Treball final de grau

GRAU DE MATEMÀTIQUES

Facultat de Matemàtiques i Informàtica
Universitat de Barcelona

---

# Teorema de Waring

---

Autor: Jaime Madrid Gómez

Director: Dr. Luis Dieulefait
Realitzat a: Departament d'Àlgebra i Geometria

Barcelona, 19 de enero de 2018

# Abstract

In number theory, Waring's problem (1770) asks whether for each natural number $k$ exists an associated positive integer $s(k)$ such that every natural number is the sum of at most $s$ natural numbers to the power of $k$. The statement was proved by Hilbert in 1909.

We present an overview of Hilbert-Waring theorem. First, we introduce the modern notation and find several lower and upper bounds using elementary methods. Next, we offer a proof of the theorem based on Schnirelmann's density. Finally, we summarize the current state of the problem.



# Resumen

En teoría de números, el problema de Waring (1770) cuestiona si para cada número natural $k$ existe un entero positivo asociado $s(k)$ tal que todo número natural es la suma de $s(k)$ o menos potencias $k$-ésimas naturales. Hilbert demostró la veracidad del enunciado en 1909.

El presente trabajo ofrece un estudio del teorema de Hilbert-Waring. Introducimos la notación moderna y encontramos algunas cotas al problema mediante métodos elementales. Después, ofrecemos una demostración del teorema basada en la densidad de Schnirelmann. Finalizamos la memoria revisando el estado actual del problema.

# Agradecimientos

Este trabajo cierra un capítulo en la historia de mi vida. Con él se pone fin a cinco años de estudios, amistades, anécdotas y recuerdos que han terminado por conformar al hombre que ahora soy. No puedo, por ello, dejar sin agradecimiento a todos aquellos que me han apoyado y animado con mis proyectos durante el último lustro. Y, en especial, a mi familia, por hacer toda esta aventura posible.

Asimismo, me gustaría dar las gracias a mi tutor, Luis Dieulefait, por ofrecerme un tema tan rico en matices junto a la libertad de poder explorarlos por mí mismo.

# Índice

**1. Introducción** **1**

1.1. El problema histórico . . . . . 1

1.2. Los números $g(k)$ y $G(k)$ . . . . . 1

1.3. Cotas inferiores del problema . . . . . 2

**2. Casos particulares del problema** **6**

2.1. El teorema de los cuatro cuadrados . . . . . 6

2.2. El teorema de los nueve cubos . . . . . 17

2.3. Sumas de potencias más grandes . . . . . 20

2.4. Antecedentes para la generalización . . . . . 22

**3. El teorema de Hilbert-Waring** **23**

3.1. Densidad de Schnirelmann . . . . . 23

3.2. Demostración del teorema de Hilbert-Waring . . . . . 27

**4. Recorrido histórico y estado actual** **35**

4.1. Métodos elementales . . . . . 35

4.2. El método del círculo y potencias superiores . . . . . 36

4.3. Cotas actuales . . . . . 37

**5. Conclusiones** **39**

# 1. Introducción

## 1.1. El problema histórico

En el año 1770, en sus *Meditationes Algebraicae*, el matemático Edward Waring introduce el siguiente resultado:

*Todo entero positivo es la suma de cuatro cuadrados, nueve cubos, diecinueve potencias cuartas, y así sucesivamente.*

De esta manera, Waring propone la existencia de un número, $s(k)$, tal que cualquier entero positivo es la suma de $s(k)$ potencias $k$-ésimas. Aun así, no ofrece ninguna demostración del resultado, y hubo que esperar hasta 1909 para que Hilbert aportara la primera prueba de la existencia de $s(k)$, conformando el teorema de Hilbert-Waring.

El problema, y sus decenas de variantes, se han convertido en un clásico dentro de la teoría de números, no solo por demostrar la existencia de $s(k)$, sino por calcular también su valor exacto. En este trabajo, fieles a la propuesta original de Waring, estudiaremos el siguiente problema:

**Problema 1.1** (de Waring)**.** Sea $k$ un entero positivo. Buscamos saber si existe un número $s(k)$ tal que, para todo $n > 0$, la ecuación

$$n = x_1^k + x_2^k + \cdots + x_{s(k)}^k \qquad x_i \geqslant 0 \tag{1.1}$$

es resoluble siempre con enteros, $x_i$.

## 1.2. Los números $g(k)$ y $G(k)$

**Definición 1.2.** *Denotamos con $g(k)$ al entero $s(k)$ más pequeño que hace resoluble la ecuación (1.1) para cualquier $n$.*

Según el enunciado original de Waring, tendríamos $g(2) = 4$, $g(3) = 9$, $g(4) = 19$ y, en general, $g(k) < \infty$, como acabaremos demostrando en esta memoria.

Existe otro número muy útil a la hora de estudiar el problema:

**Definición 1.3.** *Denotamos con $G(k)$ al entero $s(k)$ más pequeño que hace resoluble la ecuación (1.1) para cualquier $n$ suficientemente grande.*

Pongamos de ejemplo el caso $k = 3$. Hoy sabemos que todo natural se puede expresar como suma de $g(3) = 9$ cubos o menos. Pero solo hay dos números que precisan tantos cubos: el $23 = 2 \cdot 2^3 + 7 \cdot 1^3$ y el $239 = 2 \cdot 4^3 + 4 \cdot 3^3 + 3 \cdot 1^3$. El resto de naturales se puede escribir como suma de ocho cubos o menos. Además, solo 15 números necesitan ochos cubos en su descomposición, siendo el mayor de ellos el 454. Es decir, cualquier entero por encima de 455 se puede escribir como suma de siete cubos.

Véase, entonces, que $g(k)$ no es siempre el número más representativo del problema. En ciertas ocasiones conviene resolver el problema para *la mayoría de los números*, admitiendo algunas excepciones finitas.

Cabe destacar, además, que $G(k) \leqslant g(k)$ para cualquier valor de $k$.

## 1.3. Cotas inferiores del problema

Los métodos para calcular el valor de $g(k)$ y $G(k)$ se han basado, desde el primer momento, en acotaciones con mayor o menor grado de precisión. Acotar superiormente el valor $g(k)$ resolvería directamente nuestro problema, pero esta resulta ser una tarea sumamente complicada, que debe ser estudiada por separado para cada valor de $k$. Las cotas inferiores, por otro lado, sí que pueden estudiarse para valores genéricos de $k$.

**Teorema 1.4.** *Si $[x]$ representa la parte entera de $x$, entonces*

$$g(k) \geqslant 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2.$$

*Demostración.* Sea $q = \left[\left(\frac{3}{2}\right)^k\right]$ y sea $n = 2^k q - 1$. Observamos que $n < 3^k$, lo que implica que $n$ solo podrá escribirse como suma de potencias $1^k$ y $2^k$. La descomposición con menos términos será

$$n = (q-1)2^k + (2^k - 1)1^k,$$

que requiere $2^k + q - 2$ potencias $k$-ésimas. En conclusión, $g(k) \geqslant 2^k + q - 2$. □

A partir de este resultado, podemos dar algunas cotas inferiores de $g(k)$:

$$g(2) \geqslant 4 \qquad g(3) \geqslant 9 \qquad g(4) \geqslant 19 \qquad g(5) \geqslant 37.$$

El rápido crecimiento de $g(k)$, como sugiere la demostración, se debe a la dificultad de escribir los números pequeños como suma de potencias $k$-ésimas.

**Teorema 1.5.** *Si $k \geqslant 2$, se cumple $G(k) \geqslant k + 1$.*

*Demostración.* Sea $A(N)$ el número de enteros positivos menores que $N$ que se pueden expresar como

$$x_1^k + x_2^k + \cdots + x_k^k, \qquad x_i \geqslant 0. \tag{1.2}$$

Suponemos que los enteros $x_i$ están ordenados de tal manera que

$$0 \leqslant x_1 \leqslant \cdots \leqslant x_k \leqslant \left[N^{\frac{1}{k}}\right].$$

Observamos que $A(N)$ no puede exceder el número de soluciones de este conjunto de desigualdades, es decir,

$$A(N) \leqslant \sum_{x_k=0}^{[N^{1/k}]} \sum_{x_{k-1}=0}^{x_k} \sum_{x_{k-2}=0}^{x_{k-1}} \cdots \sum_{x_1=0}^{x_2} 1,$$

y un método inductivo permite calcular el valor de los sumatorios, $B(N)$.

$$B(N) = \frac{1}{k!} \prod_{n=1}^{k} \left( [N^{1/k}] + n \right).$$

Para grandes valores de $N$, se cumple

$$B(N) \sim \frac{N}{k!} < \frac{2}{3} N,$$

lo que termina por concluir que $A(N) < \frac{2}{3}N$. Este resultado muestra que, para valores grandes de $N$, los $A(N)$ números involucrados en la ecuación (1.2) no pueden incluir todos los enteros menores que $N$. Por tanto,

$$G(k) \geqslant k + 1.$$

□

Podemos mejorar esta última acotación para ciertos valores de $k$, empleando un análisis de los residuos modulares.

**Teorema 1.6.** *Si $m \geqslant 2$, entonces $G(2^m) \geqslant 2^{m+2}$.*

*Demostración.* Sea $k = 2^m$. Para $m \geqslant 2$ tendremos $2^m \geqslant m + 2$.

Si $x$ es par, entonces satisface

$$x^{2^m} \equiv 0 \ (\text{mód } 2^{m+2}).$$

Si $x$ es impar, entonces satisface

$$\begin{aligned} x^{2^m} &= (1+2n)^{2^m} \equiv 1 + 2^{m+1}n + 2^{m+1}(2^m - 1)n^2 \equiv 1 - 2^{m+1}n(n+1) \\ &\equiv 1 \ (\text{mód } 2^{m+2}). \end{aligned}$$

En cualquier caso, $x^{2^m} \equiv 0$ o $1$ (mód $2^{m+2}$), lo que implica que los números de la forma $x \equiv -1$ (mód $2^{m+2}$) necesitan un mínimo de $2^{m+2} - 1$ potencias $k$-ésimas para ser escritos. Pero todavía podemos mejorar la cota.

**Supongamos $m = 2$.** En este caso obtenemos $x^4 \equiv 0$ o $1$ (mód 16), de lo que se deduce que los números de la forma $16n + 15$ requieren al menos 15 bicuadrados para ser escritos. Además, si $16n$ es la suma de 15 bicuadrados o menos, cada uno de ellos debe ser múltiplo de 16. Así pues,

$$16n = \sum_{i=1}^{15} x_i^4 = \sum_{i=1}^{15} (2y_i)^4 \quad \Longrightarrow \quad n = \sum_{i=1}^{15} y_i^4.$$

En síntesis, si $16n$ es suma de 15 o menos bicuadrados, $n$ también lo será. Puesto que 31 no se puede escribir como suma de 15 o menos potencias cuartas, los números de la forma $16^q \cdot 31$ tampoco podrán, para cualquier $q$.

**Supongamos** $m \geqslant 2$**.** Consideremos $n$ un número impar y supongamos que $2^{m+2}n$ es la suma de $2^{2^m}-1$ o menos potencias $k$-ésimas. Cada una de estas potencias debe ser par, debido a los residuos $x^{2^m} \equiv 0$ o 1 (mód $2^{m+2}$), y, en consecuencia, cada una también será divisible por $2^k$. Se deduce entonces que $2^{k-m-2} \mid n$, así que $n$ es par, en contradicción con nuestra suposición inicial.

Por lo tanto, $G(k) \geqslant 2^{m+2}$.

□

**Teorema 1.7.** *Para* $m \geqslant 2$*,* $G(3 \cdot 2^m) \geqslant 2^{m+2}$*.*

*Demostración.* A partir del teorema anterior, advirtiendo que

$$G(3 \cdot 2^m) \geqslant G(2^m) \geqslant 2^{m+2}.$$

□

**Teorema 1.8.** *Si* $p > 2$ *y* $m \geqslant 0$*, entonces* $G\left(p^m(p-1)\right) \geqslant p^{m+1}$*.*

*Demostración.* Sea $k = p^m(p-1)$. Bajo las condiciones del enunciado, tendremos $m+1 \leqslant 3^m < k$. Además, si $p \mid x$,

$$x^k \equiv 0 \text{ (mód } p^{m+1}).$$

Y si $p \nmid x$,

$$x^k = x^{p^m(p-1)} \equiv 1 \text{ (mód } p^{m+1}),$$

según el teorema de Euler-Fermat. Supongamos que $p^{m+1}n$, con $p \nmid n$, es la suma de $p^{m+1}-1$ potencias $k$-ésimas o menos. Entonces cada una de ellas debería ser divisible por $p^{m+1}$, y entonces por $p^k$. Así pues, $p^k \mid p^{m+1}n$, lo que es imposible. Se concluye que $G(k) \geqslant p^{m+1}$. □

**Teorema 1.9.** *Si* $p > 2$ *y* $m \geqslant 0$*, entonces* $G\left(\frac{1}{2}p^m(p-1)\right) \geqslant \frac{1}{2}\left(p^{m+1}-1\right)$*.*

*Demostración.* Se satisface $k = \frac{1}{2}p^m(p-1) \geqslant p^m > m+1$, excepto en el caso trivial $p = 3$, $m = 0$ y $k = 1$. Además, si $p \mid x$,

$$x^k \equiv 0 \text{ (mód } p^{m+1}).$$

Y, si $p \nmid x$, entonces

$$x^{2k} \equiv 1 \text{ (mód } p^{m+1})$$

por el teorema de Euler-Fermat. En este caso, $p^{m+1} \mid (x^{2k}-1)$, es decir,

$$p^{m+1} \mid (x^k-1)(x^k+1).$$

Dado que $p > 2$, $p$ no puede dividir $x^k-1$ y $x^k+1$ a la vez, y solo uno de estos será divisible por $p^{m+1}$. Se deduce que

$$x^k \equiv -1, 0, \text{ o } 1 \text{ (mód } p^{m+1})$$

para cualquier valor de $x$, lo que implica que los números de la forma

$$p^{m+1}n \pm \frac{1}{2}(p^{m+1}-1)$$

requieren al menos $\frac{1}{2}(p^{m+1}-1)$ potencias $k$-ésimas para ser escritos.

□

A modo de conclusión, resumimos las cotas inferiores de $G(k)$ en el siguiente teorema.

**Teorema 1.10.** *$G(k)$ tiene las siguientes cotas inferiores:*

I. $2^{m+2}$, *si $k$ es $2^m$ o $3 \cdot 2^m$ con $m \geqslant 2$.*

II. $p^{m+1}$, *si $k = p^m(p-1)$ con $p > 2$.*

III. $\frac{1}{2}(p^{m+1}-1)$, *si $k = \frac{1}{2}p^m(p-1)$ con $p > 2$.*

IV. $k+1$, *en cualquier caso.*

Estas son las mejores cotas inferiores conocidas para $G(k)$. Puede comprobarse que ninguna de ellas excede $4k$, así que las cotas de $G(k)$ son mucho más pequeñas que las cotas de $g(k)$, para valores grandes de $k$. Esto se debe, como ya habíamos remarcado, a la dificultad de representar números pequeños como potencias $k$-ésimas. Esta dificultad puede obviarse a la hora de calcular $G(k)$, lo que reduce significativamente la cota.

Cerramos la sección con un ejemplo ilustrativo del teorema 1.10. En ocasiones podemos expresar $k$ de maneras distintas dentro del teorema. Por ejemplo,

$$6 = 3^1(3-1) = 7^1 - 1 = \frac{1}{2}(13-1),$$

lo que nos deja con las cotas

$$3^2 = 9, \quad 7^1 = 7, \quad \frac{1}{2}(13-1) = 6, \quad 6+1 = 7.$$

De todas ellas, la más fuerte es la primera, aunque presenta un valor muy por debajo del esperado para $g(6)$.

# 2. Casos particulares del problema

## 2.1. El teorema de los cuatro cuadrados

Nuestra primera aproximación al problema de Waring será estudiar el caso $k = 2$. Los antecedentes se remontan a 1770, año en que Lagrange demuestra el *teorema de los cuatro cuadrados*. En esta memoria ampliaremos el resultado de Lagrange, hasta demostrar que

$$g(2) = G(2) = 4.$$

En primer lugar, introducimos el teorema que da nombre a la sección.

**Teorema 2.1** (Lagrange)**.** *Todo número natural es suma de cuatro cuadrados.*

La demostración que ofrecemos aquí consta de dos partes. Para la primera, basta advertir que:

**Teorema 2.2.** *El producto de dos números expresables como suma de cuatro cuadrados es, también, expresable como suma de cuatro cuadrados.*

*Demostración.* A partir de la identidad de los cuatro cuadrados de Euler,

$$\begin{aligned}&(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^4)\\ &= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2\\ &+ (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2.\end{aligned}$$

□

Con este resultado, la demostración de teorema de Lagrange se reduce a demostrar que todos los números primos admiten una descomposición como suma de cuatro cuadrados. Para ello, introducimos algunos lemas.

**Lema 2.3.** *Sea $p$ un primo impar. Los números $1^2,\ 2^2,\ 3^2,\ ...,\ \left(\frac{1}{2}(p-1)\right)^2$ son todos incongruentes módulo $p$.*

*Demostración.* Si se cumpliera $a^2 \equiv b^2 \pmod{p}$, tendríamos $a \equiv b \pmod{p}$ o bien $a \equiv -b \pmod{p}$. Los números del enunciado no pueden cumplir ninguna de estas relaciones. □

**Lema 2.4.** *Sea $p$ un primo impar. Existen enteros $x$ e $y$ tales que $1+x^2+y^2 = mp$, con $0 < m < p$.*

*Demostración.* En virtud del lema 2.3, los conjuntos $A = \left\{x^2 \mid 0 \leqslant x \leqslant \frac{1}{2}(p-1)\right\}$ y $B = \left\{-1-y^2 \mid 0 \leqslant y \leqslant \frac{1}{2}(p-1)\right\}$ están formados, cada uno, por $\frac{1}{2}(p+1)$ elementos incongruentes entre sí. Puesto que solo hay $p$ restos distintos (mód $p$), existirá una pareja de elementos, $a \in A$ y $b \in B$, congruente módulo $p$. Es decir, existen $x$ e $y$ que cumplen:

$$x^2 \equiv -1 - y^2 \pmod{p} \quad \Longleftrightarrow \quad x^2 + y^2 + 1 = mp.$$

Además, $0 < 1 + x^2 + y^2 < 1 + 2(\frac{1}{2}p)^2 < p^2$, lo que prueba que $0 < m < p$. □

**Teorema 2.5.** *Todo número primo es la suma de cuatro cuadrados.*

*Demostración.* Puesto que $2 = 1^2 + 1^2 + 0^2 + 0^2$, consideraremos $p > 2$.

Del lema 2.4 se deduce que existe un múltiplo de $p$ tal que

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2, \tag{2.1}$$

con $0 < m < p$ y $x_1$, $x_2$, $x_3$, $x_4$ no todos divisibles por $p$. Procedemos a demostrar que el $m$ más pequeño que cumple esta propiedad es $m = 1$.

Sea $m_0 p$ el múltiplo de $p$ más pequeño que satisface (2.1). Si $m_0 = 1$, la demostración está acabada. Consideramos $1 < m_0 < p$.

Si $m_0$ es par, entonces $x_1 + x_2 + x_3 + x_4$ es par. Esto da lugar a tres posibilidades: que todos los $x_i$ sean pares, que todos los $x_i$ sean impares o que haya dos pares y dos impares. En este último caso, podemos suponer que $x_1$ y $x_2$ son pares y que $x_3$ y $x_4$ son impares, sin pérdida de generalidad. Y en cualquiera de los tres casos, $x_1 + x_2$, $x_1 - x_2$, $x_3 + x_4$ y $x_3 - x_4$ son todos pares.

Si tomamos

$$\left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2 = \frac{1}{2} m_0 p,$$

podemos comprobar que $\frac{1}{2} m_0 p$ se puede escribir como suma de cuatro cuadrados, no todos divisibles divisibles por $p$ (ya que $x_1$, $x_2$, $x_3$ y $x_4$ no son todos divisibles por $p$). Como esto contradice nuestra definición de $m_0$, se deduce que $m_0$ debe ser impar.

Observamos que $x_1$, $x_2$, $x_3$ y $x_4$ no son todos divisibles por $m_0$, pues esto implicaría

$$m_0^2 \mid m_0 p \implies m_0 \mid p,$$

lo que es absurdo. Así que $m_0$ es impar, y al menos 3.

Podemos elegir, además, $b_1$, $b_2$, $b_3$ y $b_4$ de tal manera que los enteros

$$y_i = x_i - b_i m_0 \quad (i = 1, 2, 3, 4)$$

satisfagan

$$|y_i| < \frac{1}{2} m_0, \qquad y_1^2 + y_2^2 + y_3^2 + y_4^2 > 0.$$

En ese caso,

$$0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4\left(\frac{1}{2} m_0\right)^2 = m_0^2,$$

y, por la definición de los $y_i$,

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \ (\text{mód } m_0).$$

Tenemos entonces que:

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 + x_4^2 &= m_0 p && (0 < m_0 < p), \\ y_1^2 + y_2^2 + y_3^2 + y_4^2 &= m_1 m_0 && (0 < m_1 < m_0). \end{aligned}$$

Al multiplicar estas últimas expresiones entre sí, con la fórmula introducida en la proposición 2.2, llegamos a $m_0^2 m_1 p = z_1^2 + z_2^2 + z_3^2 + z_4^2$. No obstante,

$$z_1 = \sum x_i y_i = \sum x_i(x_i - b_i m_0) \equiv \sum x_i^2 \equiv 0 \text{ (mód } m_0),$$

y un razonamiento similar permite afirmar que $z_2$, $z_3$ y $z_4$ son todos divisibles por $m_0$. Si escribimos $z_i = m_0 t_i$, con $i = 1, 2, 3, 4$, llegamos a

$$m_1 p = t_1^2 + t_2^2 + t_3^2 + t_4^2.$$

Este resultado contradice la definición de $m_0$, ya que $m_1 < m_0$. En conclusión, la única posibilidad es $m_0 = 1$. □

**Teorema 2.6.** *Se tiene* $g(2) = G(2) = 4$.

*Demostración.* El teorema de Lagrange queda probado con los teoremas 2.2 y 2.5. Podemos afirmar entonces que todo número natural se puede escribir como la suma de cuatro cuadrados o menos, $G(2) \leqslant g(2) \leqslant 4$.

Por otro lado,

$$(2m)^2 \equiv 0 \text{ (mód } 4), \qquad (2m+1)^2 \equiv 1 \text{ (mód } 8),$$

lo que nos deja con $x^2 \equiv 0, 1,$ o $4$ (mód 8). De aquí se deduce que la ecuación $x^2 + y^2 + z^2 \equiv 7$ (mód 8) no tiene soluciones enteras, o lo que es lo mismo, los números de la forma $8m+7$ no se pueden representar como suma de tres cuadrados. En ese caso,

$$G(2) = g(2) = 4.$$

□

En referencia al problema de Waring, los valores de $g(2)$ y $G(2)$ siempre han sido los más estudiados y conocidos. Se han aportado demostraciones muy variadas de su valor, algunas basadas en el método del descenso infinito, otras en la norma de los cuaterniones.

Se podría completar el resultado de Lagrange con el teorema de Legendre (1798), que identifica los números que se pueden escribir como suma de solo tres cuadrados. Y aunque queda fuera del objetivo de este trabajo, sí que ofrece una idea de la atención que ha recibido el caso $k = 2$ a lo largo de la historia.

Cabe destacar, además, que el valor de $g(2)$ coincide con la cota inferior del teorema 1.4. Como veremos, este es un comportamiento habitual: el valor de $g(k)$ coincide con su cota mínima.

### Cuaterniones, otro enfoque al teorema de Lagrange

El resultado de los cuatro cuadrados de Lagrange, expuesto en la sección anterior, podría calificarse de puramente aritmético. No obstante, la suma de cuadrados es un elemento recurrente en muchas ramas de la matemática, desde el teorema de Pitágoras hasta la norma de un número complejo. Por eso no es de extrañar que, aprovechando la estructura de la norma de los cuaterniones, una extensión de los números complejos, podamos dar demostración al teorema de Lagrange desde un planteamiento radicalmente distinto.

**Definición 2.7.** *Se denominan cuaterniones los números de la forma*

$$\alpha = a_0 + a_1 i + a_2 j + a_3 k,$$

*donde $a_0$, $a_1$, $a_2$, $a_3$ son números reales (las coordenadas de $\alpha$) y $i$, $j$, $k$ son elementos característicos del sistema que satisfacen*

$$i^2 = j^2 = k^2 = ijk = -1.$$

A la hora de operar con cuaterniones, se dice que dos de ellos son iguales si sus coordenadas son iguales. Por otro lado, la suma de cuaterniones mantiene las reglas del álgebra habitual, es decir,

$$\begin{aligned}\alpha + \beta &= (a_0 + a_1 i + a_2 j + a_3 k) + (b_0 + b_1 i + b_2 j + b_3 k) \\ &= (a_0 + b_0) + (a_1 + b_1)i + (a_2 + b_2)j + (a_3 + b_3)k.\end{aligned}$$

En cuanto al producto de cuaterniones, podemos decir que es asociativo y distributivo, pero generalmente no conmutativo. A partir de la definición 2.7 se establecen las siguientes expresiones,

$$jk = i = -kj, \qquad ki = j = -ik, \qquad ij = k = -ji.$$

Por tanto, en general,

$$\begin{aligned}\alpha\beta &= (a_0 + a_1 i + a_2 j + a_3 k)(b_0 + b_1 i + b_2 j + b_3 k) \\ &= c_0 + c_1 i + c_2 j + c_3 k,\end{aligned}$$

donde

$$\begin{cases} c_0 = a_0 b_0 - a_1 b_1 - a_2 b_2 - a_3 b_3, \\ c_1 = a_0 b_1 + a_1 b_0 + a_2 b_3 - a_3 b_2, \\ c_2 = a_0 b_2 - a_1 b_3 + a_2 b_0 + a_3 b_1, \\ c_3 = a_0 b_3 + a_1 b_2 - a_2 b_1 + a_3 b_0. \end{cases}$$

Quedan establecidas, por tanto, las expresiones de la suma y el producto de cuaterniones. Por último, cabe destacar el resultado particular

$$(a_0 + a_1 i + a_2 j + a_3 k)(a_0 - a_1 i - a_2 j - a_3 k) = a_0^2 + a_1^2 + a_2^2 + a_3^2,$$

que utilizaremos posteriormente para definir la norma de un cuaternión. En ella se puede observar la estructura cuadrática que impulsa esta demostración.

**Definición 2.8.** *Decimos que un cuaternión $\alpha$ es entero si todas sus coordenadas son enteros o todas sus coordenadas son múltiplos enteros impares de $\frac{1}{2}$ (se dice entonces que tiene coordenadas semienteras).*

Puesto que ahora nos centramos en el estudio de los cuaterniones enteros, de aquí en adelante utilizaremos *cuaternión* o *entero* para referirnos a *cuaternión entero*. Para evitar la ambigüedad, usaremos letras griegas para denotar los cuaterniones, salvo que $a_1 = a_2 = a_3 = 0$ y, entonces, $\alpha = a_0$.

**Definición 2.9.** *El cuaternión $\bar{\alpha} = a_0 - a_1 i - a_2 j - a_3 k$ se denomina el conjugado de $\alpha = a_0 + a_1 i + a_2 j + a_3 k$.*

**Definición 2.10.** *Se define la norma de un cuaternión $\alpha$, $N(\alpha)$, como*

$$N(\alpha) = \alpha\bar{\alpha} = a_0^2 + a_1^2 + a_2^2 + a_3^2.$$

*Diremos que un cuaternión entero es par o impar según si $N(\alpha)$ es par o impar.*

Es fácil comprobar que la norma de un cuaternión entero es un número entero, lo que da sentido a la definición. Además, según las reglas de la multiplicación de cuaterniones, se puede deducir que

$$\overline{\alpha\beta} = \bar{\beta}\bar{\alpha},$$

y, entonces,

$$N(\alpha\beta) = \alpha\beta \cdot \overline{\alpha\beta} = \alpha\beta\bar{\beta}\bar{\alpha} = \alpha \cdot N(\beta) \cdot \bar{\alpha} = \alpha\bar{\alpha} \cdot N(\beta) = N(\alpha)N(\beta)$$

**Definición 2.11.** *Cuando $\alpha \neq 0$ definimos el inverso de $\alpha$ como*

$$\alpha^{-1} = \frac{\bar{\alpha}}{N(\alpha)}.$$

*Se cumple entonces que $\alpha\alpha^{-1} = \alpha^{-1}\alpha = 1$. Si tanto $\alpha$ como $\alpha^{-1}$ son enteros, se dice que $\alpha$ es una unidad, y escribiremos $\alpha = \varepsilon$.*

Dado que $\varepsilon\varepsilon^{-1} = 1$, tendremos que $N(\varepsilon)N(\varepsilon^{-1}) = 1$ y, por tanto, $N(\varepsilon) = 1$. Por otro lado, si $\alpha$ es entero y $N(\alpha) = 1$, entonces $\alpha^{-1} = \bar{\alpha}$ es también entero, así que $\alpha$ es una unidad. Es decir, podríamos haber definido una unidad de manera equivalente como un cuaternión entero con norma 1.

Tomemos ahora una unidad, $\varepsilon$, con $N(\varepsilon) = a_0^2 + a_1^2 + a_2^2 + a_3^2 = 1$. Si cada $a_n$, con $n = 0, 1, 2, 3$, es un entero, se deduce que uno de los $a_n^2$ debe ser 1 y el resto de ellos 0. Si cada $a_n$ es un semientero, se deduce que cada $a_n^2$ debe ser $\frac{1}{4}$. Esto nos deja con 24 posibles unidades:

$$\pm 1, \quad \pm i, \quad \pm j, \quad \pm k, \quad \frac{1}{2}(\pm 1 \pm i \pm j \pm k).$$

Si escribimos

$$\rho = \frac{1}{2}(1 + i + j + k),$$

entonces cualquier cuaternión entero se puede expresar como

$$\alpha = b_0\rho + b_1 i + b_2 j + b_3 k,$$

donde $b_0$, $b_1$, $b_2$ y $b_3$ son enteros; y cualquier cuaternión escrito de esta forma es entero. Además, es fácil ver que la suma de dos cuaterniones enteros es entero y, a partir de las expresiones para el producto de cuaterniones, podemos establecer que

$$\begin{aligned}
\rho^2 &= \frac{1}{2}(-1 + i + j + k) = \rho - 1, \\
\rho i &= \frac{1}{2}(-1 + i + j - k) = -\rho + i + j, \\
i\rho &= \frac{1}{2}(-1 + i - j + k) = -\rho + i + k,
\end{aligned}$$

con expresiones similares de $\rho j$, $j\rho$, etcétera. Como todos estos productos son enteros, podemos concluir que el producto de dos cuaterniones enteros es entero.

**Definición 2.12.** *Si $\varepsilon$ es una unidad, entonces $\alpha\varepsilon$ se denomina asociado de $\alpha$.*

Se deduce rápidamente que los asociados de un cuaternión tienen la misma norma que el original. Además, si $\alpha$ es entero, sus asociados también lo serán.

**Definición 2.13.** *Sea $\gamma = \alpha\beta$. Se dice entonces que $\alpha$ es un divisor de $\gamma$ por la izquierda y que $\beta$ es un divisor por la derecha. Si $\alpha = a_0$ o bien $\beta = b_0$, entonces $\alpha\beta = \beta\alpha$ y la distinción de izquierda o derecha es innecesaria.*

Una vez visto que el producto de cuaterniones enteros es entero, y aclarados los conceptos de unidad y divisor, estamos en condiciones de establecer un algoritmo de división de cuaterniones. Serán necesarios un par de resultados previos.

**Teorema 2.14.** *Si $\alpha$ es un cuaternión entero, entonces al menos uno de sus asociados tiene coordenadas enteras. Si $\alpha$ es impar, entonces al menos uno de sus asociados tiene coordenadas no enteras.*

*Demostración.* Si las coordenadas de $\alpha$ no son enteras, podemos escoger los signos adecuadamente para que

$$\alpha = (b_0 + b_1 i + b_2 j + b_3 k) + \frac{1}{2}(\pm 1 \pm i \pm j \pm k) = \beta + \gamma,$$

donde $b_0$, $b_1$, $b_2$ y $b_3$ son pares. Cualquier asociado de $\beta$ tiene coordenadas enteras y $\gamma\bar{\gamma}$, un asociado de $\gamma$, es 1. Concluimos que $\alpha\bar{\gamma}$, un asociado de $\alpha$, tiene coordenadas enteras.

Si $\alpha$ es impar y tiene coordenadas enteras, entonces

$$\alpha = (b_0 + b_1 i + b_2 j + b_3 k) + (c_0 + c_1 i + c_2 j + c_3 k) = \beta + \gamma,$$

donde $b_0$, $b_1$, $b_2$ y $b_3$ son pares y cada $c_0$, $c_1$, $c_2$, $c_3$ es 0 o 1. Como $N(\alpha)$ es impar, entonces o solo un $c_i$ es 1, o hay tres $c_i$ que son 1. Cualquier asociado de $\beta$ tiene coordenadas enteras, así que basta comprobar que cada uno de los cuaterniones

$$1, \quad i, \quad j, \quad k, \quad 1 + i + j, \quad 1 + i + k, \quad 1 + j + k, \quad i + j + k$$

tiene un asociado con coordenadas no enteras. Esto se puede verificar de manera sencilla. Por ejemplo, si $\gamma = i$, entonces $\rho i$ no tiene coordenadas enteras. Y la demostración es análoga para $j$ y $k$. Si $\gamma = 1 + i + j$, entonces

$$\gamma = 1 + j + k = (1 + i + j + k) - i = \lambda + \mu,$$

y, entonces,

$$\lambda\varepsilon = \lambda \cdot \frac{1}{2}(1 - i - j - k) = 2$$

y las coordenadas de $\mu\varepsilon$ no son enteras. La demostración es análoga para los demás cuaterniones propuestos. □

**Teorema 2.15.** *Si $\kappa$ es un cuaternión entero, y $m$ un entero positivo, entonces existe un cuaternión entero $\lambda$ tal que*

$$N(\kappa - m\lambda) < m^2$$

*Demostración.* El caso $m = 1$ es trivial y podemos suponer $m > 1$. Escribimos

$$\kappa = a_0\rho + a_1 i + a_2 j + a_3 k, \qquad \lambda = b_0\rho + b_1 i + b_2 j + b_3 k,$$

donde $a_n$ y $b_n$, con $n = 0, 1, 2, 3$, son enteros. Las coordenadas de $\kappa - m\lambda$ son

$$\frac{1}{2}(a_0 - mb_0), \qquad \frac{1}{2}\left(a_0 + 2b_1 - m(b_0 + 2b_1)\right),$$
$$\frac{1}{2}\left(a_0 + 2a_2 - m(b_0 + 2b_2)\right), \qquad \frac{1}{2}\left(a_0 + 2a_3 - m(b_0 + 2b_3)\right).$$

Podemos escoger $b_0$, $b_1$, $b_2$ y $b_3$ sucesivamente para que estas coordenadas no excedan $\frac{1}{4}m$, $\frac{1}{2}m$, $\frac{1}{2}m$ y $\frac{1}{2}m$. En ese caso,

$$N(\kappa - m\lambda) \leqslant \frac{1}{16}m^2 + 3 \cdot \frac{1}{4}m^2 < m^2$$

□

**Teorema 2.16.** *Si $\alpha$ y $\beta$ son cuaterniones enteros, y $\beta \neq 0$, entonces existen cuaterniones enteros $\lambda$ y $\gamma$ tales que*

$$\alpha = \lambda\beta + \gamma, \qquad N(\gamma) < N(\beta).$$

*Demostración.* Tomamos $\kappa = \alpha\bar{\beta}$ y $m = \beta\bar{\beta} = N(\beta)$, y determinamos $\lambda$ según el teorema 2.15. Entonces tenemos que

$$(\alpha - \lambda\beta)\bar{\beta} = \kappa - \lambda m = \kappa - m\lambda,$$

y, tomando la norma,

$$N(\alpha - \lambda\beta)N(\bar{\beta}) = N(\kappa - m\lambda) < m^2.$$

En conclusión,

$$N(\gamma) = N(\alpha - \lambda\beta) < m = N(\beta).$$

□

El siguiente paso lógico en el desarrollo de una teoría de divisibilidad será demostrar la existencia y unicidad del máximo común divisor entre dos cuaterniones. Este resultado podrá utilizarse posteriormente para construir un algoritmo de Euclides, en virtud del teorema 2.16. No obstante, hay que matizar que, al carecer de estructura conmutativa, se impone la necesidad de distinguir entre máximo común divisor por la derecha o por la izquierda.

**Definición 2.17.** *Decimos que dos cuaterniones $\alpha$ y $\beta$ tienen un máximo común divisor por la derecha $\delta$ si (i) $\delta$ es un divisor por la derecha de $\alpha$, y (ii) todo divisor por la derecha de $\alpha$ y $\beta$ es divisor por la derecha de $\delta$.*

**Definición 2.18.** *Un conjunto de cuaterniones enteros $S$, con al menos un elemento distinto de 0, se denomina ideal por la derecha si satisface:*

1. *Si $\alpha \in S$ y $\beta \in S$, entonces $\alpha \pm \beta \in S$,*
2. *Si $\alpha \in S$, entonces $\lambda\alpha \in S$ para cualquier cuaternión $\lambda$.*

**Definición 2.19.** *Sea $\delta$ un cuaternión entero. El conjunto $S = (\lambda\delta)$, formado por todos los múltiplos por la izquierda de $\delta$ por cuaterniones enteros $\lambda$, es un ideal derecho. Se denomina ideal principal por la derecha.*

**Teorema 2.20.** *Todo ideal por la derecha es un ideal principal por la derecha.*

*Demostración.* De todos los elementos no nulos de $S$ tomamos uno que tenga la norma mínima, $\delta$. Si $\gamma \in S$ y $N(\gamma) < N(\delta)$, entonces $\gamma = 0$.

Si $\alpha \in S$, entonces $\alpha - \lambda\delta \in S$, para cualquier cuaternión entero $\lambda$, por la definión de ideal por la derecha. Por el teorema 2.16, podemos escoger $\lambda$ tal que $N(\gamma) = N(\alpha - \lambda\delta) < N(\delta)$. En ese caso, $\gamma = 0$ y $\alpha = \lambda\delta$, y $S$ resulta ser el ideal principal por la derecha $(\lambda\delta)$. □

**Teorema 2.21.** *Dos cuaterniones enteros $\alpha$ y $\beta$, no ambos nulos, tienen un máximo común divisor por la derecha $\delta$, que es único excepto por un factor unitario por la izquierda. Además, podemos expresarlo como*

$$\delta = \mu\alpha + \nu\beta, \tag{2.2}$$

*donde $\mu$ y $\nu$ son cuaterniones enteros.*

*Demostración.* El conjunto $S$ de todos los cuaterniones de la forma $\mu\alpha + \nu\beta$ es un ideal por la derecha que, por el teorema 2.20, es un ideal principal por la derecha formado por todos los múltiplos $\lambda\delta$ de un cierto $\delta$. Dado que $\delta \in S$, entonces $\delta$ se puede escribir de la forma (2.2). Además, como $S$ incluye a $\alpha$ y $\beta$, $\delta$ es un divisor por la derecha común a $\alpha$ y $\beta$; y cada divisor común a $\alpha$ y $\beta$ es un divisor por la derecha de cada miembro de $S$, y también de $\delta$. Así pues, $\delta$ es el máximo común divisor por la derecha de $\alpha$ y $\beta$.

Finalmente, si $\delta$ y $\delta'$ satisfacen las condiciones del enunciado, entonces $\delta' = \lambda\delta$ y $\delta = \lambda'\delta'$, donde $\lambda$ y $\lambda'$ son cuaterniones enteros. En ese caso, $\delta = \lambda\lambda'\delta$, así que $\lambda\lambda' = 1$ y $\lambda$ y $\lambda'$ son unidades. □

Si resultara que el máximo común divisor por la derecha $\delta$ es una unidad, $\varepsilon$, entonces cada máximo común divisor por la derecha de $\alpha$ y $\beta$ sería una unidad. En ese caso,

$$\mu'\alpha + \nu'\beta = \varepsilon,$$

para algún $\mu'$ y $\nu'$; y

$$(\varepsilon^{-1}\mu')\alpha + (\varepsilon^{-1}\nu')\beta = 1,$$

así que

$$\mu\alpha + \nu\beta = 1 \tag{2.3}$$

para algunos cuaterniones enteros $\mu$ y $\nu$. En ese caso, escribiríamos

$$(\alpha, \beta)_d = 1. \tag{2.4}$$

Todos los resultados anteriores podrían desarrollarse de manera análoga para obtener una teoría similar con el máximo común divisor por la izquierda. Dicha teoría no es estrictamente necesaria para nuestro objetivo.

Si $\alpha$ y $\beta$ tienen un divisor común por la derecha $\delta$, no una unidad, entonces $N(\alpha)$ y $N(\beta)$ tienen un divisor común $N(\delta) > 1$. Hay un caso importante donde el recíproco también es cierto.

**Teorema 2.22.** *Si $\alpha$ es un cuaternión entero y $\beta = m$ un entero positivo, una condición necesaria y suficiente para que $(\alpha, \beta)_d = 1$ es que $(N(\alpha), N(\beta)) = 1$, o equivalentemente, que $(N(\alpha), m) = 1$.*

*Demostración.* Si tenemos $(\alpha, \beta)_d = 1$, entonces la forma (2.3) es cierta para algún $\mu$ y $\nu$. Así pues,

$$\begin{aligned} N(\mu\alpha) = N(1 - \nu\beta) &= (1 - m\nu)(1 - m\bar{\nu}), \\ N(\mu)N(\alpha) &= 1 - m\nu - m\bar{\nu} + n^2 N(\nu), \end{aligned}$$

y $N(\alpha, m)$ divide cada término de la ecuación salvo al 1. Así pues, $(N(\alpha), m) = 1$. Como $N(\beta) = m^2$, las dos formas de la condición del enunciado son equivalentes. □

**Definición 2.23.** *Un cuaternión entero $\pi$, que no sea una unidad, es primo si sus únicos divisores son las unidades y sus asociados. Es decir, si $\pi = \alpha\beta$, entonces o $\alpha$ o $\beta$ es una unidad.*

A partir de esta definición podemos observar que todos los asociados de un cuaternión primo son primos. Y si $\pi = \alpha\beta$, entonces $N(\pi) = N(\alpha)N(\beta)$, lo que implica que $\pi$ es primo si $N(\pi)$ es un número primo. El recíproco de esta afirmación también es cierto, aunque la demostración es un poco más elaborada. Necesitamos, primero, un resultado previo.

**Teorema 2.24.** *Un número primo no puede ser un cuaternión primo.*

*Demostración.* Puesto que

$$2 = (1 + i)(1 - i),$$

tenemos que 2 no es un cuaternión primo. Podemos suponer, entonces, $p$ impar.

Por el lema 2.4, existen enteros $r$ y $s$ tales que

$$0 < r < p, \quad 0 < s < p, \quad 1 + r^2 + s^2 \equiv 0 \text{ (mód } p).$$

Si consideramos $\alpha = 1 + sj - rk$, entonces

$$N(\alpha) = 1 + r^2 + s^2 \equiv 0 \text{ (mód } p),$$

y se tiene $(N(\alpha), p) > 1$. Se deduce, por el teorema 2.22, que $\alpha$ y $p$ tienen un divisor común por la derecha, $\delta$, que no es una unidad. Si

$$\alpha = \delta_1 \delta, \qquad p = \delta_2 \delta,$$

entonces $\delta_2$ no es una unidad. Si lo fuera, $\delta$ sería un asociado de $p$, y en ese caso $p$ dividiría todas las coordenadas de

$$\alpha = \delta_1 \delta = \delta_1 \delta_2^{-1} p,$$

y, en particular, dividiría a 1. Así pues, $p = \delta_2 \delta$, donde ni $\delta$, ni $\delta_2$ son unidades, así que $p$ no es primo. □

**Teorema 2.25.** *Un cuaternión entero $\pi$ es primo si y solo si $N(\pi)$ es un número primo.*

*Demostración.* Como ya hemos comentado, si $\pi = \alpha\beta$, entonces $N(\pi) = N(\alpha)N(\beta)$, lo que implica que $\pi$ es primo si $N(\pi)$ es un número primo.

Supongamos ahora que $\pi$ es primo y $p$ un número primo divisor de $N(\pi)$. Por el teorema 2.22, $\pi$ y $p$ tienen un divisor común por la derecha, $\pi'$, que no es una unidad. Como $\pi$ es primo, $\pi'$ es un asociado de $\pi$, y $N(\pi') = N(\pi)$. Además, $p = \lambda\pi'$, donde $\lambda$ es entero; y $p^2 = N(\lambda)N(\pi') = N(\lambda)N(\pi)$, así que $N(\lambda)$ es o bien 1, o bien $p$. Si ocurriera $N(\lambda) = 1$, $p$ sería un asociado de $\pi'$ y $\pi$, y también un cuaternión primo, lo que resulta imposible. Así que $N(\pi) = p$, un número primo. □

Aquí finaliza nuestro estudio de la factorización de cuaterniones. Con estos resultados es sencillo demostrar el teorema de Lagrange. La clave, como observamos en el teorema 2.2, residía en demostrar que todo número primo se puede escribir como suma de cuatro cuadrados. Gracias a los cuaterniones, sabemos que si $p$ es un número primo, entonces $p = \lambda\pi$, donde $N(\lambda) = N(\pi) = p$. Si $\pi$ tiene coordenadas enteras $a_0$, $a_1$, $a_2$ y $a_3$, entonces

$$p = N(\pi) = a_0^2 + a_1^2 + a_2^2 + a_3^2.$$

Si $\pi$ no tuviera coordenadas enteras, entonces, por el teorema 2.14, existe un asociado $\pi'$ de $\pi$ que tiene coordenadas enteras. Se llega a la misma conclusión que antes, pues

$$p = N(\pi) = N(\pi').$$

Podríamos continuar desarrollando esta sección hasta obtener un estudio completo de la factorización de cuaterniones. Estos resultados conducen, por ejemplo, a calcular cuántas maneras distintas hay de representar un entero positivo como suma de cuatro cuadrados. También existen algunos ejemplos más inmediatos, como el siguiente.

**Teorema 2.26.** *Si $p$ es un primo impar, entonces $4p$ es la suma de cuatro cuadrados de enteros impares.*

*Demostración.* Tomamos $p$ un primo impar, y escogemos un asociado $\pi'$ de $\pi$ cuyas coordenadas sean semienteros. Un asociado con estas características existe, en virtud del teorema 2.14. Entonces

$$p = N(\pi) = N(\pi') = \left(b_0 + \frac{1}{2}\right)^2 + \left(b_1 + \frac{1}{2}\right)^2 + \left(b_2 + \frac{1}{2}\right)^2 + \left(b_3 + \frac{1}{2}\right)^2,$$

con $b_0$, $b_1$, $b_2$ y $b_3$ enteros, y

$$4p = (2b_0 + 1)^2 + (2b_1 + 1)^2 + (2b_2 + 1)^2 + (2b_3 + 1)^2.$$

□

## 2.2. El teorema de los nueve cubos

La existencia de $G(3)$ y $g(3)$ es más complicada de probar debido, principalmente, a que un cubo también puede ser negativo, hipótesis que no contempla el problema original de Waring. Por ello, los métodos elementales de acotación no ofrecen tan buenos resultados como los de la suma cuadrados. Presentamos, a continuación, algunos resultados.

**Teorema 2.27.** *Se cumple* $G(3) \leqslant 13$.

*Demostración.* Denotamos por $C_s$ un número que es la suma de $s$ cubos no negativos. Consideramos $z \equiv 1 \pmod 6$ y el intervalo

$$I_z = \left\{ n \in \mathbb{N} \mid \phi(z) = 11z^9 + (z^3+1)^3 + 125z^3 \leqslant n \leqslant 14z^9 = \psi(z) \right\}. \tag{2.5}$$

Para valores de $z$ suficientemente grandes, se tiene que $\phi(z+6) < \psi(z)$, así que los intervalos $I_z$ se acaban solapando y todo $n$ suficientemente grande pertenece a algún $I_z$.

El siguiente paso es demostrar que todo $n \in I_z$ se puede expresar como

$$n = N + 8z^9 + 6mz^3\ , \qquad \text{con } N = C_5 \text{ y } 0 < m < z^6.$$

Para ello, definimos $r$, $s$ y $N$ como:

$$\begin{aligned} &n \equiv 6r \pmod{z^3} \qquad (1 \leqslant r \leqslant z^3), \\ &n \equiv s + 4 \pmod 6 \quad (0 \leqslant s \leqslant 5), \\ &N = (r+1)^3 + (r-1)^3 + 2(z^3 - r)^3 + (sz)^3. \end{aligned}$$

De esta manera, $N = C_5$ y

$$0 < N < (z^3+1)^3 + 3z^9 + 125z^3 = \phi(z) - 8z^9 \leqslant n - 8z^9,$$

así que

$$8z^9 < n - N < 14z^9. \tag{2.6}$$

Ahora, podemos observar que

$$N \equiv (r+1)^3 + (r-1)^3 - 2r^3 = 6r \equiv n \equiv n - 8z^9 \pmod{z^3},$$

y dado que $x^3 \equiv x \pmod 6$ para todo $x$, también se cumple

$$\begin{aligned} N &\equiv (r+1) + (r-1) + 2(z^3 - r) + sz = 2z^3 + sz \\ &\equiv (2+s)z \equiv 2 + s \equiv n - 2 \\ &\equiv n - 8 \equiv n - 8z^9 \pmod 6. \end{aligned}$$

A partir de estas expresiones se deduce que $n - N - 8z^9$ es múltiplo de $6z^3$, lo que permite escribir cualquier $n \in I_z$ según la expresión

$$n = N + 8z^9 + 6mz^3,$$

con $N = C_5$ y $0 < m < z^6$, desigualdad que se desprende de (2.6). Además, gracias al teorema de Lagrange, podemos escribir $m = x_1^2 + x_2^2 + x_3^2 + x_4^2$, con $0 \leqslant x_i < z^3$, así que

$$n = N + 8z^9 + 6z^3(x_1^2 + x_2^2 + x_3^2 + x_4^2) = N + \sum_{i=1}^{4} \left[(z^3 + x_i)^3 + (z^3 - x_i)^3\right]$$
$$= C_5 + C_8 = C_{13}.$$

□

La existencia de $g(3)$ se deduce como corolario del teorema anterior. En síntesis, la demostración consiste acotar los números que no pertenecen a ninguno de los intervalos $I_z$.

**Corolario 2.28.** *Si $n \geqslant 10^{25}$, entonces $n = C_{13}$.*

*Demostración.* Comprobamos que los intervalos $I_z$ definidos en (2.5) se solapan si $z \geqslant 373$. Para ello, basta comprobar la veracidad de

$$\phi(z+6) \leqslant \psi(z) \iff 11t^9 + (t^3+1)^3 + 125t^3 \leqslant 14(t-6)^9$$
$$\iff 14\left(1 - \frac{6}{t}\right)^9 \geqslant 12 + \frac{3}{t^3} + \frac{128}{t^6} + \frac{1}{t^9}$$

cuando $t \geqslant 379$. Se puede simplificar la expresión aplicando la desigualdad de Bernoulli,

$$(1-\alpha)^m > 1 - m\alpha, \qquad \text{con } 0 < \alpha < 1.$$

Así pues, si $t > 6$,

$$14\left(1 - \frac{54}{t}\right) \geqslant 12 + \frac{3}{t^3} + \frac{128}{t^6} + \frac{1}{t^9} \iff 2(t - 7\cdot 54) \geqslant \frac{3}{t^2} + \frac{128}{t^5} + \frac{1}{t^8},$$

expresión que es claramente cierta si $t \geqslant 7 \cdot 54 + 1 = 379$.

En conclusión, los intervalos $I_z$ se solapan de $z = 373$ en adelante, y cualquier $n \geqslant 14 \cdot 373^9$ pertenece a alguno de ellos. Esta cota de $n$ es menor que $10^{25}$. □

El camino para acotar $g(3)$ de manera eficiente termina por esclarecer el comportamiento de los enteros menores de $10^{25}$. En realidad, la existencia de $g(3)$ ya está probada, pues todos los menores de $10^{25}$ se pueden escribir como la suma reiterada de $1^3$, lo que arroja un resultado finito para $g(3)$. Podemos, aun así, mejorar bastante la cota.

**Lema 2.29.** *Los números menores que* 40000 *son suma de nueve cubos. En la notación habitual,*

$$n = C_9 \ \ (1 \leqslant n \leqslant 239), \qquad n = C_8 \ \ (240 \leqslant n \leqslant 40000).$$

*Demostración.* Evidencia computacional. De los números menores que 40000, solo 23 y 239 requieren nueve cubos. El resto solo necesita ocho. □

**Teorema 2.30.** *Se tiene* $g(3) \leqslant 13$.

*Demostración.* Si consideramos $N \geqslant 1$ y $m = \left[N^{\frac{1}{3}}\right]$, entonces

$$N - m^3 = \left(N^{\frac{1}{3}}\right)^3 - m^3 \leqslant 3N^{\frac{2}{3}}\left(N^{\frac{1}{3}} - m\right) < 3N^{\frac{2}{3}}.$$

Tomamos ahora $240 \leqslant n \leqslant 10^{25}$, y escribimos $n = 240 + N$, con $0 \leqslant N < 10^{25}$. En ese caso,

$$\begin{array}{lll} N = m^3 + N_1, & m = \left[N^{\frac{1}{3}}\right], & 0 \leqslant N_1 < 3N^{\frac{2}{3}}, \\ N_1 = m_1^3 + N_2, & m_1 = \left[N_1^{\frac{1}{3}}\right], & 0 \leqslant N_2 \leqslant 3N_1^{\frac{2}{3}}, \\ \cdots & \cdots & \cdots \\ N_4 = m_4^3 + N_5, & m_4 = \left[N_4^{\frac{1}{3}}\right], & 0 \leqslant N_5 < 3N_4^{\frac{2}{3}}. \end{array}$$

Con esta descomposición,

$$n = 240 + N = 240 + N_5 + m^3 + m_1^3 + m_2^3 + m_3^3 + m_4^3. \tag{2.7}$$

Además, se da la siguiente cadena de desigualdades.

$$\begin{aligned} 0 \leqslant N_5 \leqslant 3N_4^{\frac{2}{3}} &\leqslant 3\left(3N_3^{\frac{2}{3}}\right)^{\frac{2}{3}} \leqslant \cdots < 3 \cdot 3^{\frac{2}{3}} \cdot 3^{\left(\frac{2}{3}\right)^2} \cdot 3^{\left(\frac{2}{3}\right)^3} \cdot 3^{\left(\frac{2}{3}\right)^4} \cdot N^{\left(\frac{2}{3}\right)^5} \\ &= 27\left(\frac{N}{27}\right)^{\left(\frac{2}{3}\right)^5} < 27\left(\frac{10^{25}}{27}\right)^{\left(\frac{2}{3}\right)^5} < 35000. \end{aligned}$$

Así pues, $240 \leqslant 240 + N_5 < 35240 < 40000$, lo que prueba que $240 + N_5$ es $C_8$. Esto, junto a la ecuación (2.7), demuestra que todos los enteros positivos son suma de trece cubos. □

El valor real de $g(3)$ es 9, resultado que aportó Wieferich en 1909. La prueba es más complicada y precisa del teorema de Legendre, que establece cuándo un número es representable como suma de tres cuadrados. En nuestra demostración utilizamos el teorema de los cuatro cuadrados, lo que nos da una cota más imprecisa. Destacamos, finalmente, que el valor de $g(3)$ coincide con la cota proporcionada en el teorema 1.4.

El valor de $G(3)$ sigue siendo un problema abierto. En 1909, Landau estableció que $G(3) \leqslant 8$, resultado que completó Dickson en 1939, probando que los únicos enteros que requieren nueve cubos son el 23 y el 239. Más tarde se extendió el resultado, demostrando que solo quince enteros necesitan ocho cubos en su descomposición: 15, 22, 50, 114, 167, 175, 186, 212, 231, 238, 303, 364, 420, 428, y 454. A día de hoy, el número más grande que requiere siete cubos es 8042, pero se trata de una evidencia computacional.

Los cálculos por ordenador apuntan hacia $G(3) = 4$ o $G(3) = 5$. A nivel teórico, de $G(3)$ solo tenemos una acotación:

$$4 \leqslant G(3) \leqslant 7.$$

## 2.3. Sumas de potencias más grandes

La generalización del problema de Waring es muy complicada. La demostración de la existencia de $g(k)$ y $G(k)$ requiere un análisis profundo, y el valor exacto de $G(k)$ solo se conoce para 2 y 4.

En este capítulo, daremos algunas acotaciones tradicionales. La mayoría de ellas ofrecen cotas poco precisas, pero mantienen su interés como demostraciones de existencia.

**Teorema 2.31.** *Existe $g(4)$, y no sobrepasa 50.*

*Demostración.* Denotamos por $B_s$ a un número que se puede escribir como suma de $s$ bicuadrados. A partir de la identidad

$$\begin{aligned} 6(a^2+b^2+c^2+d^2)^2 = {} & (a+b)^4+(a-b)^4+(c+d)^4+(c-d)^4 \\ & +(a+c)^4+(a-c)^4+(b+d)^4+(b-d)^4 \\ & +(a+d)^4+(a-d)^4+(b+c)^4+(b-c)^4, \end{aligned}$$

podemos observar que $6(a^2+b^2+c^2+d^2)^2 = B_{12}$. Aplicando el teorema de los cuatro cuadrados de Lagrange, llegamos a que

$$6x^2 = B_{12},$$

para cualquier $x$ natural.

Ahora bien, podemos escribir cualquier entero positivo de la forma

$$n = 6N + r, \qquad \text{con } N \geqslant 0 \quad \text{y} \quad r = 0, 1, 2, 3, 4, \text{ o } 5.$$

A partir del teorema de los cuatro cuadrados, cualquier $n$ positivo se puede escribir como

$$n = 6(x_1^2 + x_2^2 + x_3^2 + x_4^2) + r.$$

Así pues,

$$n = B_{12} + B_{12} + B_{12} + B_{12} + r = B_{48} + r = B_{53},$$

ya que $r$ se puede expresar como mucho con cinco $1^4$ sumados, lo que implica que $g(4)$ existe y vale, como mucho, 53.

Se puede mejorar este resultado observando que cualquier $n \geqslant 81$ se puede expresar como

$$n = 6N + t, \qquad \text{con } N \geqslant 0 \quad \text{y} \quad t = 0, 1, 2, 81, 16, \text{ o } 17.$$

Estos valores de $t$ mantienen las congruencias habituales módulo 6, pero como

$$1 = 1^4, \qquad 2 = 1^4 + 1^4, \qquad 81 = 3^4, \qquad 16 = 2^4, \qquad 17 = 2^4 + 1^4,$$

se concluye que $t = B_2$, lo que nos deja con $n = B_{48} + B_2 = B_{50}$ para cualquier $n \geqslant 81$.

Se puede comprobar que $n = B_{19}$ para cualquier $n \leqslant 80$. De hecho, el único número que precisa 19 bicuadrados es $79 = 4 \cdot 2^4 + 15 \cdot 1^4$. □

Cabe destacar que la acotación de $g(4)$ emplea los resultados conocidos para $g(2)$. Un análisis similar permite deducir la existencia de $g(6)$ y $g(8)$ a partir de las cotas para $g(3)$ y $g(4)$.

**Teorema 2.32.** *$g(6)$ existe, y no excede 2451.*

*Demostración.* El resultado se desprende de la identidad

$$60(a_1^2+a_2^2+a_3^2+a_4^2)^3 = \sum_{i>j>k}(a_i \pm a_j \pm a_k)^6 + 2\sum_{i>j}(a_i \pm a_j)^6 + 36\sum_i a_i^6,$$

donde la parte derecha contiene $16 + 2 \cdot 12 + 36 \cdot 4 = 184$ potencias sextas. Puesto que todo $n$ es de la forma

$$n = 60N + r, \qquad \text{con } N \geqslant 0 \quad \text{y} \quad r = 0, 1, ..., 59,$$

y dado que

$$60N = 60\sum_{i=1}^{g(3)} X_i^3 = 60\sum_{i=1}^{g(3)}(a_i^2+b_i^2+c_i^2+d_i^2)^3,$$

podemos deducir que todo número de la forma $60N$ es la suma de $184g(3)$ potencias sextas. En ese caso, un $n$ cualquiera es la suma de

$$184g(3) + r \leqslant 184g(3) + 59$$

potencias sextas, lo que nos deja con

$$g(6) \leqslant 184g(3)c + 59 \leqslant 2451$$

según la cota de $g(3)$ encontrada en el capítulo anterior, $g(3) \leqslant 13$. □

**Teorema 2.33.** *$g(8)$ existe, y no excede 42273.*

*Demostración.* En la identidad

$$(a_1^2+a_2^2+a_3^2+a_4^2)^4 = 6\sum(a_1 \pm a_2 \pm a_3 \pm a_4)^8 + \sum_{i>j>k}(2a_i \pm a_j \pm a_k)^8$$
$$+ 60\sum_{i>j}(a_i \pm a_j)^8 + 6\sum_i(2a_i)^8,$$

la parte derecha contiene $6 \cdot 8 + 48 + 60 \cdot 12 + 6 \cdot 4 = 840$ potencias octavas. El mismo razonamiento de antes permite decir que cualquier número de la forma $5040N$ es suma de $840g(4)$ potencias octavas. Y puesto que cualquier número menor que 5039 es suma de, como mucho, 273 potencias octavas de 1 y 2 (de hecho, el número que más necesita es $4863 = 18 \cdot 2^8 + 255 \cdot 1^8$), entonces

$$g(8) \leqslant 840g(4) + 273 \leqslant 42273,$$

según las cotas encontradas para $g(4)$. □

Los valores encontrados en este capítulo distan de los valores reales para cada $g(k)$. Hoy sabemos que $g(4) = 19$, $g(6) = 73$ y $g(8) = 279$.

## 2.4. Antecedentes para la generalización

Los métodos aquí recogidos dan idea de la dificultad para generalizar el problema de Waring. El estudio de cada caso se ha realizado atendiendo siempre a propiedades de residuos modulares e identidades que relacionan sumas de potencias. No se desprende ninguna generalización a partir de estas demostraciones.

La existencia de $g(k)$ fue demostrada finalmente por Hilbert en 1909, dándole un enfoque radicalmente distinto al de los métodos elementales. Hasta ese momento, otros ya habían demostrado la existencia de $g(k)$ para los casos $k = 2, 3, 4, 5, 6, 7, 8$ y 10, aunque solo se conocía el valor exacto para $k = 2$ y 3. En la última sección del trabajo daremos un repaso histórico a las contribuciones del problema, haciendo hincapié en su estado actual.

La demostración que ofreceremos del teorema de Hilbert-Waring, no obstante, sigue las líneas generales de la proporcionada por Linnik [4] en 1943, con algunas simplificaciones.

# 3. El teorema de Hilbert-Waring

## 3.1. Densidad de Schnirelmann

Introducimos, como primera aproximación a la demostración del teorema, el concepto de densidad de Schnirelmann, una herramienta sencilla pero cargada de potencial. Como su nombre indica, la densidad mide cómo de *densa* es una secuencia de enteros, y ofrece resultados concluyentes en diversos teoremas de la teoría de números.

**Definición 3.1.** *Sea $\mathcal{U}$ un conjunto de enteros no negativos (y distintos). Denotamos por $A(n)$ al número de enteros positivos en $\mathcal{U}$ que no exceden $n$; es decir*

$$A(n) = \sum_{1 \leqslant a \leqslant n} 1, \qquad \text{con } a \in \mathcal{U}.$$

*Supongamos que existe un número positivo $\alpha$ tal que $A(n) \geqslant \alpha n$ para cada entero positivo $n$. Decimos entonces que $\mathcal{U}$ tiene densidad positiva. El mayor $\alpha$ con esta propiedad se denomina densidad de $\mathcal{U}$.*

Esta es la conocida como densidad de Schnirelmann. Como $A(n) \leqslant n$, se deduce que $\alpha \leqslant 1$. Además, si $\alpha = 1$, entonces $A(n) = n$ para todo $n$, así que $\mathcal{U}$ debe incluir todos los enteros positivos. Sintetizamos esta información en la siguiente observación.

**Observación 3.2.** La densidad de un conjunto cumple $\alpha \leqslant 1$. En el caso $\alpha = 1$, el conjunto incluye todos los enteros positivos.

Podemos observar que la densidad es muy sensible a los números pequeños del conjunto. Es fácil comprobar que si $1 \notin \mathcal{U}$, entonces $\alpha = 0$. Y si $2 \notin \mathcal{U}$, entonces $\alpha \leqslant 1/2$. Un análisis más completo concluye que las densidades de los conjuntos de los números pares e impares son, respectivamente, $1/2$ y $0$, un resultado poco intuitivo.

Introducimos ahora los símbolos $\mathcal{B}$, $b$, $B(n)$, $\beta$, y $\mathcal{C}$, $c$, $C(n)$, $\gamma$. Todos ellos con definiciones análogas a $\mathcal{U}$, $a$, $A(n)$ y $\alpha$. Con ellos podemos definir la suma de conjuntos y su densidad asociada.

**Definición 3.3.** *El conjunto de enteros de la forma $a+b$ ($a \in \mathcal{U}$ y $b \in \mathcal{B}$) se llama suma de $\mathcal{U}$ y $\mathcal{B}$, y se denota como $\mathcal{C}$. Podemos escribir $\mathcal{C} = \mathcal{U} + \mathcal{B}$.*

**Teorema 3.4.** *Sea $\mathcal{C} = \mathcal{U} + \mathcal{B}$ y consideremos $0 \in \mathcal{U}$. Entonces $\gamma \geqslant \alpha + \beta - \alpha\beta$.*

*Demostración.* Como $\beta > 0$, tendremos que $1 \in \mathcal{B}$. Distinguimos tres tipos de números positivos en $\mathcal{C}$, todos ellos diferentes y acotados por $n$:

(i) En $\mathcal{B}$ escribimos $b_1 = 1$, $b_2$, ..., $b_{B(n)}$, números colocados en orden creciente. Como $0 \in \mathcal{U}$, se deduce que $b_1$, $b_2$, ..., $b_{B(n)}$ son miembros de $\mathcal{C}$. Aquí tenemos $B(n)$ componentes de $\mathcal{C}$.

(ii) Para cada $v$ en $1 \leqslant v \leqslant B(n)-1$, los números de la forma $a+b_v$, con $a \in \mathcal{U}$ y $1 \leqslant a \leqslant b_{v+1}-b_v-1$, son enteros positivos y distintos en $\mathcal{C}$, ninguno de ellos excediendo $n$. De hecho,

$$a+b_v \leqslant (b_{v+1}-b_v-1)+b_v = b_{v+1}-1 \leqslant b_{B(n)}-1 \leqslant n-1$$

y, también,

$$a+b_v \geqslant 1+b_v,$$

así que

$$1+b_v \leqslant a+b_v \leqslant b_{v+1}-1.$$

Se observa que los dos tipos de números en (i) y en (ii) son distintos entre sí. Para cada $v$ fijo ($1 \leqslant v \leqslant B(n)-1$), hay $A(b_{v+1}-b_v-1)$ números $a+b_v$ en $\mathcal{C}$.

(iii) Para $a \in \mathcal{U}$ y $1 \leqslant a \leqslant n-b_{B(n)}$, los números $a+b_{B(n)}$ son enteros positivos y distintos que no exceden $n$ en el conjunto $\mathcal{C}$. Como $a+b_{B(n)} \geqslant 1+b_{B(n)}$, podemos ver que los números de este último tipo son diferentes a los de (i) y (ii), y que hay $A(n-b_{B(n)})$ números de este tipo.

De los resultados encontrados en los apartados anteriores:

$$\begin{aligned}
C(n) &\geqslant B(n) + \sum_{v=1}^{B(n)-1} A(b_{v+1}-b_v-1) + A(n-b_{B(n)}) \\
&\geqslant B(n) + \sum_{v=1}^{B(n)-1} \alpha(b_{v+1}-b_v-1) + \alpha(n-b_{B(n)}) \\
&= B(n) + \alpha\left[b_{B(n)} - b_1 - (B(n)-1) + n - b_{B(n)}\right] \\
&= B(n) + \alpha\left[n - B(n)\right] \geqslant (1-\alpha)\beta n + \alpha n \\
&= n(\alpha+\beta-\alpha\beta).
\end{aligned}$$

Así pues,

$$\frac{C(n)}{n} \geqslant \alpha+\beta-\alpha\beta, \qquad \gamma \geqslant \alpha+\beta-\alpha\beta.$$

□

Este teorema no recoge el mejor resultado de este tipo. Mann [26] demostró en 1942 que $\gamma \geqslant \min(1, \alpha+\beta)$, utilizando argumentos más complicados. Para nuestro objetivo, basta considerar el resultado aquí presentado.

**Corolario 3.5.** *Sea $\mathcal{U}_k = \mathcal{U}+\cdots+\mathcal{U}$ la suma de $k$ conjuntos $\mathcal{U}$. Sea $\alpha_k$ la densidad de $\mathcal{U}_k$. Entonces*

$$\alpha_k \geqslant 1-(1-\alpha)^k.$$

*Demostración.* Procedemos por inducción.

Para $k=1$, obtenemos $\alpha_1 = \alpha$.

Para $k>1$, a partir de $\mathcal{U}_k = \mathcal{U}+\mathcal{U}_{k-1}$ y con la hipótesis de inducción, tenemos

$$\alpha_{k-1} \geqslant 1-(1-\alpha)^{k-1}.$$

Gracias al teorema 3.4, podemos deducir que

$$\begin{aligned}\alpha_k &\geqslant \alpha + \alpha_{k-1} - \alpha\alpha_{k-1} = \alpha + (1-\alpha)\alpha_{k-1} \\ &\geqslant \alpha + (1-\alpha)\left(1 - (1-\alpha)^{k-1}\right) \\ &= 1 - (1-\alpha)^k.\end{aligned}$$

□

**Teorema 3.6.** *Sean $\mathcal{U}$ y $\mathcal{B}$, con densidades $\alpha$ y $\beta$, tales que $\alpha + \beta \geqslant 1$. Si $0 \in \mathcal{U}$, entonces $\mathcal{C} = \mathcal{U} + \mathcal{B}$ tiene densidad $\gamma = 1$, es decir, el conjunto suma contiene todos los enteros positivos.*

*Demostración.* Supongamos que $\gamma < 1$ y que existe algún entero positivo $m \notin \mathcal{C}$. Sea $n$ el menor de esos enteros. Como $\beta > 0$, deducimos que $1 \in \mathcal{B}$; y como $0 \in \mathcal{U}$, deducimos que $1 \in \mathcal{C}$. Así que $n \geqslant 2$. Además, dado $0 \in \mathcal{U}$, tendremos que $n \notin \mathcal{B}$.

Consideremos los siguientes enteros positivos, $a$ y $n - b$, ninguno de ellos mayor que $n - 1$:

$$\begin{aligned} &a, && 1 \leqslant a \leqslant n-1, && a \in \mathcal{U}, \\ &n-b, && 1 \leqslant b \leqslant n-1, && b \in \mathcal{B}. \end{aligned}$$

Cada $a$ es diferente de $n - b$, porque $a = n - b$ implicaría $n = a + b \in \mathcal{C}$. Y como ninguna de estas familias excede $n - 1$, habrá como mucho $n - 1$ números entre ambas.

Por otro lado, la cantidad de números $a$ y $n - b$ es $A(n-1) + B(n-1)$. A partir de las relaciones

$$\begin{aligned} &A(n-1) \geqslant \alpha(n-1), \\ &B(n-1) = B(n) \geqslant \beta n > \beta(n-1), \end{aligned}$$

llegamos a

$$A(n-1) + B(n-1) > \alpha(n-1) + \beta(n-1) = (\alpha+\beta)(n-1) \geqslant n-1.$$

Esto contradice que la cantidad de números $a$ y $n-b$ no excede $n-1$, lo que prueba el teorema.

□

**Teorema 3.7.** *Sea $\mathcal{U}$ un conjunto con densidad $\alpha < 1$. Sea*

$$s_0 = 2\left[\frac{\log(2)}{-\log(1-\alpha)}\right] + 2.$$

*Si $0 \in \mathcal{U}$, entonces cualquier entero positivo es la suma de $s_0$ números de $\mathcal{U}$. Y si $0 \notin \mathcal{U}$, cualquier entero positivo es la suma de, como mucho, $s_0$ números de $\mathcal{U}$.*

*Demostración.* Supongamos $0 \in \mathcal{U}$ y consideremos $\mathcal{U}_k = \mathcal{U} + \cdots + \mathcal{U}$ la suma de $k$ conjuntos $\mathcal{U}$. Denotamos por $\alpha_k$ la densidad de $\mathcal{U}_k$. Por el lema 3.5, sabemos que $\alpha_k \geqslant 1 - (1-\alpha)^k$.

Observamos ahora que

$$\frac{s_0}{2} = \left[\frac{\log(2)}{-\log(1-\alpha)}\right] + 1 > \frac{\log(2)}{-\log(1-\alpha)},$$

así que

$$(1-\alpha)^{s_0/2} \leqslant (1-\alpha)^{\frac{\log(2)}{-\log(1-\alpha)}} = e^{\frac{\log(2)}{-\log(1-\alpha)}\log(1-\alpha)} = \frac{1}{2}.$$

En ese caso,

$$\alpha_{s_0/2} \geqslant 1 - (1-\alpha)^{s_0/2} \geqslant 1 - \frac{1}{2} = \frac{1}{2}.$$

Puesto que $0 \in \mathcal{U}_{s_0/2}$, el conjunto $\mathcal{U}_{s_0} = \mathcal{U}_{s_0/2} + \mathcal{U}_{s_0/2}$ debe, por el teorema 3.6, incluir todos los enteros positivos. Es decir, cualquier entero es suma de $s_0$ elementos de $\mathcal{U}$.

La segunda parte del teorema se deduce fácilmente de la primera, insertando el 0 artificialmente en $\mathcal{U}$.

□

**Teorema 3.8.** *Sea $\mathcal{U}^*$ una colección de enteros no negativos, pudiéndose repetir elementos. Sea $\mathcal{U}$ el subconjunto más grande de $\mathcal{U}^*$ sin repetir elementos. Sea $r(a)$ la multiplicidad de un elemento $a \in \mathcal{U}$. Suponemos que*

$$\frac{1}{n}\frac{\left(\sum\limits_{1\leqslant a\leqslant n} r(a)\right)^2}{\sum\limits_{1\leqslant a\leqslant n} r^2(a)} \geqslant \alpha' > 0$$

*para todo $n \geqslant 1$. Entonces $\mathcal{U}$ tiene densidad positiva $\alpha \geqslant \alpha'$.*

*Demostración.* A partir de la desigualdad de Bunyakovsky-Schwarz, tenemos

$$\left(\sum_{1\leqslant a\leqslant n} r(a)\right)^2 \leqslant \sum_{1\leqslant a\leqslant n} r^2(a) \sum_{1\leqslant a\leqslant n} 1^2 = A(n) \sum_{1\leqslant a\leqslant n} r^2(a).$$

Puesto que

$$\frac{A(n)}{n} \geqslant \frac{1}{n}\frac{\left(\sum\limits_{1\leqslant a\leqslant n} r(a)\right)^2}{\sum\limits_{1\leqslant a\leqslant n} r^2(a)} \geqslant \alpha' > 0,$$

el teorema queda probado. □

Estos dos últimos teoremas dan las claves para la demostración del teorema de Hilbert-Waring. En primer lugar, el teorema 3.7 muestra que, dado un conjunto $\mathcal{U}$ con densidad positiva, podemos escribir cualquier número natural como una suma

no infinita de elementos del conjunto $\mathcal{U}$. La única limitación que impone es que la colección $\mathcal{U}$ no repita elementos.

En segundo lugar, el teorema 3.8 plantea cómo trabajar con colecciones de enteros que permiten la repetición de elementos, $\mathcal{U}^*$. Para ello, da condiciones suficientes para que el conjunto de los enteros sin repetición, $\mathcal{U}$, tenga densidad positiva.

## 3.2. Demostración del teorema de Hilbert-Waring

Con los teoremas obtenidos para la densidad de un conjunto, podemos encarar la demostración del teorema de Hilbert-Waring. En lo que resta de sección, las letras $c$, $c_1$, $c_2$, etc., denotarán constantes positivas que dependen solo de $k$. Las constantes que aparezcan en el símbolo $O$ dependerán también de $k$. El objetivo será demostrar:

**Teorema 3.9** (Hilbert)**.** *Para cada entero positivo $k$ existe un entero positivo $c$ tal que todos los enteros positivos son la suma de, como mucho, $c$ potencias $k$-ésimas.*

La demostración se realizará de forma escalonada, dando primero una idea general de la misma.

Definimos $\mathcal{U}_t^*$ como la colección de enteros no negativos $x_1^k + \cdots + x_t^k$, donde cada uno de los $x_i$ toma todos los valores enteros no negativos. Denotamos por $\mathcal{U}_t$ el conjunto más grande formado por elementos distintos de $\mathcal{U}_t^*$. Sea, además,

$$c_1 = c_1(k) = \frac{1}{2}8^{k-1}.$$

El objetivo principal será demostrar que $\mathcal{U}_{c_1}$ tiene densidad positiva. Este resultado, junto con el teorema 3.7, demostraría directamente el teorema de Hilbert. Puesto que la colección $\mathcal{U}_{c_1}^*$ permite la multiplicidad de sus elementos, tendremos que emplear el teorema 3.8. Es decir, $\mathcal{U}_{c_1}$ tendrá densidad positiva si, para todo $n$, se cumple

$$\frac{1}{n}\frac{\left(\sum\limits_{1\leqslant a\leqslant n} r(a)\right)^2}{\sum\limits_{1\leqslant a\leqslant n} r^2(a)} \geqslant \alpha' > 0, \tag{3.1}$$

donde $r(a)$ denota la multiplicidad del elemento $a$ en $\mathcal{U}_{c_1}^*$. Dada la naturaleza de los conjuntos escogidos, $r(a)$ será el número de soluciones a

$$x_1^k + \cdots + x_{c_1}^k = a, \qquad x_i \geqslant 0.$$

Procedemos, por tanto, a acotar cada una de las partes de la desigualdad (3.1).

**Teorema 3.10.** *Si $n \geqslant 1$, entonces*

$$\sum_{1 \leqslant a \leqslant n} r(a) \geqslant c_2(k) n^{c_1/k}.$$

*Demostración.* Podemos asumir $n > c_1$. Entonces

$$\begin{aligned}\sum_{1 \leqslant a \leqslant n} r(a) &= -1 + \sum_{0 \leqslant a \leqslant n} \sum_{\substack{x_1^k + \cdots + x_{c_1}^k = a \\ x_i \geqslant 0}} 1 \\ &\geqslant -1 + \sum_{0 \leqslant x_1 \leqslant (n/c_1)^{1/k}} \cdots \sum_{0 \leqslant x_{c_1} \leqslant (n/c_1)^{1/k}} 1 \\ &\geqslant \left(\frac{n}{c_1}\right)^{c_1/k} - 1 \geqslant c_3(k) n^{c_1/k}.\end{aligned}$$

□

La dificultad la encontramos al acotar el denominador de la desigualdad (3.1). Necesitamos algunos teoremas previos.

**Lema 3.11.** *Sean $X, Y \geqslant 1$, sea $n$ un entero y sea $q(n)$ el número de soluciones enteras $a$*

$$x_1 y_1 + x_2 y_2 = n \qquad (|x_m| \leqslant X,\ |y_m| \leqslant Y,\ m = 1, 2). \tag{3.2}$$

*Entonces*

$$q(n) \leqslant \begin{cases} 27 X^{3/2} Y^{3/2}, & si \ \ n = 0, \\ 60 XY \sum_{d \mid n} \frac{1}{d}, & si \ \ n \neq 0. \end{cases}$$

*Demostración.* En primer lugar, consideremos $n = 0$. Entonces los valores tomados por $x_1$, $x_2$ y $y_1$ no pueden exceder $2X + 1$, $2X + 1$ y $2Y + 1$. Cuando $x_1$, $x_2$ y $y_1$ están especificados, $y_2$ solo puede tomar un valor. Así pues

$$q(0) \leqslant (2X + 1)^2 (2Y + 1) \leqslant (3X)^2 (3Y) = 27 X^2 Y.$$

Similarmente, $q(0) \leqslant 27 XY^2$. Entonces

$$q(0) \leqslant \text{mín}(27X^2 Y, 27XY^2) \leqslant \sqrt{27X^2 Y \cdot 27XY^2} = 27 X^{3/2} Y^{3/2}.$$

Consideremos ahora $n \neq 0$. Podemos asumir sin pérdida de generalidad que $X \leqslant Y$. Sea $q_1(n)$ el número soluciones enteras a

$$x_1 y_1 + x_2 y_2 = n \qquad ((x_1, x_2) = 1,\ |x_2| \leqslant |x_1| \leqslant X,\ |y_m| \leqslant Y,\ m = 1, 2)$$

Claramente $x_1 \neq 0$, porque de lo contrario $x_2 = 0$, dando $n = 0$, en contradicción con nuestra hipótesis. Ahora, para un conjunto fijo de $x_1$, $x_2$, con $(x_1, x_2) = 1$ y $|x_2| \leqslant |x_1| \leqslant X$, denotamos por $q_2(n; x_1, x_2)$ el número de soluciones enteras en $y_1$,

$y_2$ a la ecuación anterior. Se trata de un sistema resoluble, y si $y_1'$, $y_2'$ es un conjunto de soluciones, entonces todas las soluciones del sistema vienen dadas por

$$y_1 = y_1' + tx_2, \qquad y_2 = y_2' - tx_1, \qquad t \in \mathbb{Z}.$$

Esto es consecuencia de que $x_1y_1 + x_2y_2 = n$ y $x_1y_1' + x_2y_2' = n$, lo que hace que $x_1(y_1 - y_1') + x_2(y_2 - y_2') = 0$. Como $(x_1, x_2) = 1$, se cumplirá $x_1|(y_1 - y_1')$, es decir, $y_1 = y_1' + tx_2$. De la ecuación inicial se despeja $y_2 = y_2' - tx_1$.

Entonces

$$|t| = \left|\frac{y_2' - y_2}{x_1}\right| \leqslant \frac{Y + Y}{|x_1|} = \frac{2Y}{|x_1|},$$

y el número de valores que toma $t$ no excede

$$2 \cdot \frac{2Y}{|x_1|} + 1 \leqslant \frac{4Y + X}{|x_1|} \leqslant \frac{5Y}{|x_1|}.$$

Esto es,

$$q_2(n; x_1, x_2) \leqslant \frac{5Y}{|x_1|}.$$

Por tanto,

$$\begin{aligned} q_1(n) &\leqslant \sum_{1 \leqslant |x_1| \leqslant X} \sum_{|x_2| \leqslant |x_1|} \frac{5Y}{|x_1|} \leqslant 5Y \sum_{1 \leqslant |x_1| \leqslant X} \frac{2|x_1| + 1}{|x_1|} \\ &\leqslant 5Y \cdot 3 \cdot 2X = 30XY. \end{aligned}$$

Observamos que, con la condición añadida $(x_1, x_2) = 1$, el número de soluciones a la ecuación (3.2) no excede $2 \cdot 30XY = 60XY$.

Ahora, consideremos $(x_1, x_2) = d \neq 1$, donde $d|n$. En ese caso, $x_1' = x_1/d$ y $x_2' = x_2/d$, lo que permite modificar el sistema hasta llegar a uno similar al ya estudiado,

$$x_1'y_1 + x_2'y_2 = \frac{n}{d} \qquad \left((x_1', x_2') = 1,\ |x_m| \leqslant \frac{X}{d},\ |y_m| \leqslant Y,\ m = 1, 2)\right).$$

Observamos que el número de soluciones de este sistema no excede $60\frac{X}{d}Y$. En conclusión,

$$q(n) \leqslant 60XY \sum_{d|n} \frac{1}{d}.$$

□

**Teorema 3.12.** *Sea $k \geqslant 2$ y $P \geqslant 1$, y sea $f(x)$ una función polinómica de grado $k$ con coeficientes enteros:*

$$f(x) = a_kx^k + a_{k-1}x^{k-1} + \cdots + a_1x + a_0,$$

$$a_k = O(1), \quad a_{k-1} = O(P), \quad ..., \quad a_1 = O(P^{k-1}), \quad a_0 = O(P^k)$$

*Entonces*

$$\int_0^1 \left|\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right|^{8^{k-1}} d\alpha = O(P^{8^{k-1}-k}). \tag{3.3}$$

*Demostración.* Cuando $k = 2$, la parte izquierda de la expresión (3.3) es el número de soluciones enteras a

$$f(x_1) + f(x_2) - f(y_1) - f(y_2) = f(x_3) + f(x_4) - f(y_3) - f(y_4)$$

$$(f(x) = a_2x^2 + a_1x + a_0, \quad a_2 = O(1), \quad a_2 = O(P), \quad a_0 = O(P^2)),$$

$$0 \leqslant x_m, y_m \leqslant P, \qquad 1 \leqslant m \leqslant 4 \tag{3.4}$$

Esto se deduce a partir de la identidad

$$\left|\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right|^8 = \left[\sqrt{\left(\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right)\left(\sum_{x=0}^{P} e^{-2\pi i f(x)\alpha}\right)}\right]^8$$
$$= \left(\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right)^4 \left(\sum_{x=0}^{P} e^{-2\pi i f(x)\alpha}\right)^4,$$

donde un término genérico del sumatorio será

$$e^{2\pi i\alpha(f(x_1)+f(x_2)+f(x_3)+f(x_4)-f(y_1)-f(y_2)-f(y_3)-f(y_4))}$$

con $0 \leqslant x_m, y_m \leqslant P$. Puesto que, para cualquier entero $q$,

$$\int_0^1 e^{2\pi i q\alpha} d\alpha = \begin{cases} 1, & \text{si } q = 0, \\ 0, & \text{si } q \neq 0, \end{cases}$$

concluimos que la integral *suma 1* cada vez que se anula el exponente del término genérico.

Sea $x_i - y_i = z_i$, $a_2(x_i + y_i) + a_1 = w_i$ $(1 \leqslant i \leqslant 4)$. Este cambio de variables muestra que el número de soluciones de (3.4) no excede el número de soluciones enteras a

$$z_1w_1 + z_2w_2 = z_3w_3 + z_4w_4 \qquad (z_i = O(P),\ w_i = O(P),\ 1 \leqslant i \leqslant 4). \tag{3.5}$$

Denotamos por $q(n)$ al número de soluciones enteras de

$$z_1w_1 + z_2w_2 = n, \tag{3.6}$$

con $z_i = O(P)$, $w_i = O(P)$, $i = 1, 2$, y donde las constantes implicadas en el símbolo $O$ son las mismas que en (3.5). Entonces, el número de soluciones a la ecuación (3.5) será

$$\sum_{|n| \leqslant c_4P^2} q^2(n),$$

donde $c_4$ es una constante positiva que solo depende de $k$. Este resultado se deduce de sumar el número de soluciones de cada sistema (3.6), donde $|n|$ recorre todos los valores posibles entre 0 y $c_4P^2$, dado que $z_i = O(P)$ y $w_i = O(P)$, con $i = 1, 2$.

En virtud del lema 3.11,

$$\begin{aligned}\sum_{|n|\leqslant c_4P^2} q^2(n) &= O(P^6) + O\left(\sum_{1\leqslant n\leqslant c_4P^2}\left(P^2\sum_{d|n}\frac{1}{d}\right)^2\right)\\ &= O(P^6) + O\left(P^4\sum_{1\leqslant d_1,d_2\leqslant c_4P^2}\frac{1}{d_1d_2}\sum_{\substack{\frac{d_1d_2}{(d_1,d_2)}\mid n\\ 1\leqslant n\leqslant c_4P^2}} 1\right)\\ &= O(P^6) + O\left(P^4\sum_{d_1=1}^{\infty}\sum_{d_2=1}^{\infty}\frac{P^2}{(d_1d_2)^{3/2}}\right)\\ &= O(P^6).\end{aligned}$$

Este resultado demuestra el caso $k = 2$, donde la convergencia del sumatorio se puede comprobar sencillamente por el criterio de la integral.

Supongamos $k \geqslant 3$ y procedamos por inducción. Asumimos que el teorema es cierto para $k-1$. Observamos que

$$\begin{aligned}\left|\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right|^2 &= \sum_{x=0}^{P} e^{-2\pi i f(x)\alpha}\sum_{-x\leqslant h\leqslant P-x} e^{2\pi i f(x+h)\alpha}\\ &= \sum_{0<|h|\leqslant P}^{*}\sum_{x=0}^{*\,P} e^{2\pi i h\varphi(x,h)\alpha} + P,\end{aligned}$$

donde los sumatorios con el asterisco se extienden solo sobre los enteros que incluya su intervalo de definición, y donde $\varphi(x,h) = \frac{1}{h}(f(x+h) - f(x))$, con $h \neq 0$. Al tomar $\varphi(x,h)$ como un polinomio en la variable $x$, deducimos que $\varphi(x,h)$ es un polinomio de grado $k-1$ que satisface las condiciones del teorema. Si escribimos

$$a_h = \sum_{x=0}^{*\,P} e^{2\pi i h\varphi(x,h)\alpha},$$

tenemos, entonces,

$$\left|\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right|^{2\cdot 8^{k-2}} \leqslant 2^{8^{k-2}}\,\text{máx}\left(\left|\sum_{0<|h|\leqslant P}^{*} a_h\right|^{8^{k-2}}, P^{8^{k-2}}\right),$$

de acuerdo con la expresión del binomio de Newton. Si tuviéramos

$$\left|\sum_{0<|h|\leqslant P}^{*} a_h\right| \leqslant P,$$

entonces obtendríamos el resultado que buscamos y el teorema quedaría probado. Si no se diera este caso, la desigualdad de Bunyakovsky-Schwarz permitiría escribir

la siguiente cadena de desigualdades, al aplicarla repetidamente sobre el sumatorio de las $|a_h|$:

$$\begin{aligned} 2^{-8^{k-2}} \left| \sum_{x=0}^{P} e^{2\pi i f(x)\alpha} \right|^{2\cdot 8^{k-2}} &\leqslant \left| \sum_{0<|h|\leqslant P}^{*} a_h \right|^{8^{k-2}} \leqslant \left( \sum_{0<|h|\leqslant P}^{*} 1 \cdot \sum_{0<|h|\leqslant P}^{*} |a_h|^2 \right)^{2^{3(k-2)-1}} \\ &\leqslant \left[ \left( \sum_{0<|h|\leqslant P}^{*} 1 \right)^{2^2-1} \sum_{0<|h|\leqslant P}^{*} |a_h|^{2^2} \right]^{2^{3(k-2)-2}} \leqslant \cdots \\ &\leqslant \left[ \left( \sum_{0<|h|\leqslant P}^{*} 1 \right)^{2^{3(k-1)-1}-1} \sum_{0<|h|\leqslant P}^{*} |a_h|^{2^{3(k-2)-1}} \right]^{2} \\ &\leqslant (3P)^{8^{k-2}-1} \sum_{0<|h|\leqslant P}^{*} |a_h|^{8^{k-2}}. \end{aligned} \tag{3.7}$$

Con este resultado, concluimos que

$$2^{-8^{k-2}} \left| \sum_{x=0}^{P} e^{2\pi i f(x)\alpha} \right|^{2\cdot 8^{k-2}} \leqslant O\left( P^{8^{k-2}-1} \sum_{0<|h|\leqslant P}^{*} \left| \sum_{x=0}^{*\,P} e^{2\pi i h\varphi(x,h)\alpha} \right|^{8^{k-2}} \right). \tag{3.8}$$

Solo queda por acotar cada uno de los $|a_h|$. Para ello, sea

$$\left| \sum_{x=0}^{*\,P} e^{2\pi i h\varphi(x,h)\alpha} \right|^{8^{k-2}} = \sum_{n} A(n) e^{2\pi i h n\alpha}. \tag{3.9}$$

Para $0 \leqslant x \leqslant P$, deducimos que

$$n = O\left( \max_{0\leqslant x\leqslant P} |\varphi(x,h)| \right) = O(P^{k-1}).$$

De la expresión (3.9) y la hipótesis de inducción, tenemos

$$\begin{aligned} |A(n)| &= \left| \int_0^1 \left| \sum_{x=0}^{*\,P} e^{2\pi i \varphi(x,h)\beta} \right|^{8^{k-2}} e^{-2\pi i n\beta} d\beta \right| \\ &\leqslant \int_0^1 \left| \sum_{x=0}^{P} e^{2\pi i \varphi(x,h)\beta} \right|^{8^{k-2}} d\beta = O(P^{8^{k-2}-(k-1)}). \end{aligned}$$

Si ahora elevamos a la cuarta potencia el resultado de (3.8), y después integramos

la expresión respecto a $\alpha$, entre 0 y 1, concluimos que

$$\begin{aligned}\int_0^1 \left|\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right|^{8^{k-1}} d\alpha &= O\left(P^{4\cdot 8^{k-2}-4}\int_0^1 \left(\sideset{}{^*}\sum_{0<|h|\leqslant P}\left|\sum_{x=0}^{*\ P} e^{2\pi i h\varphi(x,h)\alpha}\right|^{8^{k-2}}\right)^4 d\alpha\right)\\ &= O\left(P^{4\cdot 8^{k-2}-4}\sum_{\substack{n_1h_1+n_2h_2=n_3h_3+n_4h_4\\ 0<|h_i|\leqslant P\\ n_i=O(P^{k-1})\\ i=1,2,3,4}} A(n_1)A(n_2)A(n_3)A(n_4)\right)\\ &= O\left(P^{4\cdot 8^{k-2}-4}P^{4\cdot 8^{k-2}-4(k-1)}\sum_{\substack{n_1h_1+n_2h_2=n_3h_3+n_4h_4\\ 0<|h_i|\leqslant P\\ n_i=O(P^{k-1})\\ i=1,2,3,4}} 1\right)\\ &= O(P^{4\cdot 8^{k-2}-4}P^{4\cdot 8^{k-2}-4(k-1)}P^{3k}) = O(P^{8^{k-1}-k}),\end{aligned}$$

donde la última igualdad surge de un razonamiento análogo al ofrecido al resolver el sistema (3.5). Este resultado completa la prueba del teorema. □

Ya estamos en condiciones de acotar el denominador de la desigualdad (3.1).

**Teorema 3.13.** *Si $k \geqslant 2$ y $n \geqslant 1$, entonces*

$$\sum_{1\leqslant a\leqslant n} r^2(a) \leqslant c_6(k)n^{2c_1/k-1}.$$

*Demostración.* Del teorema 3.12 sabemos que, si $k \geqslant 2$ y $P \geqslant 1$, entonces

$$\int_0^1 \left|\sum_{x=0}^{P} e^{2\pi i x^k\alpha}\right|^{2c_1} d\alpha \leqslant c_5(k)P^{2c_1-k},$$

donde, recordamos, $c_1 = \frac{1}{2}8^{k-1}$.

Tomamos $P = \left[n^{1/k}\right]$ para que, con $n$ grande, $c_1P^k > n$. Tenemos en cuenta que, para cualquier entero $q$,

$$\int_0^1 e^{2\pi i q\alpha} d\alpha = \begin{cases}1, & \text{si } q = 0,\\ 0, & \text{si } q \neq 0.\end{cases}$$

Definimos

$$Q(a) = \sum_{\substack{x_1^k+\cdots+x_{c_1}^k=a\\ 0\leqslant x_i\leqslant P\\ 1\leqslant i\leqslant c_1}} 1.$$

Así pues,

$$\begin{aligned}\sum_{1\leqslant a\leqslant n} r^2(a) &\leqslant \sum_{0\leqslant a\leqslant c_1P^k} Q(a)^2\\ &= \int_0^1 \left|\sum_{0\leqslant a\leqslant c_1P^k} e^{2\pi i a\alpha}Q(a)\right|^2 d\alpha\\ &= \int_0^1 \left|\sum_{x_1=0}^{P}\cdots\sum_{x_{c_1}=0}^{P} e^{2\pi i(x_1^k+\cdots+x_{c_1}^k)\alpha}\right|^2 d\alpha\\ &= \int_0^1 \left|\sum_{x=0}^{P} e^{2\pi i x^k\alpha}\right|^{2c_1} d\alpha \leqslant c_5(k)P^{2c_1-k}\\ &\leqslant c_6(k)n^{2c_1/k-1}.\end{aligned}$$

□

Una vez acotados los dos términos de la desigualdad (3.1), podemos demostrar que nuestro conjunto inicial tiene densidad positiva.

**Teorema 3.14.** *Si $k \geqslant 2$, entonces $\mathcal{U}_{c_1}$ tiene densidad positiva.*

*Demostración.* A partir de las cotas encontradas en los teoremas 3.10 y 3.13 observamos que

$$\frac{1}{n}\frac{\left(\sum\limits_{1\leqslant a\leqslant n} r(a)\right)^2}{\sum\limits_{1\leqslant a\leqslant n} r^2(a)} \geqslant \frac{1}{n}\frac{\left(c_2(k)n^{c_1/k}\right)^2}{c_6(k)n^{2c_1/k-1}} = c_7(k) > 0$$

Por el teorema 3.8, queda visto que $\mathcal{U}_{c_1}$ tiene densidad positiva. □

Concluye así la demostración del teorema de Hilbert-Waring, según lo expuesto al principio del capítulo.

En síntesis, hemos comprobado que el conjunto $\mathcal{U}_{c_1}$, formado por todos los enteros de la forma $x_1^k+\cdots+x_{c_1}^k$, donde cada uno de los $x_i$ toma todos los valores enteros no negativos, tiene densidad positiva. Este resultado, junto con el teorema 3.7, muestra que existe un natural $s(k)$ tal que $\mathcal{U}_{s(k)}$ tiene densidad 1. En otras palabras, existe un natural $s(k)$ tal que cualquier entero no negativo es suma de $s(k)$ potencias $k$-ésimas.

# 4. Recorrido histórico y estado actual

Desde el momento de su publicación, en 1770, el problema de Waring ha sido objeto de una minuciosa investigación matemática. No todo el desarrollo se ha centrado en el enunciado original de Waring, sino que, con el tiempo, se han propuesto y estudiado decenas de variantes distintas del problema. En la actualidad, todas ellas se engloban dentro de una categoría propia en la teoría de números.

## 4.1. Métodos elementales

El primer aporte se lo debemos a Lagrange [3] y su teorema de los cuatro cuadrados, publicado en 1770. Como ya hemos comentado, el caso $k = 2$ ha recibido mucha atención a lo largo de la historia, y es el que más resultados ha conseguido. Podríamos destacar, en ese aspecto, el teorema de Fermat, que establece qué primos son expresables como suma de dos cuadrados, de 1640. Y también el teorema de Legendre [7], de 1798, que completaba el resultado de Lagrange dando condiciones necesarias y suficientes para escribir un número como suma de tres cuadrados.

Más interés tiene el caso $k = 3$, dado que aún sigue parcialmente abierto. El primer aporte lo realizó Maillet [6] en 1895, demostrando que cualquier entero positivo se puede representar como suma de 21 cubos. No es una cota muy acertada, pero sentó las bases para desmenuzar el problema de los cubos: la identidad

$$(r + x)^3 + (r - x)^3 = 2r^3 + 6rx^2.$$

Esta expresión permite reformular el problema, pasando de representar un entero como la suma de cubos a representar otro entero asociado como suma de cuadrados. Guiado por esta idea, Wieferich [8] consiguió demostrar que $g(3) = 9$ en 1909. El esquema de la demostración es similar a nuestro teorema 2.30: la parte puramente teórica solo demostraba que los enteros superiores a $2{,}25 \cdot 10^9$ podían escribirse como suma de nueve cubos, y hubo que comprobar computacionalmente el resto, con ayuda de algunas simplificaciones.

El resultado de Wierferich sugiere la acotación natural $G(3) \leqslant 9$. Landau [9], en 1911, mejoró el resultado hasta $G(3) \leqslant 8$ y Baer [10], en 1913, precisó que todo entero mayor de $14{,}1 \cdot 233^6 \simeq 2{,}26 \cdot 10^{15}$ es la suma de ocho cubos. Por último, Dickson [11], en 1939, concluyó que todos los enteros positivos, a excepción del 23 y el 239, son suma de ocho cubos.

Linnik [12], en 1943, consiguió reducir la cota hasta $G(3) \leqslant 7$; y McCurley [13], en 1984, precisó que todo entero mayor de $\exp(\exp(13{,}94))$ se puede escribir como suma de siete cubos. Samir Seisik [14] terminó de completar el problema en 2016, concluyendo que los únicos números que necesitan más de siete cubos para ser representados son:

$$15,\ 22,\ 23,\ 50,\ 114,\ 167,\ 175,\ 186,\ 212,$$
$$231,\ 238,\ 239,\ 303,\ 364,\ 420,\ 428,\ 454.$$

Este resultado se presentó en los *Barcelona Mathematical Days* de 2017.

Poco más se puede decir del caso $k = 3$. La evidencia computacional muestra que 8042 es el número más grande que requiere siete cubos para ser escrito, y los ordenadores apuntan hacia $G(3) = 4$ o 5. Como Jacobi [15], en 1851, demostró que los enteros congruentes con 4 o 5 (mód 9) no se pueden representar con tres cubos, la acotación más actualizada es

$$4 \leqslant G(3) \leqslant 7.$$

## 4.2. El método del círculo y potencias superiores

La concepción del problema de Waring cambió radicalmente entre 1920 y 1928 a raíz de unos artículos publicados por Hardy y Littlewood [16] bajo el título genérico *Some problems of partitio numerorum*. En ellos, desarrollaban un nuevo método analítico, conocido en la actualidad como método del círculo, que ha ofrecido resultados tan contundentes como:

1. La demostración del problema de Waring, junto con estimaciones de las cantidades $g(k)$ y $G(k)$.

2. La demostración del teorema de Vinogradov, que afirma que todo número impar suficientemente grande es suma de tres primos.

3. La prueba de que casi todo número par (en el sentido de densidad) es suma de dos primos.

Hardy y Littlewood aportaron cotas superiores de $G(k)$ para todo $k$. La primera de ellas fue $G(k) \leqslant (k-2)2^{k-1} + 5$, y la segunda un poco más complicada que es asintótica a $k2^{k-2}$ para $k$ grandes. En particular, probaron que

$$G(4) \leqslant 19, \quad G(5) \leqslant 41, \quad G(6) \leqslant 87, \quad G(7) \leqslant 193, \quad G(8) \leqslant 425. \tag{4.1}$$

Su método no dio ningún resultado para G(3), pero probaron que casi todos los números, en el sentido de densidad, son sumas de 5 cubos.

En lo que concierne a $g(k)$, los mejores resultados hasta 1933, para valores pequeños de k pequeños, eran

$$g(4) \leqslant 37, \quad g(5) \leqslant 58, \quad g(6) \leqslant 478, \quad g(7) \leqslant 3806, \quad g(8) \leqslant 31353, \tag{4.2}$$

encontrados, respectivamente, por Wieferich, Baer, Baer, Wieferich y Kempner mediante métodos elementales [3]. Un año después, R. D. James tuvo éxito al demostrar que

$$g(6) \leqslant 183, \quad g(7) \leqslant 322, \quad g(8) \leqslant 595, \tag{4.3}$$

y también encontró cotas para $g(9)$ y $g(10)$.

El trabajo posterior de Vinogradov [17], a partir de 1924, hizo posible obtener resultados más satisfactorios, gracias a la modificación del método del círculo. Entre otros logros, mejoró las cotas existentes para valores de $k$ grandes:

$$G(k) \leqslant 6k \log k + (4 + \log 216)k. \tag{4.4}$$

Puede deducirse de la cota anterior que $G(k)$ es, como mucho, del orden de $k \log k$, lo que arroja cierta información sobre el comportamiento asintótico de $G(k)$.

Poco más tarde, la prueba de Vinogradov fue simplificada por Heilbronn [18], quien probó que

$$G(k) \leqslant 6k \log k + \left(4 + \log\left(3 + \frac{2}{k}\right)\right) k + 3. \tag{4.5}$$

Esta acotación es mejor que la obtenida en (4.1) para $k > 6$. En 1947, Vinogradov [19] mejoró el resultado a

$$G(k) \leqslant k(3 \log k + 11), \tag{4.6}$$

y Tong [20], en 1957, y Cheng [21], en 1958, remplazaron el 11 de la cota por 9 y 5.2, respectivamente.

En 1959, Vinogradov [22] demostró que

$$G(k) \leqslant k(2 \log k + 4 \log\log k + 2 \log\log\log k + 13) \tag{4.7}$$

para $k$ mayores de 170 000.

Llegados a este punto, podríamos distinguir dos áreas de estudio diferenciadas en el problema de Waring. En primer lugar, determinar el comportamiento asintótico de $G(k)$, o lo que es lo mismo, estudiar su comportamiento para valores grandes de $k$. En segundo lugar, mejorar las cotas ya existentes para valores pequeños de $k$. Dado que el primer punto ha sido revisado en las líneas anteriores, dedicaremos las siguientes a resumir las cotas para potencias bajas.

## 4.3. Cotas actuales

Los únicos valores conocidos de $G(k)$ son

$$G(2) = 4, \qquad G(4) = 16. \tag{4.8}$$

Del primero, esta memoria ofrece un par de demostraciones. En cuanto al segundo, podríamos atribuírselo a Davenport [23], quien demostró que $G(4) \leqslant 16$. Este resultado, junto con nuestro teorema 1.6, termina por determinar el valor exacto de $G(4)$.

Para el resto de potencias $k$-ésimas, solo se conoce una acotación, siendo las mejores, en la actualidad,

$$G(3) \leqslant 7, \quad G(5) \leqslant 17, \quad G(6) \leqslant 24, \quad G(7) \leqslant 33, \quad G(8) \leqslant 42.$$

En cuanto a $g(k)$, a lo largo del siglo XX se ha podido construir una solución bastante completa para determinar su valor. Consideramos $[x]$ como la parte entera de $x$, y definimos $\{x\} = x - [x]$. Si $k \geqslant 6$, entonces

$$g(k) = 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2.$$

Este resultado se basa en la hipótesis

$$2^k \left\{ \left(\frac{3}{2}\right)^k \right\} + \left[ \left(\frac{3}{2}\right)^k \right] \leqslant 2^k, \tag{4.9}$$

que aún no ha podido ser demostrada. Si la hipótesis resultara ser falsa, entonces

$$g(k) = 2^k + \left[ \left(\frac{3}{2}\right)^k \right] + \left[ \left(\frac{4}{3}\right)^k \right] - \theta,$$

donde $\theta$ es 2 o 3 dependiendo de si $[(4/3)^k][(3/2)^k] + [(4/3)^k] + [(3/2)^k]$ iguala o excede $2^k$.

La condición (4.9) se conoce cierta para $k \leqslant 471\ 600\ 000$ [24], y Mahler [25] demostró que solo existe un número finito de valores que no la satisfacen. Además, encaja con la cota inferior que encontramos en el teorema 1.4. Ella constituye el último eslabón del problema de Waring, del que podríamos decir que está prácticamente solucionado.

| $k$ | $g(k)$ | $G(k)$ |
|---|---|---|
| 2 | 4 | 4 |
| 3 | 9 | $\leqslant 7$ |
| 4 | 19 | 16 |
| 5 | 37 | $\leqslant 17$ |
| 6 | 73 | $\leqslant 24$ |
| 7 | 143 | $\leqslant 33$ |
| 8 | 279 | $\leqslant 42$ |
| 9 | 548 | $\leqslant 51$ |
| 10 | 1079 | $\leqslant 59$ |

Tabla 1: Valores conocidos de $g(k)$ y $G(k)$ para $k$ pequeños.

# 5. Conclusiones

En la presente memoria hemos ofrecido un análisis exhaustivo de los principales resultados relativos al teorema de Hilbert-Waring y, asimismo, hemos dado un repaso a la trayectoria histórica del problema. Tras dos siglos y medio de investigación matemática, podemos considerarlo prácticamente cerrado.

Nuestro estudio se ha centrado en dos aspectos fundamentales. En primer lugar, hemos introducido la notación moderna del problema y hemos empleado métodos elementales para encontrar diversas cotas superiores e inferiores. Cabe destacar que, según aumentaba el exponente $k$, las acotaciones elementales se tornaban más imprecisas, aun manteniendo su interés como demostraciones de existencia. Como hemos remarcado, los resultados obtenidos con estos métodos no pueden generalizarse, pues se sustentan en propiedades específicas de residuos modulares e identidades que involucran sumas de potencias $k$-ésimas.

En segundo lugar, hemos demostrado la veracidad del enunciado del problema de Waring a partir de la densidad de Schnirelmann. Para ello, hemos simplificado la prueba que ofreció Linnik [4, 5] en 1943. Esta demostración mantiene su interés en calidad de existencia, pues no desprende, de manera directa, ninguna expresión para estimar la cantidad de potencias $k$-ésimas necesarias para resolver el problema.

Finalmente, hemos ofrecido, sin demostrar, las acotaciones más actuales del problema de Waring. Hemos mostrado que los números $g(k)$ se conocen para todo valor de $k$, a falta de matizar la veracidad de la desigualdad (4.9), que se ha comprobado cierta para $k < 471\ 000\ 000$. Por otro lado, de $G(k)$ solo se conoce el valor exacto para $G(2) = 4$ y $G(4) = 16$, estando el resto de casos acotados con mayor o menor grado de precisión. De hecho, uno de los últimos aportes a la cota de $G(3)$ data del año 2016, lo que muestra que el problema de Waring sigue siendo un elemento activo de la investigación matemática.

# Referencias


[1] Waring, E.: *Meditationes Algebraicae*, Typis Academicis, Cambridge, 1770.

[2] Hilbert, D. (1909). "Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen (Waringsches Problem)". *Mathematische Annalen.* 67 (3): 281-300.

[3] Hardy, G. H. and Wright, E. M.: *An Introduction to the Theory of Numbers, 5th ed.*, cap. XX-XXI. Oxford, England: Clarendon Press, 1979.

[4] Linnik, Y. V.: An elementary solution of Waring's problem by Shnirelman's method (Russian), *Mat. Sbornik NS 12* (1943), 225-230.

[5] Hua, L.-K.: *Introduction to Number Theory*, pp. 514-533. New York, Springer-Verlag Berlin Heidelberg, 1982.

[6] Maillet, E.: Sur la decomposition d'un nombre entier en une somme de cubes d'entiers positifs. *Assoc. Franç. Bordeaux,* XXIV: 242-247, 1895

[7] Legendre, A.-M. *Essai sur la theorie des nombres.* Duprat, Paris, 1798.

[8] Wieferich, A.: Beweis des Satzes, daß sich eine jede ganze Zahl als Summe von höchstens neun positiven Kuben darstellen läßt. *Math. Ann.,* vol 66 (1909) 95-101.

[9] Landau, L. *Mathematische Annalen,* vol. 66 (1909), pp. 102-5;

[10] Baer, W. S.: Uber die Zerlegung der ganzen Zahlen in sieben Kuben, *Math. Ann.*, 74(4): 511-514, 1913.

[11] Dickson, L. E.: All integers except 23 and 239 are sums of eight cubes. *Bull. Amer. Math. Soc.*, 45: 588-591, 1939.

[12] Linnik, U. V.: On the representation of large numbers as sums of seven cubes, *Rec. Math. [Mat. Sbornik] N.S.*, 1943, Volume 12(54), Number 2, 218-224.

[13] McCurley, K. S.: An effective seven cube theorem. *J. Number Theory,* 19(2):176-183, 1984.

[14] Siksek, S.: Every integer greater than 454 is the sum of at most seven positive cubes. *Algebra Number Theory* 10 (2016) 2093-2119.

[15] Jacobi, C. G. J.: Uber die zusammensetzung der zahlen aus ganzen positiven cuben; nebst einer tabelle fr die kleinste cubenanzahl, aus welcher jede zahl bis 12000 zusammengesetzt werden kann. *Journal für die reine und angewandte Mathematik*, XLII, 1851.

[16] Hardy, G. H., and Littlewood, J. E.: Some problems of 'Partitio numerorum'; I: A new solution of Waring's problem. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse,* 1920 (1920): 33-54.

[17] Vinogradov, I. M.: The upper bound for $G(n)$ in Waring's problem, *Izv. Akad. Nauk SSSR Ser. Phiz.-Matem.* 10 (1934), 1455-1469.

[18] Heilbronn, H.: Über das Waringsche Problem, *Acta Arith. 1* (1936), 212-221.

[19] Vinogradov, I. M.: The method of trigonometrical sums in the theory of numbers, *Trav. Inst. Math. Stekloff* 23 (1947), 109 pp.

[20] Tong, K.-C.: On Waring's problem, *Advancement in Math.* 3 (1957), 602-607.

[21] Chen, J.-R. On Waring's problem for n-th powers, *Acta Math. Sinica* 8 (1958), 253-257.

[22] Vinogradov, I. M. *Izv.Akad. Nauk SSSR, ser. mat.*, 42,751-62.

[23] Davenport, H.: On Waring's Problem for Fourth Powers. *Annals of Mathematics* Second Series, Vol. 40, No. 4 (Oct., 1939), pp. 731-747.

[24] Kubina, J. M. and Wunderlich, M. C.: Extending Waring's Conjecture to 471600000. *Math. Comput.* 55, 815-820, 1990.

[25] Mahler, K.: On the Fractional Parts of the Powers of a Rational Number (II). *Mathematica* 4, 122-124, 1957.

[26] Mann, H. B.: A Proof of the Fundamental Theorem on the Density of Sets of Positive Integers. *Ann. Math.* 43, 523-527, 1942.