Se tiene que $f(\tau + 2) = f(\tau)$, $f(\tau) = f(-1/\tau)$ y que f está acotada, por lo que se cumplen las condiciones que permiten emplear el Teorema 3.4 para ver que $f(\tau)$ es constante. Por lo establecido en la Proposición 6.3, se tiene que $\frac{48}{\pi^4}E_4^*$ y θ^8 tienen las mismas propiedades, por lo que $f(\tau) = \frac{\frac{48}{\pi^4} E_4^*(\tau)}{\theta(\tau)^4} = 1$. Así, queda probado que la constante va a ser igual a 1. De esta forma, se ha visto que θ^8 y E_4^* cumplen las mismas propiedades estructurales y por tanto la igualdad $\theta^8 = \frac{48}{\pi^4} E_2^*$ se cumple. Por la Proposición 6.2, esta identidad es equivalente al teorema de los ocho cuadrados, por lo que este queda probado.

$$c^2 + d^2 = \frac{a^2}{4} + \frac{ab}{2} + \frac{b^2}{4} + \frac{a^2}{4} - \frac{ab}{2} + \frac{b^2}{4} = \frac{a^2}{2} + \frac{b^2}{2} = \frac{1}{2}(a^2 + b^2).$$

Bibliografía

[1] Ahlfors, L. (1979). *Complex analysis: An Introduction to The Theory of Analytic Functions of One Complex Variable*. McGraw Hill.

[2] Christianidis, J.; Oaks, J. (2022). *The Arithmetica of Diophantus: A complete translation and commentary*. Routledge. https://doi.org/10.4324/9781315171470

[3] Conway, J. B. (1973). *Functions of One Complex Variable* (Graduate Texts in Mathematics). Springer. https://doi.org/10.1007/978-1-4615-9972-2

[4] Cox, D. A. (1997). *Primes of the Form* $x^2 + ny^2$. John Wiley & Sons.

[5] Ireland, K.; Rosen, M. I. (1990) *A Classical Introduction to Modern Number Theory* (Graduate Texts in Mathematics). Springer.

[6] Stein, E. M.; Shakarchi, R. (2003). *Complex Analysis* (Princeton Lectures in Analysis II). Princeton University Press.

[7] Stein, E. M.; Shakarchi, R. (2003). *Fourier Analysis: An Introduction* (Princeton Lectures in Analysis I). Princeton University Press.