Universidad Autónoma de Madrid

departamento de matemáticas

Departamento de Matemáticas, Facultad de Ciencias
Universidad Autónoma de Madrid

Las sumas de Gauss en matemáticas y física

Trabajo de fin de grado

Grado en Matemáticas

Autor: Samuel de Lucas Maroto

Tutor: Fernando Chamizo Lorente

Curso 2024-2025

Resumen

Este trabajo estudia las sumas de Gauss y su utilidad en diversas áreas de la física, partiendo de su definición y propiedades básicas hasta conseguir una fórmula cerrada para las mismas. El primer capítulo desarrolla varios resultados preliminares, destacando aquellos que permiten evaluar casos particulares de las sumas de Gauss. El segundo capítulo utiliza estos resultados para demostrar propiedades de los símbolos de Legendre y de Jacobi, como la ley de reciprocidad cuadrática, y culmina con la obtención de una fórmula general para la evaluación de las sumas de Gauss. Los últimos tres capítulos aplican estos resultados a diferentes fenómenos físicos. En el primero se estudia el efecto Talbot, un fenómeno óptico en el que, a distancias adecuadas, los patrones de difracción replican la estructura de la red de difracción. En el segundo se analiza la evolución de filamentos de vórtice poligonales en fluidos, determinando una fórmula para el ángulo entre lados adyacentes. Finalmente, en el último se estudia la aparición de zonas de densidad de probabilidad constante en el problema cuántico de la expansión súbita del pozo de potencial infinito.

Abstract

This work studies Gauss sums and their use in different areas of physics, starting from their definition and basic properties up to a closed formula for them. The first chapter introduces several preliminary results, with those that allow us to evaluate particular cases of Gauss sums being the main ones. The second chapter uses these results to prove properties of the Legendre and Jacobi symbols, such as the quadratic reciprocity law, and culminates with the derivation of a general formula for the evaluation of Gauss sums. The last three chapters apply these results to different phenomena in physics. The first one studies the Talbot effect, an optical phenomenon in which, at certain distances, the diffraction patterns replicate the structure of the diffraction grating. The second one analyzes the evolution of polygonal vortex filaments in fluids, deriving a formula for the angle between adjacent sides. Finally, the last chapter studies the appearance of regions of constant probability density in the quantum problem of the suddenly-expanded infinite potential well.

Índice general

CAPÍTULO 1
Evaluaciones básicas

En este capítulo se definen las sumas de Gauss cuadráticas, concepto sobre el que versa este trabajo. También se comienza el estudio de su evaluación, puesto que obtener un resultado cerrado no es trivial. Por último, se establecen los lemas sobre los que se apoyará el siguiente capítulo.

1.1. Las sumas de Gauss

Las *sumas de Gauss cuadráticas* se definen como

$$G(a,q) = \sum_{n=0}^{q-1} e\left(\frac{an^2}{q}\right) \quad \text{para } a \in \mathbb{Z} \text{ y } q \in \mathbb{Z}^+ \text{ coprimos,}$$

donde la notación $e(x)$ indica la expresión $e^{2\pi ix}$.

Se puede generalizar esta expresión añadiendo un término lineal, obteniendo así las denominadas *sumas de Gauss generalizadas*:

$$G(a,b,q) = \sum_{n=0}^{q-1} e\left(\frac{an^2+bn}{q}\right) \quad \text{con } a,b \in \mathbb{Z} \text{ y } q \in \mathbb{Z}^+, \ a \text{ y } q \text{ coprimos.}$$

Se puede comprobar que, en efecto, esta nueva expresión supone una generalización de las sumas de Gauss cuadráticas, ya que $G(a,0,q) = G(a,q)$.

La evaluación de las sumas de Gauss generalizadas admite una expresión explícita aunque compleja, dividida en varios casos y con una demostración laboriosa. Por ello, se plantea a continuación un estudio preliminar más sencillo, en el que se obtendrá una fórmula para la evaluación de su módulo.

1.2. Evaluación de las sumas de Gauss

Estudio de su módulo

El estudio del módulo de las sumas generalizadas de Gauss comienza considerando primero su cuadrado, de forma que

$$|G(a,b,q)|^2 = \sum_{m=0}^{q-1} e\Big(\tfrac{am^2+bm}{q}\Big) \cdot \sum_{n=0}^{q-1} \overline{e\Big(\tfrac{an^2+bn}{q}\Big)} = \sum_{m,n=0}^{q-1} e\Big(\tfrac{a(n^2-m^2)+b(n-m)}{q}\Big), \tag{1.1}$$

donde se han utilizado las propiedades complejas $|z|^2 = z\overline{z}$ y $\overline{z_1+z_2} = \overline{z_1}+\overline{z_2}$, además de propiedades básicas de la exponencial.

Para continuar desarrollando la expresión, se debe observar que cada sumando se comporta de forma q-periódica en n, es decir, sumando q al índice n se tiene

$$\frac{a\big((n+q)^2-m^2\big)+b(n+q-m)}{q} = \frac{a(n^2-m^2)+b(n-m)}{q} + aq + 2an + bq,$$

concluyendo que sumar q a n solo añade múltiplos de 2π al argumento, resultando en el mismo número complejo. De esta forma, se continua el desarrollo de (1.1) con el cambio $n \mapsto n+m$ módulo q, obteniendo así

$$|G(a,b,q)|^2 = \sum_{n=0}^{q-1} e\Big(\frac{an^2+bn}{q}\Big) \sum_{m=0}^{q-1} e\Big(\frac{2amn}{q}\Big). \tag{1.2}$$

Para simplificar aún más esta expresión se debe estudiar el comportamiento de la suma interior, que se resume en los siguientes casos:

Caso I: $n = 0$

$$\Big[\sum_{m=0}^{q-1} e\Big(\frac{2amn}{q}\Big)\Big]_{n=0} = \sum_{m=0}^{q-1} e(0) = \sum_{m=0}^{q-1} 1 = q.$$

Caso II: $n \neq 0$ y q impar, es decir, $q \nmid 2an$.

$$\sum_{m=0}^{q-1} e\Big(\frac{2amn}{q}\Big) = \sum_{m=0}^{q-1} e\Big(\frac{2an}{q}\Big)^m = \frac{1-e(\frac{2an}{q})^q}{1-e(\frac{2an}{q})} = \frac{1-e(2an)}{1-e(\frac{2an}{q})} = 0. \tag{1.3}$$

Caso III: $n \neq 0$ y q par. Se tiene lo mismo que en (1.3) excepto para $n = q/2 =: q'$.

$$\Big[\sum_{m=0}^{q-1} e\Big(\frac{2amn}{q}\Big)\Big]_{n=q'} = \sum_{m=0}^{q-1} e\Big(\frac{2amq}{2q}\Big) = \sum_{m=0}^{q-1} e(am) = \sum_{m=0}^{q-1} 1 = q.$$

Se concluye entonces que todos los términos de la suma exterior se anulan, excepto los correspondientes a $n = 0$ y, si q es par, a $n = q'$.

Para obtener una expresión cerrada cuando q es par, se continúa el desarrollo de (1.2) teniendo en cuenta para la última igualdad que, como a y q son coprimos, a debe ser impar.

$$\begin{aligned}\big|G(a,b,q)\big|^2 &= e\Big(\frac{a\cdot 0^2+b\cdot 0}{q}\Big)\cdot q + e\Big(\frac{aq'^2+bq'}{q}\Big)\cdot q = \Big(1+e\Big(\frac{aq'+b}{2}\Big)\Big)\cdot q\\ &= \Big(1+\cos\big(\pi(aq'+b)\big)+i\,\mathrm{sen}\,\big(\pi(aq'+b)\big)\Big)\cdot q\\ &= \big(1+(-1)^{aq'+b}\big)\cdot q = \big(1+(-1)^{q'+b}\big)\cdot q\end{aligned}$$

Resumiendo, el módulo de $G(a,b,q)$ viene determinado por la paridad de q.

$$\big|G(a,b,q)\big| = \begin{cases}\sqrt{q} & \text{si } q \text{ es impar,}\\ \frac{1+(-1)^{b+q/2}}{\sqrt{2}}\sqrt{q} & \text{si } q \text{ es par.}\end{cases} \tag{1.4}$$

Esta expresión permite estudiar más propiedades de las sumas de Gauss. A modo de ejemplo se determina a continuación cuándo su valor es cero.

$$\begin{aligned}G(a,b,q)=0 \;&\Leftrightarrow\; |G(a,b,q)|=0 \;\Leftrightarrow\; 1+(-1)^{b+q/2}=0\\ &\Leftrightarrow\; 2 \mid b+q/2-1 \;\Leftrightarrow\; 4 \mid 2b+q-2.\end{aligned}$$

Estudio de $G(1,q)$

Antes de continuar con el estudio de $G(a,b,q)$, resulta conveniente evaluar primero $G(1,q)$. Para ello se utilizará la función $F(x)$, definida como

$$F(x)=\sum_{-x\le k<q-x} e\Big(\frac{(x+k)^2}{q}\Big).$$

Esta función es 1-periódica, ya que

$$F(x+1)=\sum_{-(x+1)\le k<q-(x+1)} e\Big(\frac{(x+1+k)^2}{q}\Big)=\sum_{-x\le k'<q-x} e\Big(\frac{(x+k')^2}{q}\Big)=F(x).$$

Además, es continua en 0 porque

$$\lim_{x\to 0^-}F(x)=\lim_{x\to 0^-}\sum_{k=0}^{q-1}e\Big(\frac{(x+k)^2}{q}\Big)=\sum_{k=0}^{q-1}e\Big(\frac{k^2}{q}\Big)=F(0),$$

$$\lim_{x\to 0^+}F(x)=\lim_{x\to 0^+}\sum_{k=1}^{q}e\Big(\frac{(x+k)^2}{q}\Big)=\sum_{k=1}^{q}e\Big(\frac{k^2}{q}\Big)=\sum_{k=0}^{q-1}e\Big(\frac{k^2}{q}\Big)=F(0),$$

donde se ha utilizado la q-periodicidad del argumento de la exponencial. Por último, es de clase C^∞ en $(0,1)$, ya que F es una suma finita de funciones C^∞ en $(0,1)$.

Teniendo en cuenta estas propiedades, se deduce que la función F coincide con su *serie de Fourier* [7] [17].

$$F(x) = \sum_{n\in\mathbb{Z}} f_n\, e(nx) \qquad \text{con} \quad f_n = \int_0^1 F(t)\, e(-nt)\, dt.$$

Sustituyendo la expresión de F en la fórmula para los *coeficientes de Fourier* y teniendo en cuenta la q-periodicidad en k se obtiene

$$f_n = \int_0^1 e(-nt) \sum_{k=-t}^{q-t-1} e\Big(\frac{(t+k)^2}{q}\Big)\, dt = \int_0^1 e(-nt) \sum_{k=0}^{q-1} e\Big(\frac{(t+k)^2}{q}\Big)\, dt,$$

donde intercambiando el sumatorio con la integral y utilizando el cambio de variable $u = t + k - qn/2$, se tiene

$$\begin{aligned} f_n &= \sum_{k=0}^{q-1} \int_{k-\frac{qn}{2}}^{k+1-\frac{qn}{2}} e\Big(-n\Big(u + \frac{qn}{2} - k\Big)\Big)\, e\Big(\frac{(u+\frac{qn}{2})^2}{q}\Big)\, du \\ &= \sum_{k=0}^{q-1} \int_{k-\frac{qn}{2}}^{k+1-\frac{qn}{2}} e\Big(-nu - \frac{qn^2}{2} + nk + \frac{u^2}{q} + \frac{qn^2}{4} + nu\Big)\, du \\ &= e\Big(-\frac{qn^2}{4}\Big) \sum_{k=0}^{q-1} \int_{k-\frac{qn}{2}}^{k+1-\frac{qn}{2}} e\Big(\frac{u^2}{q}\Big)\, du. \end{aligned}$$

A simple vista, la expresión obtenida para los coeficientes de Fourier puede parecer compleja pero, al considerar su suma sobre los índices pares, se observa que la suma de las integrales recubre toda la recta real, simplificando así la expresión.

$$\sum_{n\in\mathbb{Z}} f_{2n} = \sum_{n\in\mathbb{Z}} e\big(-qn^2\big) \sum_{k=0}^{q-1} \int_{k-qn}^{k+1-qn} e\Big(\frac{u^2}{q}\Big)\, du = \int_{-\infty}^{\infty} e\Big(\frac{t^2}{q}\Big)\, dt$$

De forma análoga se obtiene la expresión para la suma sobre los índices impares.

$$\sum_{n\in\mathbb{Z}} f_{2n+1} = e\Big(\frac{-q}{4}\Big) \int_{-\infty}^{\infty} e\Big(\frac{t^2}{q}\Big)\, dt.$$

La integral que aparecen en ambas sumas es una variante de las *integrales de Fresnel*, que se presentan a continuación:

$$C(x) = \int_0^x \cos\left(t^2\right)\, dt \quad \text{y} \quad S(x) = \int_0^x \operatorname{sen}\left(t^2\right)\, dt.$$

Estas integrales son funciones pares, y su límite cuando x tiende a infinito toma el valor $\sqrt{2\pi}/4$ en ambos casos [22].

Teniendo todo esto en cuenta y expresando el término complejo en su forma trigonométrica, se tiene que

$$\begin{aligned}\int_{-\infty}^{\infty} e\Big(\frac{t^2}{q}\Big)\,dt &= \int_{-\infty}^{\infty} \cos\Big(\frac{t^2}{q}\Big)\,dt + i\int_{-\infty}^{\infty} \operatorname{sen}\Big(\frac{t^2}{q}\Big)\,dt \\ &= \frac{\sqrt{q}}{\sqrt{2\pi}}\left[\int_{-\infty}^{\infty} \cos\left(u^2\right)\,du + i\int_{-\infty}^{\infty} \operatorname{sen}\left(u^2\right)\,du\right] \\ &= \frac{2\sqrt{q}}{\sqrt{2\pi}}\Big[C(\infty)+iS(\infty)\Big] = \sqrt{q}\,(1+i).\end{aligned}$$

Recogiendo todos estos cálculos previos y suponiendo que las series convergen , se puede completar la evaluación de $G(1,q)$.

Teorema 1.1. *Sea $q \in \mathbb{Z}^+$. Entonces*

$$G(1,q) = \begin{cases} (1+i)\sqrt{q} & si\ q \equiv 0 \pmod 4, \\ \sqrt{q} & si\ q \equiv 1 \pmod 4, \\ 0 & si\ q \equiv 2 \pmod 4, \\ i\sqrt{q} & si\ q \equiv 3 \pmod 4. \end{cases}$$

Demostración. Observando la relación entre $G(1,q)$ y F se tiene que

$$\begin{aligned}G(1,q) = F(0) &= \sum_{n\in\mathbb{Z}} f_n = \sum_{n\in\mathbb{Z}} f_{2n} + \sum_{n\in\mathbb{Z}} f_{2n+1} \\ &= \left(1+e\Big(\frac{-q}{4}\Big)\right)\int_{-\infty}^{\infty} e\left(\frac{t^2}{q}\right)\,dt = \left(1+e\Big(\frac{-q}{4}\Big)\right)\sqrt{q}\,(1+i).\end{aligned}$$

Si $q' = q+4$, entonces $e(-q'/4) = e(-q/4+1) = e(-q/4)$. Atendiendo a esta periodicidad y calculando el valor de $e(-q/4)$ para $q = 1,2,3,4$, se obtiene el resultado por casos que aparece en el enunciado del teorema. □

1.3. Lemas

Para finalizar el capítulo, se introducen y demuestran los lemas que se utilizarán para completar la evaluación de las sumas de Gauss en capítulos posteriores.

Lema 1.2. *Sean $a,b \in \mathbb{Z}$ y $q \in \mathbb{Z}^+$ impar, con a y q coprimos. Entonces*

$$G(a,b,q) = e\left(\frac{-\overline{4a}\,b^2}{q}\right) G(a,q)$$

donde $\overline{n}$ indica el inverso multiplicativo módulo q.

Demostración. Para la demostración deben completarse cuadrados módulo q y tener en cuenta la q-periodicidad en n.

$$\begin{aligned} G(a,b,q) &= \sum_{n=0}^{q-1} e\Big(\frac{an^2+bn}{q}\Big) = \sum_{n=0}^{q-1} e\Big(\frac{a(n+\overline{2a}b)^2-\overline{4a}b^2}{q}\Big) \\ &= e\Big(\frac{-\overline{4a}b^2}{q}\Big)\sum_{n=0}^{q-1} e\Big(\frac{an^2}{q}\Big) = e\Big(\frac{-\overline{4a}b^2}{q}\Big)\,G(a,q) \end{aligned}$$ □

Corolario 1.3. $G(1,b,q) = e(-\overline{4}b^2/q)\,G(1,q)$.

Lema 1.4. *Sean $q_1, q_2 \in \mathbb{Z}^+$ coprimos. Entonces se cumple que*

$$G(a,b,q_1q_2) = G(aq_1,b,q_2)\,G(aq_2,b,q_1).$$

Demostración.

$$\begin{aligned} G(aq_1,b,q_2)\,G(aq_2,b,q_1) &= \sum_{n=0}^{q_2-1} e\Big(\frac{q_1an^2+bn}{q_2}\Big)\sum_{m=0}^{q_1-1} e\Big(\frac{q_2am^2+bm}{q_1}\Big) \\ &= \sum_{n=0}^{q_2-1}\sum_{m=0}^{q_1-1} e\Big(\frac{q_1^2an^2+q_1bn+q_2^2am^2+q_2bm}{q_1q_2}\Big) \\ &= \sum_{n=0}^{q_2-1}\sum_{m=0}^{q_1-1} e\Big(\frac{a(q_1n+q_2m)^2+b(q_1n+q_2m)}{q_1q_2}\Big). \end{aligned}$$

Para acabar la demostración, basta ver que q_1m+q_2n recorre los restos módulo q_1q_2 cuando $0 \le n < q_2$ y $0 \le m < q_1$. Considerando el sistema de congruencias siguiente se tiene

$$\begin{cases} x \equiv q_1n+q_2m \pmod{q_1} \\ x \equiv q_1n+q_2m \pmod{q_2} \end{cases} \Rightarrow \begin{cases} x \equiv q_2m \pmod{q_1}, \\ x \equiv q_1n \pmod{q_2}. \end{cases}$$

Como q_1 y q_2 son coprimos se tiene que, por el Teorema Chino del Resto, existe una solución única x para cada par (n,m). Si $0 \le n < q_2$ y $0 \le m < q_1$, se tienen q_1q_2 pares únicos (n,m), por lo que existe un número q_1q_2 de soluciones únicas al sistema y, por tanto, se recorren uno a uno los restos módulo q_1q_2. □

Estos lemas, además de utilizarse en las demostraciones del siguiente capítulo, permiten evaluar ciertas sumas de Gauss de forma sencilla. Por ejemplo, para $a = 30$, $b = 3$ y $q = 77$ se tiene

$$G(30,3,77) = e\Big(\frac{-\overline{4\cdot 30}\cdot 3^2}{77}\Big)\,G(30,77) = e(\alpha)\,G(30\cdot 7,11)\,G(30\cdot 11,7),$$

con $\alpha = -2/77$. Como $30\cdot 7 \equiv 1$ módulo 11, y $30\cdot 11 \equiv 1$ módulo 7, se tiene que

$$G(30,3,77) = e(\alpha)\,G(1,11)\,G(1,7) = e(\alpha)\cdot i\sqrt{11}\cdot i\sqrt{7} = -e(\alpha)\sqrt{77}.$$

CAPÍTULO 2
La ley de reciprocidad cuadrática

En este capítulo se introducen el símbolo de Legendre y una de sus generalizaciones, el símbolo de Jacobi. También se demuestran algunas de sus propiedades, como la ley de reciprocidad cuadrática, haciendo uso de las sumas de Gauss. Estas propiedades permitirán ampliar los resultados del capítulo anterior, obteniendo una fórmula cerrada para la evaluación de las sumas de Gauss con valores de q más generales.

2.1. El símbolo de Legendre

Sea $n \in \mathbb{Z}$ y p primo tal que $p \nmid n$, se define el *símbolo de Legendre* como

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{si } x^2 \equiv n \ (p) \ \text{ tiene solución,} \\ -1 & \text{si } x^2 \equiv n \ (p) \ \text{ no tiene solución,} \end{cases}$$

donde se ha utilizado (p) en lugar de (mód p) para denotar de forma reducida las congruencias. Esta notación se utilizará en el resto del trabajo.

El símbolo de Legendre expresa de forma compacta el concepto de residuo cuadrático. Un entero n se clasifica como *residuo cuadrático módulo p* si existe un entero x tal que $x^2 \equiv n \ (p)$; en caso contrario, n se denomina *no-residuo cuadrático.*

Estos conceptos son los que, eventualmente, permiten obtener la evaluación completa de las sumas de Gauss. El siguiente lema es el primer paso en esta dirección.

Lema 2.1. *Sea* $\left(\frac{q}{p}\right) = -1$ *con* $p > 2$ *primo y* $q \in \mathbb{Z}$, $p \nmid q$. *Entonces, los elementos*

$$q(\pm 1)^2,\ q(\pm 2)^2,\ \ldots,\ q\Big(\pm\frac{p-1}{2}\Big)^2,\ 0,\ (\pm 1)^2,\ (\pm 2)^2,\ \ldots,\ \Big(\pm\frac{p-1}{2}\Big)^2$$

forman todas las clases módulo p sin repeticiones cuando se fija uno de los dos signos.

Demostración. $0, 1^2, \ldots, (\frac{p-1}{2})^2$ son residuos cuadráticos, por lo que al multiplicar por q se convierten en no-residuos, excepto el 0. Se tienen entonces $\frac{p+1}{2}$ residuos

cuadráticos y $\frac{p-1}{2}$ no-residuos cuadráticos distintos[1], formando todas las clases módulo p sin repeticiones. El caso con el símbolo negativo es análogo. □

Este resultado que a primera vista puede parecer alejado de las sumas de Gauss, permite demostrar la siguiente propiedad.

Lema 2.2. *Sean $p > 2$ primo y $q \in \mathbb{Z}$ con $p \nmid q$. Entonces*

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

Demostración. La demostración se divide en dos casos.

Caso I: $\left(\frac{q}{p}\right) = 1$, es decir, $\exists\, x : x^2 \equiv q \ \ (p)$.

$$G(q,p) = \sum_{n=0}^{p-1} e\left(\frac{qn^2}{p}\right) = \sum_{n=0}^{p-1} e\left(\frac{(xn)^2}{p}\right) = \sum_{m=0}^{p-1} e\left(\frac{m^2}{p}\right) = G(1,p),$$

donde en el cambio $xn \mapsto m$ se ha utilizado que, si n recorre los restos módulo p, entonces xn también lo hace por ser p primo.

Caso II: $\left(\frac{q}{p}\right) = -1$. Sea $A_r = \left\{rn^2\right\}_{n=1}^{(p-1)/2}$ y sea $B = A_q \cup A_1 \cup \{0\}$.

$$G(q,p) + G(1,p) = \sum_{n=0}^{p-1} e\Big(\frac{qn^2}{p}\Big) + \sum_{n=0}^{p-1} e\Big(\frac{n^2}{p}\Big) = 2\sum_{k\in B} e\Big(\frac{k}{p}\Big) = 2\sum_{k=0}^{p-1} e\Big(\frac{k}{p}\Big),$$

donde se ha utilizado el lema 2.1 en la última igualdad. Esta expresión vale 0 por ser dos veces la suma de las raíces de la unidad, por lo que $G(q,p) = -G(1,p)$. □

La utilidad de este lema es, entre otros, demostrar la siguiente propiedad del símbolo de Legendre.

Lema 2.3. *El símbolo de Legendre es multiplicativo en su primer argumento. Es decir, dados $n_1, n_2 \in \mathbb{Z}$ y p primo se tiene que*

$$\left(\frac{n_1 n_2}{p}\right) = \left(\frac{n_1}{p}\right)\left(\frac{n_2}{p}\right).$$

Demostración. Basta demostrar que $G(q_1q_2,p) = \left(\frac{q_2}{p}\right) G(q_1,p)$. Para el caso $\left(\frac{q_2}{p}\right) = 1$, la demostración sigue el mismo esquema que el caso I de la demostración del lema 2.2. El caso $\left(\frac{q_2}{p}\right) = -1$ también es similar a la demostración del caso II del lema anterior, evaluando esta vez $G(q_1q_2,p) + G(q_1,p)$ y teniendo en cuenta que el lema 2.1 sigue siendo válido al multiplicar por q_1 cada elemento, tanto si q_1 es un residuo cuadrático como si no. □

[1] Son distintos ya que, suponiendo que existen a, b con $1 \le a < b \le \frac{p-1}{2}$ y $a^2 \equiv b^2 \ \ (p)$, se tiene entonces que $(a+b)(a-b) \equiv 0 \ \ (p)$. Entonces, o bien se tiene la contradicción $a \equiv b \ \ (p)$, o bien $a \equiv -b \equiv p - b$, que se contradice por ser $a \le \frac{p-1}{2} < \frac{p+1}{2} \le p - b$.

2.2. La ley de reciprocidad cuadrática

La *ley de reciprocidad cuadrática* es un resultado sobre congruencias conjeturado por Euler y demostrado por Gauss, que establece la relación entre la solubilidad de $x^2 \equiv p \ (q)$ y la de $x^2 \equiv q \ (p)$ para $p, q > 2$ dos primos distintos. El resultado proporciona una forma de determinar a cuál de los siguientes casos pertenece el par de congruencias:

- Las congruencias son *incoherentes*: una congruencia tiene solución y la otra no.
- Las congruencias son *coherentes*: ambas tienen solución o ambas no la tienen.

La ley de reciprocidad cuadrática relaciona esta clasificación con la paridad de la expresión $(p-1)(q-1)/4$. El siguiente fragmento de código `sagemath` permite realizar una comprobación empírica para los primos en el rango $2 < p < q < 100$.

```
results = []

for p in prime_range(3,100):
  for q in prime_range(p+1,100):
    sol_pq = solve_mod(x^2 == p, q)
    sol_qp = solve_mod(x^2 == q, p)

    is_incoherent = (len(sol_pq) == 0) ^^ (len(sol_qp) == 0)
    is_odd = bool(((p-1) * (q-1) / 4) % 2)
    results.append(is_incoherent == is_odd)

print(all(results))
```

Esta comprobación empírica sugiere que ambas soluciones son coherentes si y solo si $(p-1)(q-1)/4$ es un número par. Esto es lo que propone el siguiente teorema, que se demostrará utilizando las sumas de Gauss.

Teorema 2.4. *Sean $p, q > 2$ dos primos distintos, se cumple que*

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

Demostración. Partiendo de $G(1, pq)$ y utilizando los lemas 1.4 y 2.2 se tiene que

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

Utilizando el teorema 1.1 y teniendo en cuenta que p y q son primos impares, basta observar que el resultado de $G(1, pq)$ y el de $G(1, q)\,G(1, p)$ coinciden excepto en el caso en el que $p \equiv q \equiv 3 \ (4)$, donde únicamente cambia el signo. De esta forma,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} -1 & \text{si } p \equiv q \equiv 3 \ (4) \\ 1 & \text{en el resto de casos.} \end{cases}$$

Teniendo en cuenta que $(p-1)(q-1)/4$ es impar si y solo si $p \equiv q \equiv 3 \ (4)$, el resultado anterior se puede reescribir de forma más compacta como $(-1)^{(p-1)(q-1)/4}$, obteniendo así la expresión que aparece en el enunciado del teorema. □

Además de la ley de reciprocidad cuadrática, existen las denominadas *leyes suplementarias*, que también pueden ser demostradas utilizando las sumas de Gauss.

Teorema 2.5. *Sea $p > 2$ primo, se cumple que*

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \qquad y \qquad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Demostración. Para demostrar la primera ley suplementaria, se parte de $G(-1,p)$.

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

Teniendo en cuenta que $G(-1,p)$ es el conjugado complejo de $G(1,p)$ y utilizando el teorema 1.1 se tiene

$$\left(\frac{-1}{p}\right) = \frac{G(-1,p)}{G(1,p)} = \frac{|G(1,p)|^2}{G(1,p)} = \begin{cases} \frac{|\sqrt{p}|^2}{\sqrt{p}^2} = 1 & \text{si } p \equiv 1 \ (4), \\ \frac{|i\sqrt{p}|^2}{(i\sqrt{p})^2} = -1 & \text{si } p \equiv 3 \ (4). \end{cases}$$

Para la segunda ley suplementaria, se parte de $G(1,8p)$, se utiliza el lema 1.4 y se evalúa teniendo en cuenta que, por el lema 2.3, $\left(\frac{8}{p}\right) = \left(\frac{2}{p}\right)^3 = \left(\frac{2}{p}\right)$.

$$G(1,8p) = G(8,p)\,G(p,8) = \left(\frac{8}{p}\right) G(1,p)\,G(p,8) = \left(\frac{2}{p}\right) G(1,p)\,G(p,8). \tag{2.1}$$

Como $8p \equiv 0 \ (4)$, entonces $G(1,8p) = (1+i)\sqrt{8p}$. Por otra parte, para evaluar $G(p,8)$ basta considerar los casos $p = 1,3,5,7$, por periodicidad. Para simplificar la notación, los sumatorios de las siguientes ecuaciones tienen como índice $n \in \{0,1,\ldots,7\}$.

$$\begin{aligned} G(1,8) &= (1+i)\sqrt{8}, \\ G(3,8) &= \sum e\big(3n^2/8\big) = \sum e\big(n^2/8\big)\, e^{i\pi/2} = i \cdot G(1,8) = (-1+i)\sqrt{8}, \\ G(5,8) &= \sum e\big(5n^2/8\big) = \sum e\big(-3n^2/8\big) = \overline{G(3,8)} = (-1-i)\sqrt{8}, \\ G(7,8) &= \sum e\big(7n^2/8\big) = \sum e\big(-n^2/8\big) = \overline{G(1,8)} = (1-i)\sqrt{8}. \end{aligned}$$

Despejando $\left(\frac{2}{p}\right)$ en (2.1) y observando la paridad de $(p^2-1)/8$, se obtiene el resultado del enunciado. □

2.3. El símbolo de Jacobi

Hasta el momento, los resultados obtenidos sobre las sumas de Gauss requieren que q sea un número primo. Para poder obtener la evaluación de $G(a,b,q)$ siendo q un número positivo cualquiera, es necesario extender algunas definiciones y resultados a números compuestos.

Sean $n, m \in \mathbb{Z}$ con $m > 2$ impar, se define el *símbolo de Jacobi* como

$$\left(\frac{n}{m}\right) = \prod_{j=1}^{k} \left(\frac{n}{p_j}\right)^{\alpha_j}.$$

Para m no primo, que el símbolo de Jacobi tenga valor 1 no implica la solubilidad de $x^2 \equiv n \ (m)$. Al igual que el símbolo de Legendre, el símbolo de Jacobi también es multiplicativo en su primer argumento.

Corolario 2.6. *El símbolo de Jacobi es multiplicativo en su primer argumento. Es decir, dados $n_1, n_2 \in \mathbb{Z}$ y $m \in \mathbb{Z}^+$ se tiene que*

$$\left(\frac{n_1 n_2}{m}\right) = \left(\frac{n_1}{m}\right)\left(\frac{n_2}{m}\right).$$

Demostración. Se sigue de la definición del símbolo de Jacobi y de la naturaleza multiplicativa del símbolo de Legendre. □

Los símbolos de Jacobi también cumplen la la ley de reciprocidad cuadrática y las leyes suplementarias. A continuación, se demuestra un lema intermedio que se utilizará para extender la ley de reciprocidad cuadrática a los símbolos de Jacobi.

Lema 2.7. *Sean $p, q > 2$ dos primos distintos y $k, l \in \mathbb{Z}^+$, se cumple que*

$$\left(\frac{p^k}{q^l}\right)\left(\frac{q^l}{p^k}\right) = (-1)^{(p^k-1)(q^l-1)/4}.$$

Demostración. Utilizando la definición, la multiplicatividad del símbolo de Jacobi y la ley de reciprocidad cuadrática para el símbolo de Legendre se tiene que

$$\left(\frac{p^k}{q^l}\right)\left(\frac{q^l}{p^k}\right) = \left(\frac{p^k}{q}\right)^l\left(\frac{q^l}{p}\right)^k = \left(\frac{p}{q}\right)^{kl}\left(\frac{q}{p}\right)^{lk} = \left[\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)\right]^{kl} = \left[(-1)^{(p-1)(q-1)/4}\right]^{kl}.$$

Para acabar, se debe comprobar que la paridad de $kl(p-1)(q-1)/4$ coincide con la de $(p^k-1)(q^l-1)/4$. Para ello, se reescribe

$$\frac{(p^k-1)(q^l-1)}{4} = \frac{(p-1)(q-1)S_k T_l}{4} \quad \text{con} \quad S_k = \sum_{j=0}^{k-1} p^j \quad \text{y} \quad T_l = \sum_{j=0}^{l-1} q^l$$

y se observa que $S_k T_l \equiv kl$ módulo 2, quedando demostrado el lema. □

Este lema permite demostrar la ley de reciprocidad cuadrática para los símbolos de Jacobi, es decir, para n y m más generales.

Teorema 2.8. *Sean $n, m \in \mathbb{Z}^+$ dos números impares y coprimos, se cumple que*

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

Demostración. Sea $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ y $m = q_1^{\beta_1} \cdots q_l^{\beta_l}$, entonces

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = \prod_{i=1}^{l}\prod_{j=1}^{k}\left(\frac{p_j^{\alpha_j}}{q_i^{\beta_i}}\right)\prod_{j=1}^{k}\prod_{i=1}^{l}\left(\frac{q_i^{\beta_i}}{p_j^{\alpha_j}}\right) = \prod_{i=1}^{l}\prod_{j=1}^{k}\left(\frac{p_j^{\alpha_j}}{q_i^{\beta_i}}\right)\left(\frac{q_i^{\beta_i}}{p_j^{\alpha_j}}\right).$$

Aplicando el lema 2.7, se tiene

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = \prod_{i=1}^{l}\prod_{j=1}^{k}(-1)^{(p^k-1)(q^l-1)/4} = (-1)^{\frac{1}{4}\sum_{i=1}^{l}\sum_{j=1}^{k}(p^k-1)(q^l-1)}. \tag{2.2}$$

Para simplificar las sumas que aparecen en el exponente, se considera el siguiente desarrollo, donde $a_j = p_j^{\alpha_j}$:

$$n = \prod_{j=1}^{k} a_j = \prod_{j=1}^{k}(a_j - 1 + 1) = \prod_{j=1}^{k}\left(\frac{2(a_j-1)}{2} + 1\right) = \sum_{S\subseteq\{1,2,\ldots,k\}} 2^{|S|}\prod_{j\in S}\frac{(a_j-1)}{2}.$$

Estudiando el comportamiento de este sumatorio módulo 4 y atendiendo a la potencia de 2 que tienen todos los términos, es claro que únicamente sobreviven los sumandos correspondientes a $S = \emptyset$ y $S = \{j\}$, por lo que se tiene

$$n = 1 + \sum_{j=1}^{k}\frac{2(a_j-1)}{2} \mod 4 \quad\Rightarrow\quad n - 1 = \sum_{j=1}^{k}(a_j - 1) = \sum_{j=1}^{k}(p_j^{\alpha_j} - 1) \mod 4.$$

Este comportamiento módulo 4 es el que interesa para evaluar la potencia de la ecuación (2.2). Por lo tanto, sustituyendo en dicha ecuación se tiene

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{1}{4}\sum_{j=1}^{k}(p^k-1)\sum_{i=1}^{l}(q^l-1)} = (-1)^{(n-1)(m-1)/4}. \qquad \square$$

Además de su utilidad en la evaluación de las sumas de Gauss, esta extensión de la ley de reciprocidad cuadrática permite elaborar un algoritmo para determinar la solubilidad de $x^2 \equiv n \ (m)$, que es la base del *criptosistema de Goldwasser-Micali* [23].

Una vez introducido el símbolo de Jacobi y sus propiedades, es posible extender el lema 2.2 para potencias de números primos.

Lema 2.9. *Sean $p > 2$ primo y $q \in \mathbb{Z}$ con $p \nmid q$. Entonces*

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

Demostración.

$$G(q,p^k) = \sum_{n=0}^{p^k-1} e\Big(\frac{qn^2}{p^k}\Big) = \sum_{m=0}^{p-1}\sum_{\ell=0}^{p^{k-1}-1} e\Big(\frac{q(p^{k-1}m+\ell)^2}{p^k}\Big),$$

donde se ha particionado el rango $n = 0, 1, \ldots, p^k - 1$ en bloques de tamaño $p^k - 1$ mediante el cambio $n \mapsto p^{k-1}m + \ell$. Desarrollando la fracción interior se obtiene

$$\frac{q(p^{k-1}m+\ell)^2}{p^k} = \frac{q\left((p^{k-1}m)^2 + 2p^{k-1}m\ell + \ell^2\right)}{p^k} = qp^{k-2}m^2 + \frac{2qm\ell}{p} + \frac{q\ell^2}{p^k}.$$

Por tanto, recuperando la evaluación de $G(q, p^k)$ se tiene

$$G(q,p^k) = \sum_{m=0}^{p-1}\sum_{\ell=0}^{p^{k-1}-1} e\Big(qp^{k-2}m^2 + \frac{2qm\ell}{p} + \frac{q\ell^2}{p^k}\Big) = \sum_{\ell=0}^{p^{k-1}-1} e\Big(\frac{q\ell^2}{p^k}\Big)\sum_{m=0}^{p-1} e\Big(\frac{2qm\ell}{p}\Big).$$

Para evaluar la suma interior, se dividen los casos $p \nmid 2q\ell$ y $p \mid 2q\ell$. Teniendo en cuenta las hipótesis, se observa que las condiciones $p \mid 2q\ell$ y $p \mid \ell$ son equivalentes. Denotando $\ell = pn$ para el primer caso se tiene

$$\sum_{m=0}^{p-1} e\Big(\frac{2qm\ell}{p}\Big) = \begin{cases} \displaystyle\sum_{m=0}^{p-1} e(2qmn) \;=\; \sum_{m=0}^{p-1} 1 \;=\; p & \text{si } p \mid \ell, \\ \displaystyle\sum_{m=0}^{p-1} e(2q\ell/p)^m = \frac{1-e(2q\ell/p)^p}{1-e(2q\ell/p)} = 0 & \text{si } p \nmid \ell. \end{cases}$$

Por tanto,

$$G(q,p^k) = p \sum_{\ell=0,\ p\mid\ell}^{p^{k-1}-1} e\Big(\frac{q\ell^2}{p^k}\Big) = p \sum_{n=0}^{p^{k-2}-1} e\Big(\frac{q(pn)^2}{p^k}\Big) = p \sum_{n=0}^{p^{k-2}-1} e\Big(\frac{qn^2}{p^{k-2}}\Big) = p\,G(q,p^{k-2}).$$

Iterando este resultado y teniendo en cuenta que $p^k \equiv 1 \pmod 4$ y $\left(\frac{q}{p^k}\right) = 1$ cuando k es par, se tiene que

$$G(q,p^k) = p^{k/2}\,G(q,1) = \sqrt{p^k}\cdot 1 = \left(\frac{q}{p^k}\right) G(1,p^k)$$

De igual forma, teniendo en cuenta que $\left(\frac{q}{p^k}\right) = \left(\frac{q}{p}\right)$ cuando k es impar, se concluye que

$$G(q,p^k) = p^{\lfloor k/2\rfloor}\,G(q,p) = p^{(k-1)/2}\left(\frac{q}{p}\right) G(1,p) = \left(\frac{q}{p^k}\right) G(1,p^k). \qquad \square$$

2.4. Evaluación de $G(a,b,q)$

Los conceptos introducidos, junto con los lemas, teoremas y propiedades desarrollados en estos dos primeros capítulos, permiten demostrar el siguiente resultado.

Teorema 2.10. *Sea $q \in \mathbb{Z}^+$ impar, no necesariamente primo. Entonces, se cumple que*

$$G(a,b,q) = i^{(q-1)^2/4}\cdot\sqrt{q}\cdot\left(\frac{a}{q}\right)\cdot e\Big(-\frac{\overline{4a}b^2}{q}\Big),$$

donde $\overline{4a}$ indica el inverso módulo q.

Demostración. Teniendo en cuenta el resultado del lema 1.2 es suficiente demostrar que, bajo las hipótesis del teorema, $G(a,q) = i^{(q-1)^2/4}\sqrt{q}\left(\frac{a}{q}\right)$.

Sea $q = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$. Se define $P_j = \prod_{i=1,i\neq j}^{k} p_i^{\alpha_i}$. Aplicando el lema 1.4 de forma iterativa para desarrollar $G(a,q)$ y utilizando el lema 2.9 se tiene

$$G(a,q) = G(a,p_1^{\alpha_1}\cdots p_k^{\alpha_k}) = \prod_{j=1}^{k} G(aP_j,p_j^{\alpha_j}) = \prod_{j=1}^{k}\left(\frac{aP_j}{p_j^{\alpha_j}}\right) G(1,p_j^{\alpha_j}). \tag{2.3}$$

Para desarrollar el productorio, resulta conveniente separarlo en dos productorios, uno por cada factor. Utilizando el teorema 1.1 para desarrollar el productorio que contiene únicamente sumas de Gauss, se tiene que

$$\prod_{j=1}^{k} G(1, p_j^{\alpha_j}) = \sqrt{q} \cdot i^N,$$

donde N cuenta el número de factores $G(1, p_j^{\alpha_j})$ cuya evaluación contiene i. De manera más formal, $N = \#\{j : p_j^{\alpha_j} \equiv 3 \pmod 4\}$. Teniendo esto en cuenta y observando el comportamiento de $(q-1)^2/4$, se puede reescribir la expresión anterior como

$$\prod_{j=1}^{k} G(1, p_j^{\alpha_j}) = \begin{cases} \sqrt{q} \cdot i^{(q-1)^2/4} & \text{si } N \equiv 0 \text{ o } N \equiv 1 \ (4), \\ \sqrt{q} \cdot i^{(q-1)^2/4} \cdot (-1) & \text{si } N \equiv 2 \text{ o } N \equiv 3 \ (4). \end{cases} \tag{2.4}$$

Para evaluar el resto del productorio de (2.3), se comienza utilizando las propiedades de los símbolos de Jacobi.

$$\prod_{j=1}^{k} \left(\frac{aP_j}{p_j^{\alpha_j}}\right) = \prod_{j=1}^{k} \left(\frac{a}{p_j^{\alpha_j}}\right) \prod_{j=1}^{k} \left(\frac{P_j}{p_j^{\alpha_j}}\right) = \left(\frac{a}{q}\right) \prod_{j=1}^{k} \left(\frac{P_j}{p_j^{\alpha_j}}\right).$$

Desarrollando el productorio de esta expresión,

$$\begin{aligned} \prod_{j=1}^{k} \left(\frac{P_j}{p_j^{\alpha_j}}\right) &= \prod_{j=1}^{k} \prod_{i=1, i\neq j}^{k} \left(\frac{p_i^{\alpha_i}}{p_j^{\alpha_j}}\right) = \prod_{j=1}^{k} \prod_{i=j+1}^{k} \left(\frac{p_i^{\alpha_i}}{p_j^{\alpha_j}}\right)\left(\frac{p_j^{\alpha_j}}{p_i^{\alpha_i}}\right) \\ &= \prod_{j=1}^{k} \prod_{i=j+1}^{k} (-1)^{(p_i^{\alpha_i}-1)(p_j^{\alpha_j}-1)/4} = (-1)^{\frac{1}{4}\sum_{j=1}^{k}\sum_{i=j+1}^{k}(p_i^{\alpha_i}-1)(p_j^{\alpha_j}-1)} \end{aligned} \tag{2.5}$$

El producto que aparece en la doble suma del exponente se comporta como sigue:

$$(p_i^{\alpha_i} - 1)(p_j^{\alpha_j} - 1) \equiv \begin{cases} 4 \pmod 8, & \text{si } p_i^{\alpha_i} \equiv p_j^{\alpha_j} \equiv 3 \pmod 4, \\ 0 \pmod 8, & \text{en otro caso.} \end{cases}$$

Es decir, el resultado de la expresión (2.5) está determinado por aquellos términos en los que $p_i^{\alpha_i} \equiv p_j^{\alpha_j} \equiv 3 \ (4)$, ya que al dividirlos entre 4 serán impares. El número de pares (i, j) que cumplen esta condición es

$$\binom{N}{2} = \frac{N(N-1)}{2} = \begin{cases} \text{par} & \text{si } N \equiv 0 \text{ o } N \equiv 1 \ (4), \\ \text{impar} & \text{si } N \equiv 2 \text{ o } N \equiv 3 \ (4). \end{cases}$$

Por lo tanto, continuando la evaluación en (2.5),

$$\prod_{j=1}^{k} \left(\frac{P_j}{p_j^{\alpha_j}}\right) = (-1)^{\binom{N}{2}} = \begin{cases} 1 & \text{si } N \equiv 0 \text{ o } N \equiv 1 \ (4), \\ -1 & \text{si } N \equiv 2 \text{ o } N \equiv 3 \ (4). \end{cases} \tag{2.6}$$

Al juntar de nuevo los productorios de (2.4) y (2.6) y observar que ambos tienen signo negativo para los mismos valores de N se concluye que

$$G(a, q) = i^{(q-1)^2/4} \sqrt{q} \left(\frac{a}{q}\right). \qquad \square$$

CAPÍTULO 3
Difracción y efecto Talbot

En este capítulo se utilizan los resultados obtenidos hasta el momento para analizar el comportamiento de la luz al pasar por una red de difracción. En esta situación, aparece el fenómeno conocido como efecto Talbot, que es estudiado haciendo uso de las sumas de Gauss. El capítulo finaliza con un resultado de análisis, que surge como una consecuencia inesperada del estudio realizado sobre la difracción.

3.1. El fenómeno de la difracción

La *difracción* es un fenómeno físico que se produce cuando una onda se encuentra con un obstáculo o atraviesa una abertura, provocando un cambio en su trayectoria y dispersándola. De esta forma, el obstáculo o la abertura se comportan como una nueva fuente emisora de esa onda. En caso de que varios obstáculos o aberturas se encuentren presentes, las diferentes ondas generadas en cada uno de ellos interfieren siguiendo el *principio de superposición de ondas* [2, §7].

La teoría de la difracción parte del *principio de Huygens-Fresnel* [2, §8.2], cuya idea básica es que todo punto de un frente de ondas es a su vez una fuente de ondas esféricas secundarias, que interfieren de forma constructiva entre ellas para dar lugar a la nueva onda en el instante siguiente. Kirchhoff tomó esta idea y la desarrolló hasta alcanzar la *fórmula de difracción de Fresnel-Kirchhoff* [2, §8.3.2, eq. 17], que relaciona la solución de la ecuación de ondas en el interior de una región con los valores en su frontera.

Esta teoría se utiliza a lo largo del capítulo para estudiar el comportamiento de la luz al encontrarse con una *red de difracción*, compuesta por una serie de rendijas de tamaño comparable a su longitud de onda e igualmente espaciadas. A su vez, una pantalla situada a cierta distancia recoge la intensidad de la luz al llegar a la misma, registrando los patrones provocados por las interferencias entre las ondas generadas en cada rendija. La figura 3.1 ilustra el experimento para dos rendijas.

En el modelo matemático utilizado, la red de difracción se ha modelizado como una serie de agujeros 1-periódicos en el eje x, que recibe rayos de luz monocromática

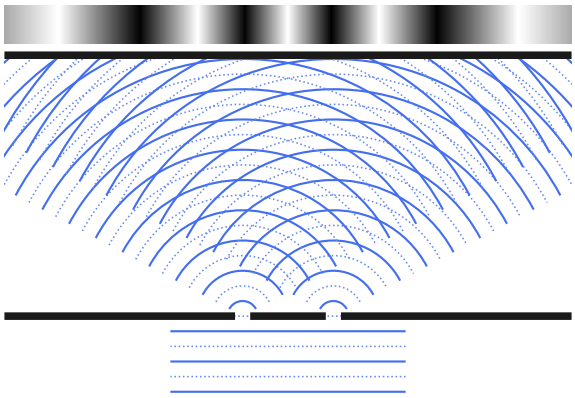

Figura 3.1: Representación simplificada del problema

desde una fuente coherente[2] situada en la parte negativa del eje y. Por otra parte, la pantalla registra la intensidad en cada punto de altura y.

Planteamiento y resolución de la EDP

Se supondrá que la luz utilizada es monocromática, por lo que se modelizará siguiendo la ecuación de una onda de la forma

$$u(x, y, t) = g(x, y)\, e(-kct),$$

donde λ es la *longitud de onda*, $k = \lambda^{-1}$ es el *número de onda* y la constante c es la velocidad de la luz.

La función u deberá, por tanto, cumplir la ecuación de ondas

$$u_{tt} = c^2 u_{xx} + c^2 u_{yy},$$

imponiendo cierta condición de frontera 1-periódica en el eje x, que se corresponde con la entrada de luz a través de la red de difracción. Además, la función g deberá cumplir la condición

$$g(x, y) = A(x, y)\, e(ky),$$

con A_{yy} despreciable. La hipótesis física tras esta restricción es que las soluciones viajen a lo largo de y sin deformarse demasiado en esta dirección. Teniendo en cuenta esta condición y derivando u y g, se tiene que

$$\begin{aligned} u_{tt} = c^2 u_{xx} + c^2 u_{yy} &\Rightarrow (-2\pi ikc)^2 g\, e(-kct) = c^2 (g_{xx} + g_{yy})\, e(-kct) \\ &\Rightarrow -4\pi^2 k^2 g = g_{xx} + g_{yy} \\ &\Rightarrow -4\pi^2 k^2 A\, e(ky) = (A_{xx} + 4\pi ikA_y - 4\pi^2 k^2 A)\, e(ky) \\ &\Rightarrow 0 = A_{xx} + 4\pi ikA_y, \end{aligned}$$

[2]Es decir, los rayos de luz alcanzan la red de difracción en fase, por lo que las ondas se generan al mismo tiempo en cada rendija.

que en términos de g equivale a $g_{xx}+4\pi ikg_y+8\pi^2k^2g=0$. Esta ecuación se denomina *ecuación paraxial*, y transforma el problema original en el siguiente:

$$\begin{cases} g_{xx}+4\pi ikg_y+8\pi^2k^2g=0, \\ g(x,0)=f(x), \end{cases} \tag{3.1}$$

donde la condición de frontera f es una función 1-periódica.

Para resolver el problema se procede utilizando separación de variables:

$$g(x,y)=X(x)\,Y(y) \Rightarrow \begin{cases} X''+\mu X=0, \\ Y'-(\frac{\mu}{4\pi ik}+2\pi ik)\,Y=0. \end{cases}$$

Teniendo en cuenta que la ecuación para X es una EDO lineal homogénea de segundo orden con coeficientes constantes, la solución será de la forma

$$X(x)=Ae^{i\sqrt{\mu}x}, \quad \text{con } A\in\mathbb{C}.$$

Como el problema es invariante por $x\mapsto x+1$, se añade la hipótesis de que X es una función 1-periódica, de donde se deduce que $\sqrt{\mu}=2\pi n$, $n\in\mathbb{Z}$. Por tanto,

$$X(x)=A_n\,e(nx), \quad \text{con } A_n\in\mathbb{C},\ n\in\mathbb{Z}.$$

Por otra parte, como la función Y es una EDO lineal homogénea de primer orden con coeficientes constantes, se tiene que la solución será de la forma

$$Y(y)=B\,e^{(\frac{\mu}{4\pi ik}+2\pi ik)y}, \quad \text{con } B\in\mathbb{C}.$$

Teniendo en cuenta que $\sqrt{\mu}=2\pi n$, $n\in\mathbb{Z}$ y que $\lambda=k^{-1}$ se tiene que

$$Y(y)=B_n\,e\Big(-\frac{\lambda n^2y}{2}\Big)\,e(ky), \quad \text{con } B_n\in\mathbb{C},\ n\in\mathbb{Z}.$$

Por lo tanto, se tiene que

$$X(x)\,Y(y)=C_n\,e\big(nx-\frac{1}{2}\lambda n^2y\big)\,e(ky), \quad \text{con } n\in\mathbb{Z}.$$

La solución de (3.1) vendrá dada por una superposición de los $X(x)\,Y(y)$ para diferentes valores de n.

$$g(x,y)=e(ky)\,F(x,y), \quad \text{con } F(x,y)=\sum_{n=-\infty}^{\infty} c_n\,e\big(nx-\frac{1}{2}\lambda n^2y\big).$$

Atendiendo a la condición inicial $g(x,0)=f(x)$, se observa que los c_n son los coeficientes de Fourier de f.

Cabe destacar que, como los patrones capturados por la pantalla reflejan la intensidad $|g|^2$, bastará con estudiar el comportamiento de $|F|$ para entender dichos patrones.

3.2. El efecto Talbot. Comportamiento fraccionario

Henry Fox Talbot descubrió en el siglo XIX que, al pasar la luz a través de una red de difracción, los patrones luminosos capturados por la pantalla son periódicos con respecto a la distancia a la misma. Concretamente, al situar la pantalla a una distancia específica, y_T, el patrón resultante reproduce la estructura de la red de difracción. Esta distancia es conocida como *distancia de Talbot*, y el efecto se produce también para múltiplos enteros de la misma.

Este efecto es aún más sorprendente cuando se analizan los patrones obtenidos a una fracción de la distancia de Talbot, obteniendo también réplicas de la estructura de la red pero con desplazamientos y cambios de escala. Esto se conoce como *efecto de Talbot fraccionario*, y a menudo se ilustra con la *alfombra de Talbot*.

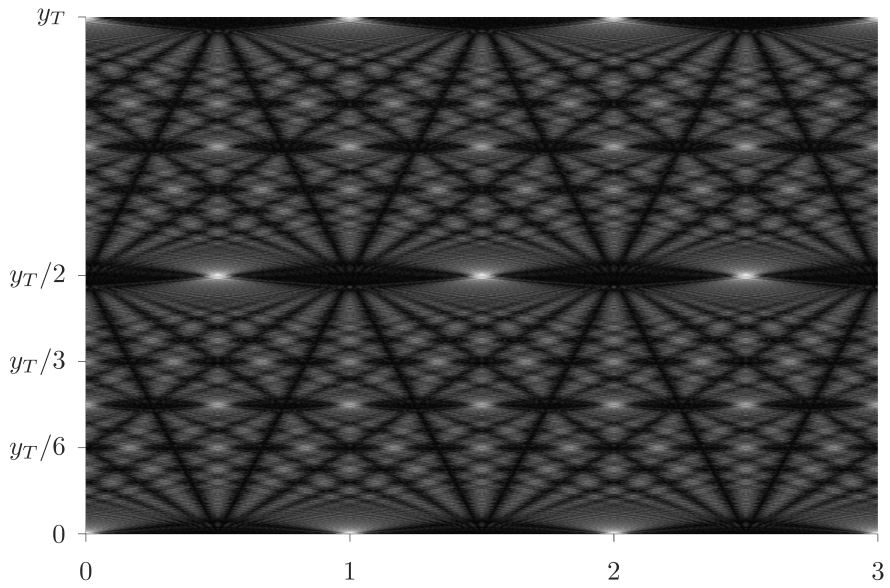

Figura 3.2: Alfombra de Talbot monocromática. En la parte inferior, la luz se difracta al pasar por la red de difracción, y este patrón se replica en la parte superior, a una distancia de Talbot de la red.

Para una red de difracción de periodo a, la distancia de Talbot correspondiente es $y_T = 2a^2/\lambda = 2a^2k$, que efectivamente cumple $F(x, my_T) = f(x)$ para $m \in \mathbb{N}$.

$$F(x, my_T) = \sum_{n=-\infty}^{\infty} c_n\, e\big(nx - \frac{1}{2}\lambda n^2 \cdot 2\lambda^{-1} m\big) = \sum_{n=-\infty}^{\infty} c_n\, e(nx - n^2 m) =$$
$$= \sum_{n=-\infty}^{\infty} c_n\, e(nx) = F(x, 0) = g(x, 0) = f(x).$$

El efecto Talbot fraccionario también se observa al analizar el comportamiento de F en puntos intermedios, como por ejemplo, en el punto medio $y = y_T/2$:

$$F\big(x, \frac{1}{2}y_T\big) = \sum_{n=-\infty}^{\infty} c_n\, e\big(nx - \frac{1}{2}n^2\big) = \sum_{n=-\infty}^{\infty} c_n\, e\big(nx - \frac{1}{2}n\big) = f\big(x - \frac{1}{2}\big).$$

Es decir, a media distancia de Talbot se replica el patrón inicial con un desfase de medio periodo. Esto se observa claramente en la figura 3.2. Para estudiar en mayor profundidad este efecto y generalizarlo a cualquier punto intermedio, es necesario utilizar las sumas de Gauss.

Lema 3.1. *Sean $a, n \in \mathbb{Z}$, $q \in \mathbb{Z}^+$ con a/q irreducible. Entonces, se cumple que*

$$e\Big(\frac{an^2}{q}\Big) = \frac{1}{q}\sum_{m=0}^{q-1} G(a, -m, q)\, e\Big(\frac{nm}{q}\Big).$$

Demostración. Utilizando la definición de las sumas de Gauss y cambiando de orden los sumatorios se obtiene

$$\frac{1}{q}\sum_{m=0}^{q-1} G(a, -m, q)\, e\Big(\frac{nm}{q}\Big) = \frac{1}{q}\sum_{k=0}^{q-1} e\Big(\frac{ak^2}{q}\Big)\sum_{m=0}^{q-1} e\Big(\frac{m(n-k)}{q}\Big).$$

Razonando de forma análoga al estudio del módulo en (1.2), se concluye que la suma exterior es q-periódica en k, por lo que utilizando el cambio $k \mapsto k + n$ se obtiene

$$\frac{1}{q}\sum_{m=0}^{q-1} G(a, -m, q)\, e\Big(\frac{nm}{q}\Big) = \frac{1}{q}\, e\Big(\frac{an^2}{q}\Big)\sum_{k=0}^{q-1} e\Big(\frac{ak^2 + 2akn}{q}\Big)\sum_{m=0}^{q-1} e\Big(\frac{-mk}{q}\Big).$$

Analizando la suma interior, se observa que esta se anula para cualquier valor de k distinto de 0, donde vale q. Por tanto,

$$\frac{1}{q}\sum_{m=0}^{q-1} G(a, -m, q)\, e\Big(\frac{nm}{q}\Big) = \frac{1}{q}\, e\Big(\frac{an^2}{q}\Big)\Big(e(0)\cdot q\Big) = e\Big(\frac{an^2}{q}\Big). \qquad \square$$

Habiendo demostrado este lema, es fácil obtener una versión general del efecto Talbot fraccionario, que se ha plasmado en el siguiente resultado.

Proposición 3.2. *Sean $a \in \mathbb{Z}$, $q \in \mathbb{Z}^+$ con a/q irreducible. Entonces,*

$$g\Big(x, \frac{a}{q}y_T\Big) = \frac{e(aky_T/q)}{q}\sum_{m=0}^{q-1} G(-a, m, q)\, f\Big(x - \frac{m}{q}\Big).$$

Demostración. Utilizando la propiedad compleja $e(-x) = \overline{e(x)}$ junto con las definiciones de g y F se tiene que

$$g\Big(x, \frac{a}{q}y_T\Big) = e\Big(\frac{aky_T}{q}\Big)\sum_{n=-\infty}^{\infty} c_n e\Big(nx - \frac{an^2}{q}\Big) = e\Big(\frac{aky_T}{q}\Big)\sum_{n=-\infty}^{\infty} c_n e(nx)\,\overline{e\Big(\frac{an^2}{q}\Big)}.$$

Desarrollando esta expresión mediante el lema 3.1, utilizando la propiedad de las sumas de Gauss $\overline{G(a,b,q)} = G(-a,-b,q)$ y recordando las definiciones de f y g se tiene que

$$\begin{aligned} g\Big(x, \frac{a}{q}y_T\Big) &= e\Big(\frac{aky_T}{q}\Big) \sum_{n=-\infty}^{\infty} c_n e(nx) \frac{1}{q} \sum_{m=0}^{q-1} \overline{G(a,-m,q)\, e\Big(\frac{nm}{q}\Big)} \\ &= \frac{e(aky_T/q)}{q} \sum_{m=0}^{q-1} G(-a,m,q) \sum_{n=-\infty}^{\infty} c_n e(nx)\, e\Big(\frac{-nm}{q}\Big) \\ &= \frac{e(aky_T/q)}{q} \sum_{m=0}^{q-1} G(-a,m,q) \sum_{n=-\infty}^{\infty} c_n e\Big(n\big(x - \frac{m}{q}\big)\Big) \\ &= \frac{e(aky_T/q)}{q} \sum_{m=0}^{q-1} G(-a,m,q)\, f\Big(x - \frac{m}{q}\Big) \end{aligned}$$

□

Esta expresión para g, además de ser consistente con el resultado obtenido anteriormente para $a/q = 1/2$, proporciona una expresión finita sencilla para la solución del problema (3.1) en un conjunto denso de valores de y.

Por otra parte, teniendo en cuenta los resultados de los capítulos anteriores, se pueden obtener fórmulas explícitas para puntos intermedios, como $a/q = 1/6$:

$$g\Big(x, \frac{y_T}{6}\Big) = \frac{e(ky_T/6)}{6} \sum_{m=0}^{5} G(-1,m,6)\, f\Big(x - \frac{m}{6}\Big).$$

Desarrollando la suma de Gauss mediante el lema 1.4 y el teorema 2.10 se obtiene

$$g\Big(x, \frac{y_T}{6}\Big) = \frac{i\sqrt{3}}{6}\, e\Big(\frac{ky_T}{6}\Big) \sum_{m=0}^{5} e\Big(-\frac{m^2}{3}\Big)\Big[1 + e\Big(\frac{m-3}{2}\Big)\Big]\, f\Big(x - \frac{m}{6}\Big),$$

que operando se reduce a la siguiente expresión:

$$g\Big(x, \frac{y_T}{6}\Big) = \frac{i\sqrt{3}}{3}\, e\Big(\frac{k^2}{3}\Big)\Big[e\Big(\frac{-1}{3}\Big) f\Big(x - \frac{1}{6}\Big) + f\Big(x - \frac{1}{2}\Big) + e\Big(\frac{-1}{3}\Big) f\Big(x - \frac{5}{6}\Big)\Big].$$

Este es un ejemplo de que la imagen formada en puntos intermedios es una combinación lineal de cambios de escala y desplazamientos de f, la estructura original de la red de difracción.

Por último, el número de puntos brillantes en un intervalo de la pantalla también viene determinado por este resultado. Atendiendo a la expresión de g dada en la proposición 3.2, es claro que los máximos en g están determinados por los máximos en f y por el valor de las sumas de Gauss de cada sumando. Recordando el resultado (1.4) se observa que si q es par, la mitad de los sumandos se anulan, mientras que si q es impar, no se anula ninguno. Como en el intervalo $[0,1)$ la función f presenta un único máximo, g tendrá $q/2$ puntos brillantes en el caso par y q en el caso impar.

3.3. Resultados adicionales

El estudio de la difracción mediante las sumas de Gauss da lugar a otros resultados que, a simple vista, no guardan relación directa con estos temas. Un ejemplo es la siguiente proposición, cuyo enunciado es puramente de análisis.

Proposición 3.3. *Si f es real, 1-periódica y suficientemente regular entonces*

$$\lim_{\substack{q\to\infty\\ q\equiv 1\ (4)}} \frac{1}{\sqrt{q}} \sum_{m=0}^{q-1} \cos\Big(\frac{\pi(q-1)m^2}{2q}\Big) f\Big(x-\frac{m}{q}\Big) = f(x).$$

Demostración. Se parte reescribiendo f como el siguiente límite:

$$f(x) = g(x,0) = \lim_{\substack{q\to\infty\\ q\equiv 1\ (4)}} g\Big(x, \frac{y_T}{q}\Big) = \lim_{\substack{q\to\infty\\ q\equiv 1\ (4)}} \frac{e(ky_T/q)}{q} \sum_{m=0}^{q-1} G(-1,m,q)\, f\Big(x-\frac{m}{q}\Big).$$

Evaluando la suma de Gauss y teniendo en cuenta que $e(ky_T/q) \xrightarrow{q\to\infty} 1$, se tiene

$$f(x) = \lim_{\substack{q\to\infty\\ q\equiv 1\ (4)}} \frac{\sqrt{q}}{q} \sum_{m=0}^{q-1} e\Big(\frac{\overline{4}m^2}{q}\Big) f\Big(x-\frac{m}{q}\Big) = \lim_{\substack{q\to\infty\\ q\equiv 1\ (4)}} \frac{1}{\sqrt{q}} \sum_{m=0}^{q-1} e\Big(\frac{-(q-1)m^2}{4q}\Big) f\Big(x-\frac{m}{q}\Big),$$

donde se ha utilizado que $-\overline{4}\cdot(q-1)/4 \equiv 1\ \ (q)$, por ser $q\equiv 1\ (4)$.

Para acabar, basta tomar partes reales y observar que la exponencial compleja da lugar al coseno del enunciado. □

Un ejemplo numérico de este resultado se puede ver en la figura 3.3. En ella se ha representado la gráfica de $f(x) = e^{\mathrm{sen}(2\pi x)}$, junto con las gráficas de la función que aparece dentro del límite para valores de q crecientes.

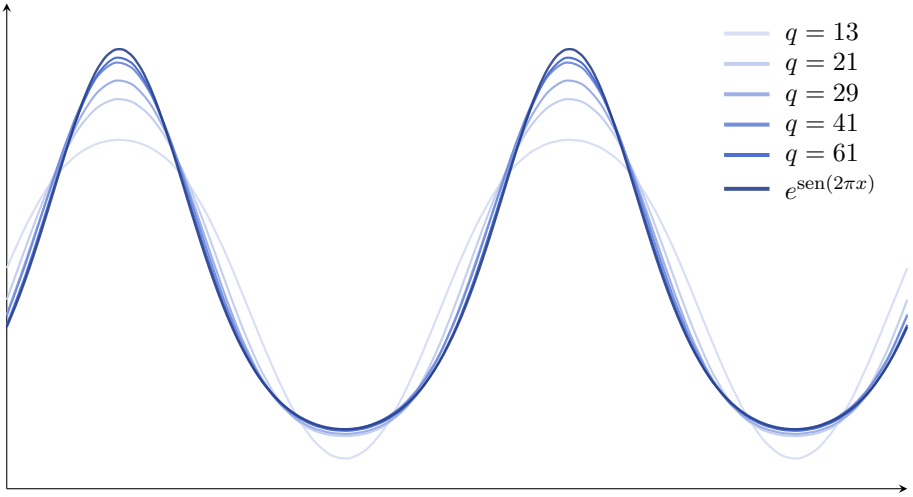

Figura 3.3: Aproximación de $f(x)$ para valores de q crecientes

CAPÍTULO 4
Vórtices en fluidos

En este capítulo se aplican de nuevo los resultados obtenidos sobre sumas de Gauss para estudiar un fenómeno que aparece en mecánica de fluidos: los filamentos de vórtice. Concretamente, se demostrará una conjetura sobre la evolución en el tiempo de uno de estos filamentos, dado un estado inicial particular.

4.1. Filamentos de vórtice. Planteamiento de la conjetura

En mecánica de fluidos, un *filamento de vórtice* es un fenómeno que surge cuando la rotación local de un fluido se concentra a lo largo de una línea o curva delgada, mientras que en el resto del fluido su efecto es prácticamente despreciable. De esta manera, el filamento modela la circulación del fluido y permite simplificar el análisis de fenómenos complejos como anillos de humo o remolinos en líquidos.

El comportamiento de estos filamentos se estudia desde hace más de cien años, comenzando con el trabajo de Da Rios [21], donde se analiza su movimiento y velocidad, además de darse ecuaciones describen su evolución en función del tiempo. Más adelante, Hasimoto [13] relaciona estos filamentos con una ecuación similar a la ecuación paraxial del capítulo anterior, por lo que es razonable pensar en posibles relaciones entre los filamentos de vórtice y las sumas de Gauss.

Siguiendo esta misma dirección, dos investigadores españoles [6] estudiaron la evolución de los filamentos de vórtice que en el instante inicial vienen dados por un polígono regular de M lados y, usando sumas de Gauss, concluyeron que para tiempos dados por múltiplos racionales de $2\pi/M^2$ el filamento se transforma en un nuevo polígono siguiendo la regla:

$$t = \frac{2\pi a}{qM^2} \quad \longrightarrow \quad \begin{array}{l}\text{polígono alabeado de } qM \text{ lados iguales y} \\ \text{ángulo constante } \rho \text{ entre lados contiguos.}\end{array}$$

donde q es impar y a/q es irreducible. En esta expresión, el *polígono alabeado* descrito puede entenderse como un polígono regular cuyos vértices no necesariamente están en el mismo plano.

Aunque no resulta evidente, el ángulo ρ está relacionado con las sumas de Gauss a través de la siguiente fórmula [6, §3]:

$$\sum_{k=0}^{(q-1)/2} T_k \cos^{q-2k}\left(\frac{\rho}{2}\right) \operatorname{sen}^{2k}\left(\frac{\rho}{2}\right) = \cos\frac{\pi}{M}$$

donde $T_0 = 1$ y para $k > 0$

$$T_k = \sum_{\vec{n}\in C_k} \cos\left(\theta_{n_1} - \theta_{n_2} + \ldots + \theta_{n_{2k-1}} - \theta_{n_{2k}}\right)$$

con $C_k = \left\{(n_1, \ldots, n_{2k}) : 0 \le n_1 < \cdots < n_{2k} < q\right\}$ y $e^{i\theta_n} = G(-a, n, q)/\sqrt{q}$.

Los autores del trabajo conjeturaron [6, (25)] que esta expresión tan compleja que define las relaciones que debe cumplir ρ puede simplificarse a la siguiente fórmula:

$$\rho = 2 \arccos\left(\sqrt[q]{\cos(\pi/M)}\right). \tag{4.1}$$

El resto del capítulo se dedicará a demostrar esta conjetura utilizando los conocimientos sobre sumas de Gauss adquiridos en capítulos anteriores.

4.2. Demostración de la conjetura

Para demostrar la conjetura, conviene obtener primero una expresión explícita para los θ_n. Partiendo de la expresión que define las relaciones que deben cumplir, y utilizando el teorema 2.10 se tiene

$$e^{i\theta_n} = \frac{G(-a, n, q)}{\sqrt{q}} = i^{(q-1)^2/4}\left(\frac{-a}{q}\right) e\Big(\frac{\overline{4a}n^2}{q}\Big) = e^{i\pi\left(\frac{(q-1)^2}{8} + \lambda_a + 2\,\frac{\overline{4a}n^2}{q}\right)},$$

con $\lambda_a \in \{0, 1\}$. Tomando logaritmos se obtiene que

$$\theta_n = \pi\Big(\frac{(q-1)^2}{8} + \lambda_a + 2\,\frac{\overline{4a}n^2}{q}\Big) \tag{4.2}$$

y, por tanto, $\theta_n \in \mathbb{R}$. Además, se supondrá que $0 \le \theta_n < 2\pi$, puesto que los θ_n se comportan de forma 2π-periódica en las expresiones en las que aparecen.

Se observa que basta con demostrar que $T_k = 0$ para todo $k \ge 1$, ya que

$$T_k = 0 \;\; \forall k \ge 1 \;\Rightarrow\; \cos^q\left(\frac{\rho}{2}\right) = \cos\left(\frac{\pi}{M}\right) \;\Rightarrow\; (4.1).$$

Además, reescribiendo la expresión de los T_k como $T_k = \Re(E_k)$, bastaría con probar que $\Re(E_k) = 0$. Para poder reescribir T_k de esta forma, E_k debe ser

$$E_k = \sum_{\vec{n}\in C_k} e\left(\frac{1}{2\pi}\left(\theta_{n_1} - \theta_{n_2} + \ldots + \theta_{n_{2k-1}} - \theta_{n_{2k}}\right)\right),$$

que, utilizando la expresión obtenida en (4.2) para los θ_n se transforma en

$$\begin{aligned} E_k &= \sum_{\vec{n}\in C_k} e\left(\frac{\overline{4a}}{q}\left(n_1^2 - n_2^2 + \ldots + n_{2k-1}^2 - n_{2k}^2\right)\right) \\ &= \sum_{\vec{n}\in C_k} e\left(\frac{b}{q}\left(n_1^2 - n_2^2 + \ldots + n_{2k-1}^2 - n_{2k}^2\right)\right), \end{aligned}$$

donde $b = \overline{4a}$ y, por tanto, b/q es irreducible.

Para demostrar que $\Re(E_k) = 0$, se verá primero el caso $k = 1$. El siguiente fragmento de código `sagemath` comprueba de forma numérica que esto se cumple para los q impares entre 1 y 100 y para $b \in \{1, 2\}$.

```
def E_k(k, b, q):
    C_k = Combinations(range(q),2*k)
    summands = []
    for n in C_k:
        inner_sum = sum([(-1)**j * n[j]**2 for j in range(2*k)])
        summands.append(e**(2 * pi * i * b * inner_sum / q))
    return sum(summands)

for b in [1,2]:
    Ek_list = [real(E_k(1, b, q)) == 0 for q in range(1,100,2)]
    print(f"b = {b}:", all(Ek_list))
```

Una vez visto de forma empírica, se procede con la demostración del caso $k = 1$. Para ello, se consideran los siguientes cambios de variable.

- $(u, v) = (n_2 - n_1, n_2) \Rightarrow (n_1, n_2) = (v - u, v)$

$$\left.\begin{array}{l} 0 \le n_1 = v - u \Rightarrow u \le v \\ n_1 < n_2 \Rightarrow v - u < v \Rightarrow u > 0 \\ n_1^2 - n_2^2 = (v-u)^2 - v^2 = u^2 - 2uv \end{array}\right\} \Rightarrow E_1 = \sum_{u=1}^{q-1}\sum_{v=u}^{q-1} e\Big(\frac{b}{q}(u^2 - 2uv)\Big)$$

- $(u, v) = (q - n_2 + n_1, q - n_2) \Rightarrow (n_1, n_2) = (u - v, q - v)$

$$\left.\begin{array}{l} 0 \le n_1 = u - v \Rightarrow u \ge v \\ n_1 < n_2 \Rightarrow u - v < q - v \Rightarrow u < q \\ n_2 < q \Rightarrow q - v < q \Rightarrow v > 0 \\ n_1^2 - n_2^2 = (u-v)^2 - (q-v)^2 = u^2 - 2uv \end{array}\right\} \Rightarrow E_1 = \sum_{u=1}^{q-1}\sum_{v=1}^{u} e\Big(\frac{b}{q}(u^2 - 2uv)\Big)$$

De esta forma, al sumar ambas expresiones para E_1 y separar la contribución $u = v$, que aparece duplicada, se obtiene

$$\begin{aligned} 2E_1 &= \sum_{u=1}^{q-1}\sum_{v=u}^{q-1} e\Big(\frac{b}{q}(u^2 - 2uv)\Big) + \sum_{u=1}^{q-1}\sum_{v=1}^{u} e\Big(\frac{b}{q}(u^2 - 2uv)\Big) \\ &= \underbrace{\sum_{u=1}^{q-1}\sum_{v=1}^{q-1} e\Big(\frac{b}{q}(u^2 - 2uv)\Big)}_{A} + \underbrace{\sum_{u=1}^{q-1} e\Big(\frac{-bu^2}{q}\Big)}_{B}. \end{aligned} \tag{4.3}$$

Desarrollando A se tiene

$$A = \sum_{u=1}^{q-1} e\Big(\frac{bu^2}{q}\Big) \sum_{v=1}^{q-1} e\Big(\frac{-2buv}{q}\Big) = \sum_{u=1}^{q-1} e\Big(\frac{bu^2}{q}\Big) \left(-1 + \sum_{v=0}^{q-1} e\Big(\frac{-2buv}{q}\Big)\right)$$
$$= -\sum_{u=1}^{q-1} e\Big(\frac{bu^2}{q}\Big) = 1 - \sum_{u=0}^{q-1} e\Big(\frac{bu^2}{q}\Big) = 1 - G(b,q).$$

De igual forma, se obtiene $B = G(-b,q) - 1$. Por tanto, continuando en (4.3) y evaluando las sumas de Gauss que aparecen en la expresión se obtiene

$$E_1 = \frac{1}{2}\Big(G(-b,q) - G(b,q)\Big) = \frac{\sqrt{q}}{2}\, i^{(q-1)^2/4} \left(\frac{b}{q}\right) \Big[(-1)^{(q-1)/2} - 1\Big].$$

Se observa que, si $(q-1)/2$ es par, entonces $E_1 = 0$. Si por el contrario es impar, se tiene que $E_1 = -i\sqrt{q}\Big(\frac{b}{q}\Big)$. Por tanto, en todos los casos se tiene que $\Re(E_1) = 0$.

El argumento utilizado para $k = 1$ no es generalizable a todos los valores de k, por lo que se seguirá otra estrategia. Dado $m \in \mathbb{Z}$ se define la biyección

$$f_m : \big\{0, 1, \ldots, q-1\big\} \;\to\; \big\{0, 1, \ldots, q-1\big\}, \quad n \;\mapsto\; n + m \mod q.$$

Al aplicar f_m componente a componente sobre un vector $\vec{n} \in C_k$, se obtiene otro vector $f_m(\vec{n}) := (f_m(n_1), \ldots, f_m(n_{2k}))$. Sin embargo, es necesario aplicar una permutación circular que reordene las coordenadas para garantizar que $f_m(\vec{n})$ cumple las restricciones de C_k. Esta permutación, denotada por $\sigma_{m,\vec{n}}$, está determinada de forma única por m y por $\vec{n}$, resultando en una biyección $\sigma_{m,\vec{n}} \circ f_m$ de C_k en sí mismo.

Esto se traduce en que, al aplicar f_m a los n_i de la definición de E_k, únicamente se modifica el signo de la suma alternada de algunos sumandos. Por tanto,

$$E_{k,m} := \sum_{\vec{n}\,\in\, C_k} e\Big(\frac{b}{q}\left(f_m(n_1)^2 - f_m(n_2)^2 + \ldots + f_m(n_{2k-1})^2 - f_m(n_{2k})^2\right)\Big)$$
$$= \sum_{\vec{n}\,\in\, C_k} e\Big(\varepsilon(\sigma_{m,\vec{n}}) \cdot \frac{b}{q}\left(n_1^2 - n_2^2 + \ldots + n_{2k-1}^2 - n_{2k}^2\right)\Big),$$

donde $\varepsilon(\sigma_{m,\vec{n}})$ representa el signo de la permutación $\sigma_{m,\vec{n}}$. Sumando entonces sobre todos los posibles valores de m se tiene

$$\sum_{m=0}^{q-1} E_{k,m} = \sum_{m=0}^{q-1} \sum_{\vec{n}\,\in\, C_k} \cos\Big(\varepsilon(\sigma_{m,\vec{n}}) \cdot \frac{2\pi b}{q}\left(n_1^2 - n_2^2 + \ldots + n_{2k-1}^2 - n_{2k}^2\right)\Big)$$
$$+ \sum_{m=0}^{q-1} \sum_{\vec{n}\,\in\, C_k} i\,\mathrm{sen}\Big(\varepsilon(\sigma_{m,\vec{n}}) \cdot \frac{2\pi b}{q}\left(n_1^2 - n_2^2 + \ldots + n_{2k-1}^2 - n_{2k}^2\right)\Big)$$

que, tras tomar partes reales y utilizar $\cos(-x) = \cos x$, resulta en

$$\Re\Big(\sum_{m=0}^{q-1} E_{k,m}\Big) = \sum_{m=0}^{q-1} \sum_{\vec{n}\,\in\, C_k} \cos\Big(\frac{2\pi b}{q}\left(n_1^2 - n_2^2 + \ldots + n_{2k-1}^2 - n_{2k}^2\right)\Big) = q\,\Re(E_k). \tag{4.4}$$

Por otra parte, utilizando la definición de f_m en la expresión que define los E_k y desarrollando los cuadrados se obtiene

$$\begin{aligned} E_{k,m} &= \sum_{\vec{n}\in C_k} e\Big(\frac{b}{q}\left((n_1+m)^2-(n_2+m)^2+\ldots+(n_{2k-1}+m)^2-(n_{2k}+m)^2\right)\Big) \\ &= \sum_{\vec{n}\in C_k} e\left(\frac{b}{q}\sum_{i=1}^{2k}(-1)^{i+1}\,n_i^2\right) e\left(\frac{2mb}{q}\sum_{i=1}^{2k}(-1)^{i+1}\,n_i\right). \end{aligned}$$

Utilizando esta expresión para los E_k junto con el resultado obtenido en (4.4) se tiene

$$\begin{aligned} q\,\Re(E_k) &= \Re\Big(\sum_{m=0}^{q-1} E_{k,m}\Big) \\ &= \Re\left[\sum_{m=0}^{q-1}\sum_{\vec{n}\in C_k} e\left(\frac{b}{q}\sum_{i=1}^{2k}(-1)^{i+1}\,n_i^2\right) e\left(\frac{2mb}{q}\sum_{i=1}^{2k}(-1)^{i+1}\,n_i\right)\right] \\ &= \Re\left[\sum_{\vec{n}\in C_k} e\left(\frac{b}{q}\sum_{i=1}^{2k}(-1)^{i+1}\,n_i^2\right)\underbrace{\sum_{m=0}^{q-1} e\left(\frac{2mb}{q}\sum_{i=1}^{2k}(-1)^{i+1}\,n_i\right)}_{S_{\vec{n}}}\right]. \end{aligned}$$

Se observa entonces que para demostrar $\Re(E_k)=0$ basta con demostrar $S_{\vec{n}}=0$.

La suma interior que aparece en $S_{\vec{n}}$ es constante para cada $\vec{n}$. Denotando esta suma como $s_{\vec{n}}$, se reescribe $S_{\vec{n}}$ como

$$S_{\vec{n}} = \sum_{m=0}^{q-1} e\left(\frac{2mb}{q}\cdot s_{\vec{n}}\right) = \sum_{m=0}^{q-1} e\left(\frac{2bs_{\vec{n}}}{q}\right)^m.$$

La fracción $s_{\vec{n}}/q$ es irreducible, ya que

$$0 \;>\; s_{\vec{n}} \;>\; n_1+(n_3-n_2)+\ldots+(n_{2k-1}-n_{2k-2})-n_{2k} \;>\; n_1-n_{2k} \;>\; -q.$$

Por tanto, $S_{\vec{n}}$ se anula por ser la suma de las q-raíces de la unidad, demostrando así que $\Re(E_k)=0$ y, por tanto, que la conjetura (4.1) es cierta. □

CAPÍTULO 5
El pozo de potencial expandido

En este último capítulo se estudia el problema de mecánica cuántica conocido como el pozo de potencial infinito, analizando qué ocurre cuando el pozo se expande al desplazar súbitamente una de las fronteras. Concretamente, se demostrará la aparición de zonas de probabilidad nula o constante en ciertos intervalos espaciales, todo ello a partir de los resultados obtenidos sobre las sumas de Gauss.

5.1. Mecánica cuántica en una dimensión

La mecánica cuántica es la rama de la física que estudia el comportamiento de la materia a escala molecular, atómica e incluso menor. La principal propiedad de las partículas a este nivel es que su comportamiento se corresponde con el de una onda, por lo que matemáticamente se modelan mediante la llamada *función de onda* [11]. En este capítulo, la función de onda se estudiará en una única dimensión espacial, por lo que será de la forma $\Psi(x,t)$, siendo $x,t \in \mathbb{R}$ las variables espacial y temporal respectivamente.

A partir de la función de onda se define la *función de densidad*, $|\Psi(x,t)|^2$, que representa la probabilidad de detectar la partícula en la posición x para un tiempo t dado. Al ser una función de densidad, cumple que $\int |\Psi|^2\, dx = 1$.

Un ejemplo de este modelo matemático para el comportamiento de las partículas a escalas cuánticas es el caso del electrón del átomo de hidrógeno no excitado, cuya función de ondas en términos de la distancia r al núcleo es

$$\Psi(r,t) = 2r_0^{-3/2} r\, e^{-r/r_0 - iE_1 t/\hbar}.$$

En esta expresión, intervienen las siguientes constantes:

- la energía del electrón, $E_1 = \frac{1}{2} m_e c^2 \alpha^2 \approx 2{,}18 \cdot 10^{-18} J$
- el radio de Bohr, $r_0 = \frac{\hbar}{m_e c \alpha} \approx 5{,}29 \cdot 10^{-11}\, m$
- la constante de Planck reducida, $\hbar = 1{,}05 \cdot 10^{-34} J \cdot s$

donde m_e es la masa del electrón, α, la constante de estructura fina y c, la velocidad de la luz [11, §6.5]

Efectivamente, se comprueba que el módulo al cuadrado de la función de onda integra uno, puesto que es la función de densidad.

$$\int_0^\infty |\Psi|^2\,dr = \int \left(2r_0^{-3/2} r\, e^{-r/r_0}\right)^2 dr = 4r_0^{-3}\int_0^\infty r^2 e^{-2r/r_0}\,dr$$
$$= 4r_0^{-3}\int_0^\infty u^2 e^{-u}\,du = \frac{1}{2}\,\Gamma(3) = 1,$$

Utilizando esta función de densidad, se puede calcular la probabilidad de detectar el electrón en cierta posición. Por ejemplo, la probabilidad de que sea detectado a una distancia menor que $3r_0$ es

$$P(r \le 3r_0) = \int_0^{3r_0} |\Psi|^2\,dr = \frac{1}{2}\int_0^6 u^2 e^{-u}\,du$$
$$= \frac{1}{2}\big[-u^2e^{-u} - 2ue^{-u} - 2e^{-u}\big]_0^6 = \frac{1}{2}(2 - 50e^{-6}) \approx 0{,}938.$$

5.2. La expansión del pozo de potencial infinito

El *pozo de potencial infinito* es un problema de mecánica cuántica que modela una partícula encerrada en un intervalo $I = [0, a]$ con fronteras de potencial infinito, es decir, infranqueables. De esta forma, la función de onda Ψ solo está definida en I, y toma el valor 0 en sus extremos. A lo largo de este capítulo se estudiará la evolución de este sistema cuando se desplaza súbitamente una de las fronteras, haciendo más grande el intervalo. Este problema se denomina el *pozo de potencial expandido* [1].

La base del sistema es la *ecuación de Schrödinger* [9, §9]

$$i\partial_t \Psi = -\frac{\hbar}{2m}\partial_{xx}\Psi,$$

que regula la función de ondas de una partícula de masa m no sometida a fuerzas. En este sistema, dicha partícula está en su *estado fundamental*[3], y se encuentra encerrada en el intervalo $[0, 1]$ cuando se desplaza el extremo derecho de $x = 1$ a $x = \Lambda > 1$ de forma repentina.

Todo esto permite definir formalmente el problema a estudiar, donde la ecuación de ondas viene determinada por

$$\begin{cases} i\partial_t\Psi = -\frac{\hbar}{2m}\partial_{xx}\Psi & \text{si } 0 < x < \Lambda, \\ \Psi(0,t) = \Psi(\Lambda,t) = 0, \\ \Psi(x,0) = f(x) \end{cases} \qquad \text{con} \quad f(x) = \begin{cases} \sqrt{2}\,\mathrm{sen}(\pi x) & \text{si } 0 \le x \le 1, \\ 0 & \text{si } 1 \le x \le \Lambda. \end{cases}$$

Al igual que en el capítulo 3, el método de separación de variables muestra que la siguiente expresión para Ψ resuelve el problema:

$$\Psi(x,t) = \sum_{n\in\mathbb{Z}} a_n\, e\Big(\frac{nx}{2\Lambda} - \frac{n^2 t}{T}\Big) \qquad \text{con} \quad T = \frac{4m\Lambda^2}{\pi\hbar}, \tag{5.1}$$

[3] Estado más bajo de energía. En este contexto implica $\Psi(x,t) = \sqrt{2}\,\mathrm{sen}(\pi x)e^{-i\pi^2\hbar t/(2m)}$.

donde los a_n son los coeficientes de Fourier de la función g, definida como la extensión 2Λ-periódica de la función que vale $\sqrt{2}\,\mathrm{sen}(\pi x)$ en $[-1,1]$ y se anula en $[-\Lambda,\Lambda]-[-1,1]$. En particular, g es impar y coincide con f en $[0,\Lambda]$. Su desarrollo de Fourier es

$$g(x)=\sum_{n\in\mathbb{Z}} a_n e\Big(\frac{nx}{2\Lambda}\Big) \qquad \text{con} \quad a_n=-a_{-n}.$$

La expresión concreta de los a_n se da en [1, (2.3)], pero no es necesaria para el análisis que se realizará a continuación.

Para verificar que Ψ resuelve el problema, se calculan

$$\partial_t\Psi=\sum_{n\in\mathbb{Z}}\frac{-2n^2a_n\pi i}{T}\,e\Big(\frac{nx}{2\Lambda}-\frac{n^2t}{T}\Big) \quad \text{y} \quad \partial_{xx}\Psi=\sum_{n\in\mathbb{Z}}\frac{-\pi^2n^2a_n}{\Lambda^2}\,e\Big(\frac{nx}{2\Lambda}-\frac{n^2t}{T}\Big)$$

y se comprueba que, al sustituir estas expresiones en la ecuación de Schrödinger y despejar, se obtiene la misma expresión para T que la definida en (5.1). Además, utilizando que $-a_n=a_{-n}$ se verifica que Ψ cumple las condiciones iniciales del problema.

Por último, Ψ debe cumplir la condición $\int_0^\Lambda|\Psi|^2\,dx=1$. Utilizando la identidad de Parseval para desarrollar la integral auxiliar con límites $[-\Lambda,\Lambda]$ se tiene

$$\begin{aligned}\int_{-\Lambda}^{\Lambda}|\Psi(x,t)|^2\,dx&=\sum_{n,m\in\mathbb{Z}}a_n\overline{a_m}\,e\Big(\frac{-(n^2-m^2)t}{T}\Big)\int_{-\Lambda}^{\Lambda}e\Big(\frac{(n-m)x}{2\Lambda}\Big)\,dx\\&=\sum_{n,m\in\mathbb{Z}}a_n\overline{a_m}\,e\Big(\frac{-(n^2-m^2)t}{T}\Big)\cdot(2\Lambda\cdot\delta_{m,n})=2\Lambda\sum_{n,m\in\mathbb{Z}}|a_n|^2.\end{aligned}$$

Se observa que esta integral no depende de t. Por otra parte, la definición en (5.1) permite extender Ψ a $\mathbb{R}$ como una función 2Λ-periódica impar, ya que $-a_n=a_{-n}$. Teniendo todo esto en cuenta se concluye que

$$\int_0^\Lambda|\Psi(x,t)|^2\,dx=\frac12\int_{-\Lambda}^{\Lambda}|\Psi(x,t)|^2\,dx=\frac12\int_{-\Lambda}^{\Lambda}|\Psi(x,0)|^2\,dx=\frac12\int_{-\Lambda}^{\Lambda}|g(x)|^2\,dx=1.$$

Una vez comprobado que Ψ resuelve el problema, resulta interesante obtener una expresión cerrada para su valor en tiempos fraccionarios.

Proposición 5.1. *Sean $a\in\mathbb{Z}$, $q\in\mathbb{Z}^+$ con a/q irreducible. Entonces,*

$$\Psi(x,aT/q)=\frac1q\sum_{m=0}^{q-1}G(-a,m,q)\,g\Big(x-\frac{2\Lambda m}{q}\Big).$$

Demostración. La prueba es análoga a la realizada para la proposición 3.2. □

Esta expresión para Ψ en tiempos fraccionarios permite, entre otros, estudiar la existencia de *zonas prohibidas*, es decir, subintervalos de $[0,\Lambda]$ donde $\Psi=0$, lo que implica una probabilidad nula de detectar la partícula en ellos. La existencia de zonas prohibidas vendrá determinada por el comportamiento de g.

Sea q impar y $1 < q < \Lambda$, se tiene que

$$g\Big(x - \frac{2\Lambda m}{q}\Big) \neq 0 \;\Leftrightarrow\; -1 \leq x - \frac{2\Lambda m}{q} \leq 1 \;\Leftrightarrow\; x \in \Big[\frac{2\Lambda m}{q} \mp 1\Big] =: I_m.$$

Es decir, bajo estas condiciones g se anula si $x \notin I_m$ para ningún m. Como las distancias entre dos intervalos consecutivos es mayor que 0, los intervalos I_m no se solapan. Por ello, existen subintervalos de $[0, \Lambda]$ donde g se anula y, por tanto, Ψ también.

Por lo general, cuando $\Lambda < q$ no existen zonas prohibidas. Sin embargo, en ocasiones surgen intervalos donde la probabilidad es uniforme para tiempos fraccionarios. Un ejemplo de este fenómeno se observa para $\Lambda = 5/2$ y $a/q = 1/3$ en el intervalo $[2/3, 1]$. En este caso, la función de ondas Ψ tiene la siguiente expresión.

$$\Psi\big(x, T/3\big) = \frac{1}{3}\sum_{m=0}^{2} G(-1, m, 3)\, g\Big(x - \frac{5m}{3}\Big).$$

Atendiendo al valor particular de g para cada m, se observa que en el intervalo $[2/3, 1]$ el término correspondiente a $m = 2$ se anula. Por lo tanto, evaluando las sumas de Gauss con el teorema 2.10, desarrollando el módulo al cuadrado y utilizando la identidad $\operatorname{sen}^2 x + \cos^2 x = 1$ se tiene que

$$\begin{aligned}|\Psi(x, T/3)|^2 &= \frac{2}{9}\Big|\, G(-1,0,3)\operatorname{sen}(\pi x) + G(-1,1,3)\operatorname{sen}(\pi x - 5\pi/3)\Big|^2 \\ &= \frac{2}{16}\Big|\Big(\operatorname{sen}(\pi x) + \sqrt{3}\cos(\pi x)\Big) + \Big(\cos(\pi x) - \sqrt{3}\operatorname{sen}(\pi x)\Big)i\,\Big|^2 = \frac{1}{2}\,,\end{aligned}$$

es decir, se verifica que es constante en $[2/3, 1]$.

Para estudiar la aparición de estas zonas de probabilidad constante, es necesario obtener una expresión para la función de densidad cuando $\Lambda < q$.

Proposición 5.2. *Sea q impar y $\Lambda < q$. Definiendo $\beta = q/2\Lambda$, se tiene que*

$$\big|\Psi(x, aT/q)\big|^2 = \frac{2}{q}\,\Big|\sum_{k\in I(x)} e\Big(\frac{\overline{4a}k^2}{q}\Big)\operatorname{sen}(\pi x - \pi\beta^{-1}k)\Big|^2 \quad \textit{con} \quad I(x) = \big[\beta x \mp \beta\big] \cap \mathbb{Z},$$

donde $\overline{4a}$ indica el inverso de $4a$ módulo q y k es una variable entera.

Demostración. Utilizando el teorema 2.10 para evaluar las sumas de Gauss se tiene que

$$\begin{aligned}\big|\Psi(x, aT/q)\big|^2 &= \frac{1}{q^2}\,\Big|\sum_{m=0}^{q-1} G(-a, m, q)\, g(x - \beta^{-1}m)\Big|^2 \\ &= \frac{1}{q}\,\Big|\sum_{m=0}^{q-1} e\Big(\frac{\overline{4a}m^2}{q}\Big)\, g(x - \beta^{-1}m)\Big|^2.\end{aligned}$$

En esta expresión, cada sumando se anula si y solo si lo hace $g(x - \beta^{-1}m)$. Por tanto,

$$g\Big(x - \frac{2\Lambda m}{q}\Big) \neq 0 \quad\Leftrightarrow\quad -1 < x - \beta^{-1}m < 1 \quad\Leftrightarrow\quad (x-1)\beta < m < (x+1)\beta,$$

que se corresponde con los límites definidos para el intervalo $I(x)$. Sustituyendo g por su definición, se obtiene el resultado del enunciado. □

Además de esta expresión para Ψ, el siguiente teorema proporciona ciertas condiciones suficientes para que la función de ondas sea constante en cierto intervalo.

Teorema 5.3. *Sea* $\mathfrak{d} : \mathbb{R} \to [0, 1/2]$ *la función que asigna a cada* x *la distancia de* $x + 1/2$ *al entero más cercano. Sean* $q, 2\Lambda \in \mathbb{Z}_{>1}$ *impares con* $\Lambda < q$ *y sea* $c \in [0, \Lambda]$. *Entonces, se tiene que*

$$q^{-1}\beta c - a\beta^{-1} - \frac{1}{2} \in \mathbb{Z} \quad \Rightarrow \quad \big|\Psi(x, aT/q)\big|^2 \ \text{ es constante en } \ |x - c| \leq \beta^{-1}\,\mathfrak{d}(\beta).$$

Demostración. En primer lugar se debe demostrar que $I(x) = I(c)$ para todo x con $|x - c| \leq \beta^{-1}\,\mathfrak{d}(\beta)$. Para ello, se observa que los extremos de $I(x)$ se mantienen a distancia $\mathfrak{d}(\beta)$ de los extremos de $I(c)$ al variar x cerca de c. Por ejemplo, para el límite izquierdo de $I(x)$, $\beta(x-1)$, se tiene

$$\beta(x-1) = \beta(c-1) + \beta(x-c) \quad \text{con} \quad |\beta(x-c)| \leq \mathfrak{d}(\beta).$$

Por esto, basta comprobar que a distancia $\mathfrak{d}(\beta)$ de los extremos de $I(c)$ no hay enteros, es decir, que $I_1 \cap \mathbb{Z} = I_2 \cap \mathbb{Z} = \emptyset$, con

$$I_1 = \big((c+1)\beta,\ (c+1)\beta + \mathfrak{d}(\beta)\big), \quad I_2 = \big((c-1)\beta - \mathfrak{d}(\beta),\ (c-1)\beta\big).$$

Para el primer intervalo, si $\exists\, n \in I_1 \cap \mathbb{Z}$, entonces

$$(c+1)\beta < n < (c+1)\beta + \mathfrak{d}(\beta) \ \Rightarrow\ 0 < (n - \beta c) - \beta < \mathfrak{d}(\beta). \tag{5.2}$$

Por otra parte, como c cumple las condiciones del teorema se tiene que

$$\begin{aligned} q^{-1}\beta c - a\beta^{-1} - \frac{1}{2} \ \in \mathbb{Z} \ \Rightarrow\ \beta c - aq\beta^{-1} = \beta c - 2a\Lambda \ &\in \ \frac{q}{2} + \mathbb{Z} = \frac{1}{2} + \mathbb{Z} \\ \Rightarrow\ \beta c \ \in \ 2a\Lambda + \frac{1}{2} + \mathbb{Z} = \frac{1}{2} + \mathbb{Z} \ &\Rightarrow \ n - \beta c \ \in \ \frac{1}{2} + \mathbb{Z}, \end{aligned}$$

es decir, $n - \beta c$ es un semientero. Por la definición de $\mathfrak{d}$, cualquier semientero m cumple que $\big|m - \beta\big| \geq \mathfrak{d}(\beta)$, pero esto supone una contradicción con lo obtenido en (5.2), por lo que $I_1 \cap \mathbb{Z} = \emptyset$. El razonamiento para I_2 es análogo, concluyendo así que $I(x) = I(c)$ para todo x con $|x - c| \leq \beta^{-1}\,\mathfrak{d}(\beta)$.

Este resultado y la fórmula de Euler para el seno permiten reescribir el sumatorio de $\big|\Psi(x, aT/q)\big|^2$ en la proposición 5.2 para x en el intervalo del teorema como

$$\frac{S_-\, e^{i\pi x} - S_+\, e^{-i\pi x}}{2i} \quad \text{con} \quad S_\pm = \sum_{k \in I(c)} e\Big(\frac{\overline{4a}k^2}{q} \pm \frac{k}{2\beta}\Big).$$

De esta forma, probar que $S_- = 0$ es suficiente para ver que $\big|\Psi(x, aT/q)\big|^2$ es constante en dicho intervalo[4]. La transformación $k \mapsto 2\beta c - k$ mantiene $I(c)$ invariante, ya que únicamente intercambia los extremos. Por tanto, basta demostrar que

$$2S_- = e\Big(\frac{\overline{4a}k^2}{q} - \frac{k}{2\beta}\Big) + e\Big(\frac{\overline{4a}(2\beta c - k)^2}{q} - \frac{2\beta c - k}{2\beta}\Big) = 0,$$

[4]En caso de demostrar $S_+ = 0$, se obtiene una versión más general del teorema, con probabilidad uniforme para otros intervalos. Lo mismo ocurre al demostrar el teorema para q par, obteniendo también otra versión más general para intervalos ligeramente distintos.

lo cual sólo ocurre si los argumentos de ambas exponenciales difieren en un semientero, es decir, si

$$\frac{\overline{4a}k^2}{q} - \frac{k}{2\beta} - \frac{\overline{4a}(2\beta c - k)^2}{q} + \frac{2\beta c - k}{2\beta} \;\in\; \frac{1}{2} + \mathbb{Z}.$$

Partiendo de la condición principal del teorema se obtiene que $2\beta c = 4a\Lambda + q + 2qN$ para $N \in \mathbb{Z}$, por lo que la expresión equivale a

$$\frac{\overline{4a}k^2}{q} - \frac{k}{2\beta} - \frac{\overline{4a}(4a\Lambda + q + 2qN - k)^2}{q} + \frac{4a\Lambda + q + 2qN - k}{2\beta} \;\in\; \frac{1}{2} + \mathbb{Z},$$

que, tras desarrollar cuadrados y simplificar términos equivale a

$$2\,\frac{\overline{4a}k^2}{q} - \frac{k}{\beta} - 2\,\frac{\overline{4a}(4a\Lambda - k)^2}{q} + \frac{4a\Lambda + q - k}{\beta} \;\in\; 1 + 2\mathbb{Z}.$$

Utilizando $\overline{4a}4a = 1 + nq$ con $n \in \mathbb{Z}$ y la definición de β, esta expresión se reduce a

$$2\Lambda\big(2nk - 4an\Lambda + 1\big) \;\in\; 1 + 2\mathbb{Z}.$$

Como 2Λ es impar por hipótesis y $2nk - 4an\Lambda + 1$ es también impar, se concluye entonces que $S_- = 0$ y, por tanto, que $\big|\Psi(x, aT/q)\big|^2$ es constante en el intervalo del enunciado, $|x - c| \le \beta^{-1}\,\mathfrak{d}(\beta)$. □

Este teorema confirma el comportamiento visto anteriormente, donde Ψ era constante en $[2/3, 1]$ cuando $\Lambda = 5/2$ y $a/q = 1/3$. Para utilizar el teorema, se calcula primero el valor de c:

$$q^{-1}\beta c - a\beta^{-1} - \frac{1}{2} = \frac{6c - 50 - 15}{30} \in \mathbb{Z}.$$

Como $c \in [0, \Lambda]$, se deduce que necesariamente $c = 5/6$. Por lo tanto, $|\Psi(x, T/3)|^2$ será constante en el intervalo

$$\left|x - \frac{5}{6}\right| \le \beta^{-1}\,\mathfrak{d}(\beta) = \frac{5}{3}\,\mathfrak{d}\Big(\frac{3}{5}\Big) = \frac{5}{3}\cdot\frac{1}{10} = \frac{1}{6} \;\;\Rightarrow\;\; \frac{2}{3} \le x \le 1,$$

es decir, el mismo que ya se había obtenido anteriormente.

Bibliografía

[1] C. Aslangul. Surprises in the suddenly-expanded infinite well. *Journal of Physics A: Mathematical and Theoretical*, 41(7):075301, 2008.

[2] M. Born and E. Wolf. *Principles of optics: Electromagnetic theory of propagation, interference and diffraction of light*. Oxford–Paris. Pergamon Press, New York, revised edition, 1965. With contributions by A. B. Bhatia, P. C. Clemmow, D. Gabor, A. R. Stokes, A. M. Taylor, P. A. Wayman and W. L. Wilcock.

[3] F. Chamizo. Matemáticas de la difracción y su interpretación física, 2013. URL: `https://matematicas.uam.es/~fernando.chamizo/physics/files/diffraction.pdf`.

[4] F. Chamizo. Un poco de física cuántica para chicos listos de primero (del grado de física o matemáticas), 2015. URL: `https://matematicas.uam.es/~fernando.chamizo/physics/files/qf.pdf`.

[5] F. Chamizo. La ley de reciprocidad cuadrática. curso de teoría de números, 2022. URL: `https://matematicas.uam.es/~fernando.chamizo/asignaturas/2223tenum/notes/sec1.3.pdf`.

[6] F. de la Hoz and L. Vega. Vortex filament equation for a regular polygon. *Nonlinearity*, 27(12):3031–3057, 2014.

[7] H. Dym and H. P. McKean. *Fourier series and integrals*. Probability and Mathematical Statistics, No. 14. -London. Academic Press, New York, 1972.

[8] L. C. Evans. *Partial differential equations*, volume 19 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition, 2010.

[9] L. D. Faddeev and O. A. Yakubovskiĭ. *Lectures on quantum mechanics for mathematics students*, volume 47 of *Student Mathematical Library*. American Mathematical Society, Providence, RI, 2009.

[10] R. Fitzpatrick. Vortex Lines, Vortex Tubes, and Vortex Filaments, 2016. Online; accessed 12-March-2025. URL: `https://farside.ph.utexas.edu/teaching/336L/Fluidhtml/node61.html`.

[11] A. Galindo and P. Pascual. *Mecánica cuántica*. Alhambra, Madrid, 1978.

[12] J. H. Hannay and M. V. Berry. Quantization of linear maps on a torus-Fresnel diffraction by a periodic grating. *Phys. D*, 1(3):267–290, 1980.

[13] H. Hasimoto. A soliton on a vortex filament. *J. Fluid Mech.*, 51(3):477–485, 1972.

[14] L. K. Hua. *Introduction to number theory*. Springer-Verlag, Berlin-Heidelberg-New York, 1982. Transl. from the Chinese by P. Shiu.

[15] A. Komech and A. Merzon. *Stationary diffraction by wedges*, volume 2249 of *Lecture Notes in Mathematics*. Springer, Cham, 2019. Method of automorphic functions on complex characteristics.

[16] K. Konishi and G. Paffuti. *Quantum Mechanics: A New Introduction*. Oxford Philosophical Monographs. The Clarendon Press, Oxford University Press, Oxford, 2009.

[17] T. W. Körner. *Fourier analysis*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 2022. With a foreword by T. Tao.

[18] N. N. Lebedev. *Special functions and their applications*. Dover Publications, Inc., New York, revised edition, 1972. Revised edition, translated from the Russian and edited by R. A. Silverman, Unabridged and corrected republication.

[19] M. Murty and S. Pathak. Evaluation of the quadratic Gauss sum. *The Mathematics Student*, 86(1-2), 2017.

[20] Newport. Diffraction Grating Physics, 2024. Online; accessed 11-05-2025. URL: `https://www.newport.com/n/diffraction-grating-physics`.

[21] L. S. Da Rios. Sul moto d'un liquido indefinito con un filetto vorticoso di forma qualunque. *Rend. Circ. Mat. Palermo*, 22(1):117–135, 1906. In Italian.

[22] Wikipedia contributors. Fresnel integral — Wikipedia, the free encyclopedia, 2024. Online; accessed 20-October-2024. URL: `https://en.wikipedia.org/w/index.php?title=Fresnel_integral&oldid=1251285841`.

[23] Wikipedia contributors. Goldwasser–Micali cryptosystem — Wikipedia, the free encyclopedia, 2024. Online; accessed 30-November-2024. URL: `https://en.wikipedia.org/w/index.php?title=Goldwasser`.