EL MÉTODO CIRCULAR EN EL PROBLEMA DE WARING

Victor García

septiembre de 2005

Índice general

Introducción

Los *problemas aditivos*, acaso por su sencilla naturaleza, aparecen en muchas ramas de la matemática. Para la *teoría analítica de los números* el proceso de resolver *problemas aditivos* ha sido eje en el desarrollo de importantes técnicas en la materia. Dos ejemplos clásicos son:

El problema de Goldbach.

Hacia 1772, en sus misivas con Leonhard Euler, Christian Goldbach conjeturó que todo entero par, mayor o igual que 2, es una suma de dos números primos y que todo entero mayor que 2 es la suma de tres números primos. Goldbach consideró a 1 como un primo, por esta razón hoy en día los problemas de Goldbach corresponden a las afirmaciones: todo entero par, mayor o igual que 4 se escribe como suma de dos primos (problema binario de Goldbach) y todo entero impar, mayor o igual que 7 es una suma de tres números primos (problema ternario de Goldbach).

En los años 1922, 1923, Hardy y Littewood [3], [4], utilizando el *método circular* (Hardy-Littlewood-Ramanujan) y asumiendo la hipótesis de Riemann [1], probaron que todo impar suficientemente grande es, efectivamente, la suma de tres números primos y que “casi todos” los pares se escriben como la suma de dos primos. En 1937, Vinogradov [12] utilizó esencialmente el *método circular* bajo sus técnicas de *sumas trigonométricas* para demostrar los mismos resultados incondicionalmente, es decir, sin depender de la hipótesis de Riemann.

[1] La hipótesis de Riemann afirma que; para la prolongación analítica de la función $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ al plano complejo agujereado $\mathbb{C}\backslash\{1\}$, todos los ceros *no triviales* se encuentran en la linea $\Re(s) = \frac{1}{2}$.

El problema de Waring.

En su libro titulado *Meditationes Algebraicae* (1770) Edward Waring afirmó, sin demostración, que todo entero positivo es suma de cuatro cuadrados, nueve cubos, diecinueve potencias de cuatro y así sucesivamente. En suma, el problema de Waring consiste en probar que dado $n \geq 2$ existe un entero $k = k(n)$ tal que cualquier entero positivo se puede escribir a lo más como la suma de k potencias enésimas no negativas. Es natural preguntarse que tan pequeño puede ser $k = k(n)$. Denotemos por $g(n)$ al mínimo k que satisface las condiciones del problema de Waring.

El problema de Waring quizá tiene su origen en la cuestión acerca de la representabilidad de cualquier entero como suma de cuadrados. Fué en 1770 cuando Lagrange probó que, ciertamente, todo entero positivo se puede escribir como suma de cuatro cuadrados. También prueba, en el mismo año, que, salvo los enteros de la forma $4^n(8t + 7)$, todo entero se escribe como la suma de 3 cuadrados y así probó que $g(2) = 4$.

Junto con el resultado de Lagrange, hasta antes del uso del *método circular*, se tuvieron avances en el problema de Waring sólo para valores pequeños de n. En 1909, Wieferich y Kempner probaron que $g(3) = 9$. Hacia 1859, Liouville probó que $g(4) \leq 53$. Para $n = 5$, Meillet en 1896 demostró $g(5) \leq 192$ y posteriormente en 1909 Wieferich estableció que $g(5) \leq 59$.

Finalmente en 1909, mediante un complicado argumento de combinatoria basado en identidades algebraicas, Hilbert [5] demuestra la existencia de $g(n)$ y con ello una solución general para el problema de Waring. Poco después, a principios de 1920, Hardy y Littlewood [2], haciendo uso del *método circular*, probaron que dado n todo entero positivo suficientemente grande se puede escribir a lo más como la suma de $n2^{n-1} + 1$ potencias enésimas, además de exhibir una fórmula asintótica para el número de soluciones de ésta expresión.

I.M. Vinogradov, en 1928 [11], retomando el *método circular*, y utilizando sus técnicas, las *sumas trigonométricas*, demostró con elegancia y brevedad la solubilidad del problema de Waring al exhibir una expresión asintótica para el numero de representaciones de $N \geq N_0$ como suma de potencias enésimas.

De manera similar a $g(n)$ nos podemos preguntar por el mínimo k, digamos $G(n)$, tal que todo entero suficientemente grande se escriba, exactamente, como la suma de k potencias de n. El resultado de Lagrange para la suma de cuadrados establece que $G(2) = 4$. Para $n = 3$, Linnik en 1943 [9] probó que $G(3) \leq 7$ y un argumento en congruencias módulo 9 prueba que existe una cantidad infinita de enteros positivos que no son suma de 3 cubos, así $4 \leq G(3) \leq 7$. En 1939 Davenport probó que $G(4) = 16$ [1]. Para el caso general, Vinogradov en 1937 ([7], Cap. XI §3.), obtuvo una estimación superior, hasta hoy no mejorada, para el orden de $G(n)$

$$G(n) \ll n \log n.$$

De hecho, los trabajos de Vinogradov [13] muestran estimaciones más precisas. Será hasta el segundo capítulo cuando demos mayores detalles referentes al estudio de $G(n)$.

Antes de hacer una descripción a grandes razgos del *método circular*, es preciso notar que una cantidad considerable de *problemas aditivos* pueden ser escritos de la manera siguiente.

Sea k un entero positivo, $\mathcal{N}$ un subconjunto de los enteros positivos y sean $\mathcal{X}_1, \ldots, \mathcal{X}_k$ subconjuntos de los enteros no negativos. El problema es demostrar que cualquier $N \in \mathcal{N}$ se puede escribir en la forma

$$x_1 + \cdots + x_k = N, \tag{1}$$

con

$$x_1 \in \mathcal{X}_1, \ldots, x_k \in \mathcal{X}_k.$$

De aquí, con la notación establecida, los ejemplos mencionados pueden escribirse como:

a) El problema binario de Goldbach.

Tomemos $k = 2$, $\mathcal{N}$ el conjunto de los pares mayores o igual a 4, $\mathcal{X}_1 = \mathcal{X}_2 = \mathbb{P}$, $\mathbb{P} = \{2, 3, 5, 7, \ldots\}$ el conjunto de los números primos. El problema es probar que para todo $N \in \mathcal{N}$, ecuación

$$p_1 + p_2 = N,$$

tiene solución en los primos p_1, p_2.

b) El problema ternario de Goldbach.

Hagamos $k = 3$, $\mathcal{N}$ el conjunto de los impares mayores o igual que 7, $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{X}_3 = \mathbb{P}$. Ahora el problema es probar que la ecuación

$$p_1 + p_2 + p_3 = N,$$

es soluble para todo $N \in \mathcal{N}$, en los primos p_1, p_2, p_3.

c) El problema de Waring.

Dado $n \geq 2$, deseamos probar la existencia de un número $k = k(n)$ tal que al tomar $\mathcal{N}$ el conjunto de los enteros positivos y $\mathcal{X}_1 = \cdots = \mathcal{X}_k = \{0^n, 1^n, 2^n, 3^n, \ldots\}$ entonces la ecuación

$$z_1^n + \cdots + z_k^n = N, \tag{2}$$

es soluble en los enteros no negativos $z_1, \ldots, z_k$ para cada $N \in \mathcal{N}$.

En la *teoría analítica de los números* el *método circular* sirve para dar solución a una cantidad considerable de este tipo de problemas.

Para describir básicamente el *método circular*, bajo el punto de vista de las *sumas trigonométricas* de Vinogradov, retomemos (1) y denotemos por $J(k, N)$ al número de soluciones de esta expresión. Bajo las condiciones establecidas tiene lugar la igualdad:

$$J(k, N) = \sum_{\substack{x_1 \in \mathcal{X}_1 \\ x_1 \leq N}} \cdots \sum_{\substack{x_k \in \mathcal{X}_k \\ x_k \leq N}} \int_0^1 e^{2\pi i \alpha (x_1 + \cdots + x_k - N)} \, d\alpha.$$

Puesto que N es un parámetro positivo y fijo, la elección para cada uno de los enteros positivos $x_1, \ldots, x_k$ se toma sobre un conjunto finito. Luego

$$J(k, N) = \int_0^1 S_1(\alpha) \cdots S_k(\alpha) \, e^{-2\pi i \alpha N} \, d\alpha; \quad S_i(\alpha) = \sum_{x_i} e^{2\pi i \alpha x_i}, \ (1 \leq i \leq k).$$

El objeto fundamental del *método circular* consiste en hallar una expresión asintótica para $J(k, N)$; primero se divide el intervalo $[0, 1)$ en dos conjuntos ajenos E_1, E_2; posteriormente, tomando la integral J_1 sobre el conjunto E_1 se encuentra el término principal de $J(k, N)$ y finalmente se verifica que la integral, J_2, sobre E_2 es un término despreciable respecto de la parte principal conforme $N \to \infty$. La elección de los conjuntos E_1, E_2 está determinada por las propiedades aritméticas de aproximación mediante racionales para cualquier $\alpha \in [0, 1)$.

Este trabajo está enfocado en el estudio del problema de Waring en la siguiente forma: Para cada $n \geq 2$, todo entero suficientemente grande se puede escribir como la suma de $2^n + 1$ potencias enésimas mayores que cero.

Usando el *método circular*, en la forma de las *sumas trigonométricas*, será exhibida una expresión asintótica para el número de soluciones $J(n,k,N)$ de (2) tal que $J(n,k,N) > 0$ para todo $N \geq N_0$, donde N_0 depende sólo de n.

CAPÍTULO 1

Preliminares

Este capítulo tiene por objeto presentar una serie de resultados que serán utilizados en el segundo capítulo, la mayoría de ellos demostrados con técnicas de *sumas trigonométricas*.[1]

1.1. Notación

A lo largo del trabajo se indicará el sentido de las letras diversamente empleadas, ya sean constantes o variables (digamos $a, b, c, x, y, w, \alpha, \beta, \ \ldots$). Sin embargo, es importante mencionar que todo el tiempo tomaremos a p como un número primo; también aparecerá con frecuencia N_0, que entendemos por un número fijo suficientemente grande y por otra parte ε siempre denotará a un número mayor que cero tan pequeño como sea preciso, ε no representará necesariamente la misma cantidad en esta tesis.

La notación $f(x) = O(g(x))$, al igual que $f(x) \ll g(x)$ ($\ll$ es conocido como el símbolo de Vinogradov), se entiende como la existencia de una constante c, tal que

$$|f(x)| \leq c\, g(x),$$

[1] Para su estudio básico y muy serio pueden consultarse [14] y ([6] Cap. 7)

cuando $x \to \infty$ y $g(x) \geq 0$.

Dado un número primo p, daremos por hecho la existencia de alguna *raíz primitiva* módulo p. Es decir, la existencia de un número g tal que la mínima potencia positiva δ que satisface

$$g^{\delta} \equiv 1 \pmod{p},$$

es precisamente $\delta = p - 1$.

Para un entero positivo n, la función $\tau(n)$ representa el número de divisores positivos de n. Es decir

$$\tau(n) = \sum_{d|n} 1.$$

Daremos por hecho que para cualquier ε se cumple la estimación $\tau(n) \ll n^{\varepsilon}$.

1.2. Resultados básicos

Es preciso mencionar que los siguientes lemas, en su mayoría, son independientes entre sí. Será hasta el segundo capítulo donde, al ser invocados, veremos su importancia.

Lema 1.2.1. *Sean $m \geq 2$ y a enteros. Entonces*

$$\frac{1}{m} \sum_{x=0}^{m-1} e^{2\pi i \frac{a}{m} x} = \begin{cases} 1 & si \;\; a \equiv 0 \pmod{m}, \\ 0 & si \;\; a \not\equiv 0 \pmod{m}. \end{cases}$$

Demostración. Si $a \equiv 0 \pmod{m}$ la igualdad es evidente. En caso contrario se tiene

$$\sum_{x=0}^{m-1} e^{2\pi i \frac{a}{m} x} = \frac{\left\{e^{2\pi i \frac{a}{m}}\right\}^m - 1}{e^{2\pi i \frac{a}{m}} - 1} = 0$$

de donde obtenemos el resultado. □

Lema 1.2.2. *Sean $n \geq 2$ y*

$$S(a,q) = \sum_{x=1}^{q} e^{2\pi i \frac{a}{q} x^n}, \qquad (a,q) = 1.$$

Entonces, es válida la desigualdad

$$|S(a,q)| \;\leq\; e^{\frac{1}{6}(1+o(1))n^6}\, q^{1-1/n}.$$

Demostración. Sean q_1, q_2 enteros positivos primos relativos tales que $q_1 q_2 = q > 1$. Entonces la expresión $s_1\, q_2 + s_2\, q_1$ recorre el sistema completo de residuos módulo q cuando s_1 recorre el sistema completo de residuos módulo q_1 y s_2 el sistema completo de residuos módulo q_2. Luego

$$\begin{aligned}
S(a,q) &= S(a,q_1q_2) = \sum_{s_1=1}^{q_1}\sum_{s_2=1}^{q_2} e^{2\pi i \frac{a}{q_1q_2}(s_1q_1+s_2q_2)^n} \\
&= \sum_{s_1=1}^{q_1}\sum_{s_2=1}^{q_2} e^{2\pi i \frac{aq_2^{n-1}}{q_1}s_1^n} e^{2\pi i \frac{aq_1^{n-1}}{q_2}s_2^n} \\
&= \sum_{s_1=1}^{q_1} e^{2\pi i \frac{aq_2^{n-1}}{q_1}s_1^n} \sum_{s_2=1}^{q_2} e^{2\pi i \frac{aq_1^{n-1}}{q_2}s_2^n} \\
&= S(aq_2^{n-1},q_1)\, S(aq_1^{n-1},q_2) \;=\; S(a_1,q_1)S(a_2,q_2) \qquad (1.1)
\end{aligned}$$

En consecuencia, si $q = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ es la descomposición canónica de q como producto de primos se tiene:

$$S(a,q) \;=\; S(a_1,p_1^{\alpha_1}) \,\cdots\, S(a_r,p^{\alpha_r}), \qquad (1.2)$$

donde $(a_1,p_1) = \cdots = (a_r,p_r) = 1$. Por esta razón investigaremos qué sucede con $S(a,p^\alpha)$.

Supongamos $n \geq 3$ y $\alpha = 1$. Entonces

$$S(a,p) = \sum_{x=0}^{p-1} e^{2\pi i \frac{a}{p}x^n} = \sum_{x=0}^{p-1} e^{2\pi i \frac{a}{p}(xy)^n}, \qquad 1 \leq y \leq p-1.$$

Sumando sobre y, desde 1 a $p-1$ y utilizando la desigualdad de *Cauchy-Schwartz*

$$\begin{aligned}
(p-1)|S(a,p)| &= \left|\sum_{y=1}^{p-1}\sum_{x=0}^{p-1} e^{2\pi i \frac{a}{p} x^n y^n}\right| = \left|\sum_{l=1}^{p-1}\sum_{s=0}^{p-1} \nu(l)\nu(s) e^{2\pi i \frac{a}{p} l\, s}\right| \\
&\leq \left(\sum_{l=1}^{p-1} |\nu(l)|^2\right)^{1/2} \left(\sum_{l=1}^{p-1}\left|\sum_{s=0}^{p-1} \nu(s) e^{2\pi i \frac{a}{p} l\, s}\right|^2\right)^{1/2} \\
&= \left(\sum_{l=0}^{p-1} |\nu(l)|^2\right)^{1/2} \left(\sum_{0\leq s_1,s_2\leq p-1} \nu(s_1)\overline{\nu(s_2)} \sum_{l=0}^{p-1} e^{2\pi i \frac{a}{p} l(s_1-s_2)} \,-\, p^2\right)^{1/2} \\
&= \sqrt{p}\left(\sum_{l=0}^{p-1} |\nu(l)|^2\right)^{1/2} \left(\sum_{l=0}^{p-1} |\nu(l)|^2 \,-\, p\right)^{1/2},
\end{aligned}$$

donde $\nu(t)$ es el número de soluciones de

$$x^n \equiv t \pmod p; \qquad 0 \leq x \leq p-1,$$

para t fijo. Por tanto $\nu(0) = 1$ y $\nu(l) \leq n$ si $l \neq 0$. Con esto y el hecho de que

$$\sum_{l=0}^{p-1} |\nu(l)|^2,$$

es el número de soluciones de la congruencia

$$x^n \equiv y^n \pmod p; \qquad 0 \leq x, y \leq p-1,$$

deducimos

$$\sum_{l=0}^{p-1} |\nu(l)|^2 \leq 1 + n(p-1).$$

De esta forma se tiene

$$\begin{aligned}
(p-1)|S(a,p)| &\leq \sqrt{p}\left(\sum_{l=0}^{p-1} |\nu(l)|^2\right)^{1/2} \left(\sum_{l=0}^{p-1} |\nu(l)|^2 \,-\, p\right)^{1/2} \\
&\leq \sqrt{p}\,\{(p-1)(n-1)(1+n(p-1))\}^{1/2} \\
&< \sqrt{p}(p-1)n.
\end{aligned}$$

Por tanto obtenemos
$$|S(a,p)| \ < \ n\sqrt{p}.$$

Supongamos ahora $n \geq 3, \ 1 < \alpha \leq n$ y además $(n,p) = 1$. Entonces

$$\begin{aligned}
S(a,p^\alpha) &= \sum_{x=0}^{p-1}\sum_{y=1}^{p^{\alpha-1}} e^{2\pi i a\frac{(xp^{\alpha-1}+y)^n}{p^\alpha}} = \sum_{x=0}^{p-1}\sum_{y=1}^{p^{\alpha-1}} e^{2\pi i a\frac{(nxp^{\alpha-1}y^{n-1}+y^n)}{p^\alpha}} \\
&= \sum_{y=1}^{p^{\alpha-1}} e^{2\pi i a\frac{y^n}{p^\alpha}} \sum_{x=0}^{p-1} e^{2\pi i a\frac{nxy^{n-1}}{p}} = p \sum_{\substack{y=1 \\ y\equiv 0 \pmod p}}^{p^{\alpha-1}} e^{2\pi i a\frac{y^n}{p^\alpha}} \\
&= p\sum_{y=1}^{p^{\alpha-2}} e^{2\pi i a y^n p^{n-\alpha}} = p^{\alpha-1}.
\end{aligned}$$

Si ocurre $n > \alpha$ y τ satisface $n = p^\tau n_1$ con $(n, n_1) = 1$ resulta

$$\begin{aligned}
S(a,p^\alpha) &= \sum_{x=0}^{p^{\tau+1}-1}\sum_{y=1}^{p^{\alpha-(\tau+1)}} e^{2\pi i a\frac{(xp^{\alpha-(\tau+1)}+y)^n}{p^\alpha}} \\
&= \sum_{x=0}^{p^{\tau+1}-1}\sum_{y=1}^{p^{\alpha-(\tau+1)}} e^{2\pi i a\frac{(nxp^{\alpha-(\tau+1)}y^{n-1}+y^n)}{p^\alpha}} \\
&= \sum_{y=1}^{p^{\alpha-(\tau+1)}} e^{2\pi i a\frac{y^n}{p^\alpha}} \sum_{x=0}^{p^{\tau+1}-1} e^{2\pi i a\frac{n_1xy^{n-1}}{p}} \\
&= p^\tau \sum_{y=1}^{p^{\alpha-(\tau+1)}} e^{2\pi i a\frac{y^n}{p^\alpha}} \sum_{x=0}^{p-1} e^{2\pi i a\frac{n_1xy^{n-1}}{p}} \\
&= p^{\tau+1} \sum_{\substack{y=1 \\ y\equiv 0 \pmod p}}^{p^{\alpha-(\tau+1)}} e^{2\pi i a\frac{y^n}{p^\alpha}} = p^{\tau+1}\sum_{y=1}^{p^{\alpha-(\tau+2)}} e^{2\pi i a\frac{y^n}{p^{\alpha-n}}} \\
&= p^{\tau+1}p^{n-(\tau+2)}\sum_{y=1}^{p^{\alpha-n}} e^{2\pi i a\frac{y^n}{p^{\alpha-n}}} \\
&= p^{n-1}S(a,p^{\alpha-n}).
\end{aligned}$$

Introduzcamos la función

$$T(a,q) = q^{-(1-1/n)}S(a,q)$$

y, en base a los cálculos anteriores, tendremos algunas estimaciones para $T(a,p^\alpha)$.

Si $1 \leq \alpha \leq n$ y $(n,p) = p$, tomando una estimación trivial tenemos:

$$T(a,p^\alpha) = p^{-\alpha(1-1/n)}S(a,p^\alpha) \leq p^{\alpha/n} \leq p \leq n.$$

Para $\alpha = 1$ y $(n,p) = 1$, obtenemos

$$T(a,p) = p^{-(1-1/n)}S(a,p) < np^{-1/2+1/n} \leq np^{-1/6}.$$

En el caso $1 < \alpha \leq n$ con $(n,p) = 1$,

$$T(a,p^\alpha) = p^{-\alpha(1-1/n)}S(a,p^\alpha) = p^{-\alpha(1-1/n)}p^{\alpha-1} = p^{\alpha/n-1} \leq 1.$$

Así, cuando $1 \leq \alpha \leq n$ resulta

$$T(a,p^\alpha) \leq \begin{cases} n, & \text{si } p \leq n^6 \\ 1, & \text{si } p > n^6. \end{cases}$$

Si $\alpha > n$ se tiene

$$\begin{aligned} T(a,p^\alpha) &= p^{-\alpha(1-1/n)}S(a,p^\alpha) = p^{-\alpha(1-1/n)}p^{n-1}S(a,p^{\alpha-n}) \\ &= p^{(\alpha-n)(1-1/n)}S(a,p^{\alpha-n}) = T(a,p^{\alpha-n}). \end{aligned}$$

Luego, escribamos $\alpha = nl + s$ para ciertos enteros l y s con $1 \leq s \leq n$. Aplicando l veces el argumento anterior tenemos

$$T(a,p^\alpha) = T(a,p^s),$$

reduciendo el problema al caso antes estudiado.

Finalmente, si $q = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, según (1.2) y la estimación para $T(a,p^\alpha)$, tenemos

$$\begin{aligned} S(a,q)q^{-(1-1/n)} &= S(a_1,p_1^{\alpha_1})p_1^{-\alpha_1(1-1/n)} \cdots S(a_r,p_r)p_r^{-\alpha_r(1-1/n)} \\ &= T(a_1,p_1^{\alpha_1}) \cdots T(a_t,p_t^{\alpha_t}) \leq n^{\pi(n^6)}. \end{aligned}$$

El lema ha sido probado para $n \geq 3$.

Si $n=2$, comencemos estimando $S(a,p^\alpha)$ suponiendo $p\neq 2$. En este caso

$$\begin{aligned}
|S(a,p^\alpha)|^2 &= \sum_{x=0}^{p^\alpha-1}\sum_{y=0}^{p^\alpha-1} e^{2\pi i\frac{a}{p^\alpha}(y^2-x^2)} = \sum_{x=0}^{p^\alpha-1}\sum_{t=0}^{p^\alpha-1} e^{2\pi i\frac{a}{p^\alpha}(2xt+t^2)}\\
&= \sum_{t=1}^{p^\alpha} e^{2\pi i\frac{a}{p^\alpha}t^2}\sum_{x=0}^{p^\alpha-1} e^{2\pi i\frac{a}{p^\alpha}2xt}\\
&= \sum_{\substack{t=1\\ t\equiv 0 \pmod p}}^{p^\alpha} e^{2\pi i\frac{a}{p^\alpha}t^2}\sum_{x=0}^{p^\alpha-1} e^{2\pi i\frac{a}{p^\alpha}2xt}.
\end{aligned}$$

Luego, si $t=p^\tau t_1$ con $(t,t_1)=1$ se tiene

$$\sum_{x=0}^{p^\alpha-1} e^{2\pi i\frac{a}{p^\alpha}2xt} = \sum_{x=0}^{p^\alpha-1} e^{2\pi i\frac{a}{p^{\alpha-\tau}}2xt_1} = 0$$

sólo si $\tau<\alpha$. Entonces

$$|S(a,p^\alpha)|^2 = \sum_{\substack{t=1\\ t\equiv 0 \pmod p}}^{p^\alpha} e^{2\pi i\frac{a}{p^\alpha}t^2}\sum_{x=0}^{p^\alpha-1} e^{2\pi i\frac{a}{p^\alpha}2xt} = p^\alpha,$$

y obtenemos

$$|S(a,p^\alpha)| = p^{\alpha/2}.$$

En el caso $p=2$ es claro que $S(a,2^\alpha)=0$ para $\alpha=1$. Tomemos entonces $\alpha>1$. En este caso se sigue que

$$\begin{aligned}
|S(a,2^\alpha)|^2 &= \sum_{x=0}^{2^\alpha-1}\sum_{y=0}^{2^\alpha-1} e^{2\pi i\frac{a}{2^\alpha}(y^2-x^2)} = \sum_{x=0}^{2^\alpha-1}\sum_{t=0}^{2^\alpha-1} e^{2\pi i\frac{a}{2^\alpha}(2xt+t^2)}\\
&= \sum_{t=1}^{2^\alpha} e^{2\pi i\frac{a}{2^\alpha}t^2}\sum_{x=0}^{2^\alpha-1} e^{2\pi i\frac{a}{2^{\alpha-1}}xt}\\
&= 2\sum_{\substack{t=1\\ t\equiv 0 \pmod 2}}^{2^\alpha} e^{2\pi i\frac{a}{2^\alpha}t^2}\sum_{x=0}^{2^{\alpha-1}-1} e^{2\pi i\frac{a}{2^{\alpha-1}}xt},
\end{aligned}$$

donde, nuevamente, si $t = 2^\tau t_1$ con $(t_1, 2) = 1$ y $\tau > 0$, se tiene

$$\sum_{x=0}^{2^{\alpha-1}-1} e^{2\pi i \frac{a}{2^{\alpha-1}} xt} = \sum_{x=0}^{2^{\alpha-1}-1} e^{2\pi i \frac{a}{2^{\alpha-1-\tau}} xt_1} = 0$$

cuando $\tau < \alpha - 1$. En los dos casos restantes dicha suma es igual con $2^{\alpha-1}$ por lo que

$$|S(a, 2^\alpha)|^2 = 2 \sum_{\substack{t=1 \\ t \equiv 0 \pmod p}}^{2^\alpha} e^{2\pi i \frac{a}{p^\alpha} t^2} \sum_{x=0}^{p^{\alpha-1}-1} e^{2\pi i \frac{a}{p^{\alpha-1}} xt} = 2(2^{\alpha-1} + 2^{\alpha-1}) = 2^{\alpha+1}.$$

De esta manera, se tiene

$$|S(a, 2^\alpha)| = \sqrt{2}\, 2^{\alpha/2}$$

Finalmente, en virtud de (1.2), para $q = 2^\alpha p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ concluimos

$$S(a, q) \leq \sqrt{2}\, 2^{\alpha/2} p_1^{\alpha/2} \cdots p_t^{\alpha/2} = \sqrt{2} q^{1-1/2},$$

cumpliendo lo establecido por el lema. □

Lema 1.2.3. *Para $z \in \mathbb{R}$ se tiene*

$$\int_0^1 e^{2\pi i z x^n}\, \mathrm{d}x \ll \text{mín} \left\{1, |z|^{-1/n}\right\}$$

Demostración. Supongamos que $z > 1$. Al hacer el cambio $u = zx^n$ y observando que

$$\left| \int_0^1 u^{-1+1/n} e^{2\pi i u}\, \mathrm{d}u \right| \leq \int_0^1 u^{-1+1/n}\, \mathrm{d}u \; = \; n,$$

tenemos

$$\begin{aligned}
\int_0^1 e^{2\pi i z x^n}\,\mathrm{d}x &= \frac{1}{n} z^{-1/n} \int_0^z u^{-1+1/n} e^{2\pi i u}\,\mathrm{d}u \\
&= \frac{1}{n} z^{-1/n} \int_0^1 u^{-1+1/n} e^{2\pi i u}\,\mathrm{d}u + \frac{1}{2\pi i n} z^{-1/n} \int_1^z u^{-1+1/n}\,\mathrm{d}\, e^{2\pi i u} \\
&= \frac{1}{n} z^{-1/n} \int_0^1 u^{-1+1/n} e^{2\pi i u}\,\mathrm{d}u + \frac{1}{2\pi i n} z^{-1/n} \quad \times \\
& \quad \times \left\{ u^{-1+1/n} e^{2\pi i u}\, \Big|_{u=1}^{z} + \left(1 - \frac{1}{n}\right) \int_1^z u^{-2+1/n} e^{2\pi i u}\,\mathrm{d}u \right\} \\
&\ll z^{-1/n}.
\end{aligned}$$

Para $|z| \leq 1$, tomemos la estimación trivial para finalmete obtener:

$$\int_0^1 e^{2\pi i z x^n}\,\mathrm{d}x \ll \min\left\{1, |z|^{-1/n}\right\}. \ \square$$

Lema 1.2.4. *Para* $\alpha > 0$, $k \in \mathbb{Z}$ *y* $P \geq 1$ *fijo, se tiene:*

$$\sum_{1 \leq x \leq P} e^{2\pi i \alpha k x} \ll \min\left\{P, \frac{1}{\|\alpha k\|}\right\},$$

siendo $\|x\| = \min(\{x\}, 1 - \{x\})$, *el entero más cercano a* $x > 0$.

Demostración. Supongamos que αk no es un entero, entonces

$$\begin{aligned}
\left| \sum_{x=1}^{P} e^{2\pi i \alpha k x} \right| &= \frac{|e^{2\pi i \alpha k P} - 1|}{|e^{2\pi i \alpha k} - 1|} = \frac{|\operatorname{sen} \pi \alpha k P|}{|\operatorname{sen} \pi \alpha k|} \\
&\leq \frac{1}{|\operatorname{sen} \pi \alpha k|}.
\end{aligned}$$

Por otra parte, sabemos que $|\operatorname{sen}\pi x| \geq \|x\|$. De esta forma concluimos

$$\sum_{x=1}^{P} e^{2\pi i\alpha kx} \ll \text{mín}\left\{P, \frac{1}{\|\alpha k\|}\right\}. \ \square$$

Teorema 1.2.1. (*Dirichlet*) .
Sean $\alpha > 0$ *y* $\tau > 1$ *fijos. Entonces existen enteros primos relativos* a, q *con* $1 \leq q \leq \tau$ *tales que*

$$\alpha \ = \ \frac{a}{q} + \frac{\theta}{q\tau}, \quad \text{con} \quad |\theta| \leq 1.$$

Demostración. Sin perder generalidad podemos suponer que $\alpha < 1$. De esta manera consideremos al conjunto $\{\alpha m\}$, para $m = 0, \ldots, [\tau]$ y dividamos al intervalo $[0, 1]$ en $[\tau] + 1$ secciones uniformes de longitud $\frac{1}{[\tau]+1}$. Supongamos que $\{\alpha m\} \geq \frac{[\tau]}{[\tau]+1}$ para algún m, así

$$|\alpha m - ([\alpha m] + 1)| \leq \frac{1}{[\tau] + 1} < \frac{1}{\tau}; \tag{1.3}$$

en este caso tomemos $q_1 = m$ y $a_1 = [\alpha m] + 1$. Por el contrario, si los $[\tau] + 1$ números, $\{\alpha m\}$, sólo están distribuidos en los intervalos

$$\left[0, \frac{1}{[\tau] + 1}\right), \ldots, \left[\frac{[\tau] - 1}{[\tau] + 1}, \frac{[\tau]}{[\tau] + 1}\right),$$

existen enteros m_1 y m_2 con $0 \leq m_1 < m_2 \leq [\tau]$ que satisfacen

$$|\{m_2\alpha\} - \{m_1\alpha\}| = |\alpha(m_2 - m_1) - ([\alpha m_2] - [\alpha m_1])| \leq \frac{1}{[\tau] + 1} < \frac{1}{\tau}, \tag{1.4}$$

llamemos $q_1 = (m_2 - m_1)$, $a_1 = [\alpha m_2] - [\alpha m_1]$.

Notemos que en ambos casos $q_1 \leq \tau$. Así, dividiendo las desigualdades (1.3) y (1.4) por q_1 y tomando la fracción reducida $\frac{a}{q} = \frac{a_1}{q_1}$ obtenemos

$$\alpha - \frac{a}{q} = \frac{\theta}{q\tau}, \quad (a, q) = 1, \ q \leq \tau, \ |\theta| \leq 1. \ \square$$

Observe que, en particular, para cada $\alpha \in \mathbb{R}$ existen enteros a y q con $(a, q) = 1$, $q \geq 1$ tales que

$$\alpha - \frac{a}{q} = \frac{\theta}{q^2}, \qquad |\theta| \leq 1.$$

Lema 1.2.5. *Sean α, β, números reales. Entonces es válida la siguente estimación*

$$\sum_{N<k\leq N+M} \min\left\{P, \frac{1}{\|\alpha k + \beta\|}\right\} \leq 5\left(\frac{M}{q} + 1\right)(\, P + q\log q\,)\,,$$

donde

$$\alpha = \frac{a}{q} + \frac{\theta}{q^2}, \quad (a, q) = 1, \ |\theta| \leq 1.$$

Demostración. Podemos suponer que $0 < \alpha < 1$. Escribiendo $k = qt + r$ con $1 \leq t \leq M/q + 1$, $1 \leq r \leq q$ tenemos

$$\begin{aligned}
\sum_{N<k\leq N+M} \min\left\{P, \frac{1}{\|\alpha k + \beta\|}\right\} &\leq \sum_{t=1}^{\frac{M}{q}+1} \sum_{r=1}^{q} \min\left\{P, \frac{1}{\|\alpha(qt + r + N) + \beta\|}\right\} \\
&\leq \left(\frac{M}{q} + 1\right) \max_{1\leq t\leq M/q+1} \sum_{r=1}^{q} \min\left\{P, \frac{1}{\|\alpha(qt + r + N) + \beta\|}\right\} \\
&\leq \left(\frac{M}{q} + 1\right) \sum_{r=1}^{q} \min\left\{P, \frac{1}{\|\alpha r + \beta_1\|}\right\}. \qquad (1.5)
\end{aligned}$$

Por otra parte, escribiendo $\beta_1 = \frac{[q\beta_1]+\{q\beta_1\}}{q}$ tenemos

$$\alpha r + \beta_1 = \frac{ar + [q\beta_1]}{q} + \frac{\theta r + q\{q\beta_1\}}{q^2}.$$

Puesto que $(a, q) = 1$ la expresión $y = ar + [q\beta_1]$ recorre el sistema de residuos módulo q a la vez que r. También es posible escribir $\theta r + q\{q\beta_1\}$ en términos de y, pues a pertenece al sistema reducido de residuos módulo

q; $\theta r + q\{q\beta_1\} = \theta a^{-1}(y - [q\beta_1]) + q\{q\beta_1\} = \theta'(y)$, donde $|\theta'(y)| < 2q$. De esta forma:

$$\sum_{r=1}^{q} \text{mín}\left\{P, \frac{1}{\|\alpha r + \beta_1\|}\right\} = \sum_{|y|\le q/2} \text{mín}\left\{P, \frac{1}{\|\frac{y+\theta''}{q}\|}\right\},$$

con $|\theta''| = \left|\frac{\theta'(y)}{q}\right| < 2$. Supongamos que $2 < |y| \le q/2$, entonces

$$0 < \frac{|y|-2}{q} < \frac{|y|+\theta''}{q} \le \frac{1}{2} + \frac{\theta''}{q} < 1,$$

pues $\theta''/q < 1/2$. De ésta forma $\frac{|y|+\theta''}{q} = \|\frac{y+\theta''}{q}\|$ y así

$$0 < \frac{|y|-2}{q} < \left\|\frac{y+\theta''}{q}\right\|,$$

luego

$$\begin{aligned}
\sum_{|y|\le q/2} \text{mín}\left\{P, \frac{1}{\|\frac{y+\theta''}{q}\|}\right\} &\le \sum_{|y|\le 2} \text{mín}\left\{P, \frac{1}{\|\frac{y+\theta''}{q}\|}\right\} + \sum_{2<|y|\le q/2} \frac{1}{\|\frac{y+\theta''}{q}\|} \\
&\le 5P + 2q \sum_{2<y\le q/2} \frac{1}{y-2} \\
&\le 5P + 4q\log q \\
&\le 5(P + q\log q).
\end{aligned}$$

Por último, de (1.5), se obtiene:

$$\sum_{N<k\le N+M} \text{mín}\left\{P, \frac{1}{\|\alpha k + \beta\|}\right\} \le 5\left(\frac{M}{q} + 1\right)(P + q\log q). \ \square$$

Teorema 1.2.2. (*Van der Corput*).

Si $f(x)$ *es una función real, continuamente diferenciable en el intervalo* $[a, b]$, *cuya derivada es monótona y además*

$$|f'(x)| \le \delta < 1.$$

Entonces

$$\sum_{a<n\le b} e^{2\pi i f(n)} = \int_a^b e^{2\pi i f(x)}\,\mathrm{d}x + O\left(\frac{1}{1-\delta}\right).$$

Demostración. Para n fijo tomemos

$$F_n(x) = e^{2\pi i f(n+x)}, \qquad 0 < x < 1.$$

Definamos a $F_n(x)$ en los puntos 0 y 1 como

$$F_n(0) = F_n(1) = \frac{e^{2\pi i f(n)} + e^{2\pi i f(n+1)}}{2},$$

y extendamos el dominio de la función a todos los reales de manera que $F_n(x)$ tenga periodo 1. Para cada $x \in \mathbb{R}$, $x = [x] + \{x\}$ tomemos

$$F_n(x) = F_n([x] + \{x\}) = F_n(\{x\}).$$

Utilizemos el siguiente resultado, que pertenece a la teoría de series de Fourier:

Sea $f(x)$ es una función con periodo 1 definida en los reales con, a lo más, un número finito de discontinuidades de primera especie en $[0,1]$ y, salvo discontinuidades, admite derivada continua en $[0,1]$. Entonces la serie de Fourier converge y es igual a $f(x)$ para todos los puntos donde sea continua; para los puntos x_0 de discontinuidad:

$$f(x_0) = \frac{1}{2}\left(\lim_{x\to x_0-0} f(x) + \lim_{x\to x_0+0} f(x)\right). \ \Box$$

Así, nuestra función admite una expansión en serie de *Fourier*

$$F_n(x) = \sum_{m=-\infty}^{\infty} c_m e^{2\pi i m x},$$

con

$$c_m = c_m(n) = \int_0^1 F_n(u) e^{-2\pi i m u}\,\mathrm{d}u, \ \ m \neq 0; \quad c_0 = \int_0^1 e^{2\pi i f(n+u)}\,\mathrm{d}u.$$

Luego, si $m \neq 0$

$$
\begin{aligned}
c_m(n) &= -\frac{1}{2\pi i m}\int_0^1 e^{2\pi i f(n+u)}\,\mathrm{d}\,e^{-2\pi i m u}\\
&= -\frac{e^{2\pi i f(n+u)}}{2\pi i m}e^{-2\pi i m u}\,\Big|_{u=0}^{1} + \frac{1}{m}\int_0^1 f'(n+u)e^{2\pi i(f(n+u)-mu)}\,\mathrm{d}u.\\
&= \frac{1}{2\pi i m}(e^{2\pi i f(n)} - e^{2\pi i f(n+1)}) + \frac{1}{m}\int_0^1 f'(n+u)e^{2\pi i(f(n+u)-mu)}\,\mathrm{d}u.
\end{aligned}
$$

Al evaluar en 1 se obtiene

$$
\begin{aligned}
F_n(1) &= \frac{e^{2\pi i f(n)} + e^{2\pi i f(n+1)}}{2}\\
&= \int_0^1 e^{2\pi i f(n+u)}\,\mathrm{d}u \; + \sum_{m\neq 0} c_m(n)\\
&= \int_0^1 e^{2\pi i f(n+u)}\,\mathrm{d}u \; + \sum_{m\neq 0}\frac{1}{m}\int_0^1 f'(n+u)e^{2\pi i(f(n+u)-mu)}\,\mathrm{d}u\\
&= \int_n^{n+1} e^{2\pi i f(u)}\,\mathrm{d}u \; + \sum_{m\neq 0}\frac{1}{m}\int_n^{n+1} f'(u)e^{2\pi i(f(u)-mu)}\,\mathrm{d}u.
\end{aligned}
$$

Sumando sobre aquellos enteros n que cumplan $a < n \leq b$, se tiene

$$
\begin{aligned}
\sum_{a<n\leq b} e^{2\pi i f(n)} &= \int_{[a]+1}^{[b]} e^{2\pi i f(u)}\,\mathrm{d}u + \sum_{m\neq 0}\frac{1}{m}U_m + \frac{e^{2\pi i f([a]+1)} + e^{2\pi i f([b])}}{2}\\
&= \int_a^b e^{2\pi i f(u)}\,\mathrm{d}u \; + \sum_{m\neq 0}\frac{1}{m}U_m \; + \; O(1),
\end{aligned}
$$

donde

$$
\begin{aligned}
U_m &= \int\limits_{[a]+1}^{[b]} f'(u)e^{2\pi i(f(u)-mu)}\,\mathrm{d}u = \frac{1}{2\pi i}\int\limits_{[a]+1}^{[b]} \frac{f'(u)}{f'(u)-m}\,\mathrm{d}\, e^{2\pi i(f(u)-mu)} \\
&= \frac{1}{2\pi}\int\limits_{[a]+1}^{[b]} \frac{f'(u)}{f'(u)-m}\,\mathrm{d}\,\operatorname{sen} 2\pi(f(u)-mu) \\
&\quad - i\frac{1}{2\pi}\int\limits_{[a]+1}^{[b]} \frac{f'(u)}{f'(u)-m}\,\mathrm{d}\,\cos 2\pi(f(u)-mu).
\end{aligned}
$$

Tenemos el siguiente teorema de la media:

Si $g(x)$, $h(x)$ son integrables por Riemman con $g(x)$ monótona en $[a,b]$, entonces existe $\xi \in [a,b]$ tal que

$$
\int\limits_a^b g(x)f(x)\,\mathrm{d}x = g(a)\int\limits_a^{\xi} h(x)\,\mathrm{d}x + g(b)\int\limits_{\xi}^{b} h(x)\,\mathrm{d}x. \ \square
$$

Aplicando este resultado a la parte real, siendo $\frac{f'(u)}{f'(u)-m}$ monótona, obtenemos

$$
\begin{aligned}
\frac{1}{2\pi}\int\limits_{[a]+1}^{[b]} \frac{f'(u)}{f'(u)-m}\,\mathrm{d}\,\operatorname{sen} 2\pi(f(u)-mu) &\ll \left|\frac{f'([b])}{f'([b])-m}\right| \\
&\ll \frac{1}{|m|-\delta}.
\end{aligned}
$$

Con un argumento similar, obtenemos la misma cota para la parte imaginaria de U_m. Por lo tanto,

$$\begin{aligned}
\sum_{a<n\le b} e^{2\pi i f(n)} &= \int\limits_a^b e^{2\pi i f(u)}\,\mathrm{d}u \;+\; O\left(\sum_{m>0}\frac{1}{m}\cdot\frac{1}{m-\delta}\right)\\
&= \int\limits_a^b e^{2\pi i f(u)}\,\mathrm{d}u \;+\; O\left(\sum_{m>0}\frac{1}{m^2}\cdot\frac{1}{1-\delta/m}\right)\\
&= \int\limits_a^b e^{2\pi i f(u)}\,\mathrm{d}u \;+\; O\left(\frac{1}{1-\delta}\right),
\end{aligned}$$

donde la constante de O es absoluta. $\square$

CAPÍTULO 2

El problema de Waring

El problema de Waring es la cuestión acerca de la representabilidad de cualquier natural N como suma de un número fijo de enteros de la misma potencia. En términos analíticos, es la solución en enteros $x_1, \ldots, x_n$ de la expresión

$$x_1^n + \cdots + x_k^n = N; \tag{2.1}$$

con $n \geq 2\,, k = k(n)\,,\ 0 \leq\ x_1, \ldots, x_n\ \leq N^{1/n}$.

En 1770 Waring afirma, sin demostración, que el problema es soluble para cierto número de sumandos k que sólo depende de la potencia dada. Fué hasta 1909 cuando Hilbert da la primer prueba para dicha afirmación [5].

En este capítulo, parte medular del trabajo, se demostrará la solubilidad del problema de Waring, al mostrar una expresión asintótica para $J(n, k, N)$, el número de soluciones de (2.1), para $2^n + 1$ sumandos **mayores que cero** y cualquier $N \geq N_0$.

Para describir el *método circular* en el problema de Waring consideremos la igualdad

$$J(n, k, N) = \int_0^1 S^k(\alpha) e^{-2\pi i \alpha N}\, \mathrm{d}\alpha, \qquad S(\alpha) = \sum_{x \leq N^{1/n}} e^{2\pi i \alpha x^n}. \tag{2.2}$$

Ahora bien; el método consiste en dividir una traslación del intervalo $[0,1]$ en dos conjuntos ajenos E_1, E_2, elegidos según criterios de aproximación por números racionales, a fin de hallar la parte principal de $J(n,k,N)$ al integrar sobre el conjunto E_1 y posteriormente verificar que la integral sobre E_2 es despreciable respecto de la parte principal conforme N tiende a infinito.

Demos paso a los detalles formales.

Dados $n \geq 2$, $k = k(n) = 2^n + 1$ y el parámetro $N > N_0$ con $N_0 = N_0(n)$, tomemos $P = N^{1/n}$, $Q(N) = \frac{1}{n}P^{1/2}$ y recordemos que por $J(n,k,N)$ entendemos el número de soluciones de (2.1).

Considere puntos racionales en el intervalo $[0,1)$ de la forma

$$\frac{a}{q}, \qquad (a,q) = 1, \qquad 0 \leq a < q \quad \text{con} \quad q \leq Q(N), \tag{2.3}$$

las *fracciones de Farey* junto con el cero que se obtiene al elegir $q = 1$. Para cada punto de este estilo tomemos al intervalo

$$E(a,q) = \left(\frac{a}{q} - \frac{Q(N)}{N}, \frac{a}{q} + \frac{Q(N)}{N} \right).$$

Deseamos que $(-Q(N)/N, Q(N)/N)$ esté contenido en el intervalo de integración de (2.2). Para ello necesitamos desplazar $[0,1)$ al intervalo $(-Q(N)/N, 1 - Q(N)/N)$ y debido a que el periodo del integrando en (2.2) es uno, se tiene

$$J(n,k,N) = \int_{-\frac{Q(N)}{N}}^{1-\frac{Q(N)}{N}} S^k(\alpha) e^{-2\pi i \alpha N} \, d\alpha, \qquad S(\alpha) = \sum_{x \leq P} e^{2\pi i \alpha x^n}. \tag{2.4}$$

Por otra parte, la elección de $Q(N)$ garantiza que los intervalos $E(a_1,q_1)$, $E(a_2,q_2)$ son ajenos si $\frac{a_1}{q_1} \neq \frac{a_2}{q_2}$, pues de existir $z \in E(a_1,q_1) \cap E(a_2,q_2)$ es fácil verificar que tendríamos $N \leq 2Q(N)^3$, hecho que no puede ocurrir. Consideremos entonces

$$E_1 = \bigcup_{q \leq Q(N)} \bigcup_{\substack{(a,q)=1 \\ 0 \leq a < q}} E(a,q). \tag{2.5}$$

Denotaremos por $E_2 = \left[-\frac{Q(N)}{N}, 1 - \frac{Q(N)}{N}\right) \setminus E_1$ y a su vez

$$J_1(N) = \int_{E_1} S^k(\alpha) e^{-2\pi i \alpha N} \, d\alpha, \qquad J_2(N) = \int_{E_2} S^k(\alpha) e^{-2\pi i \alpha N} \, d\alpha. \tag{2.6}$$

Note además que:

$$\mu(E_1) \ll Q(N)^3/N \ll N^{\frac{3}{2n}-1} \to 0 \quad \text{si} \quad N \to \infty.$$

Casi increíble, pero probaremos que el término principal de $J(n,k,N)$ se determina precisamente por $J_1(N)$; hecho que será, en parte, el punto de discusión en las siguientes secciones.

2.1. Acerca de J_1

Teorema 2.1.1. *Para J_1 es válida la siguiente expresión asintótica*

$$J_1(N) \;=\; N^{\frac{k}{n}-1}\left(\,\sigma(N)\,\gamma \,+\, O(N^{-\frac{1}{2n^2}})\right),$$

donde

$$\sigma(N) \;=\; \sum_{q=1}^{\infty} \sum_{\substack{(a,q)=1\\ 0\le a<q}} \left(\frac{S(a,q)}{q}\right)^k e^{-2\pi i\frac{a}{q}N}, \quad S(a,q) = \sum_{s=1}^{q} e^{2\pi i\frac{a}{q}s^n}$$

$$\gamma \;=\; \int_{-\infty}^{\infty} \left\{ \int_0^1 e^{2\pi i z x^n}\,\mathrm{d}x \right\}^k e^{-2\pi i z}\,\mathrm{d}z.$$

Demostración. En virtud de la representación de E_1 dada en (2.5), tenemos

$$J_1(N) = \sum_{q\le Q(N)} \sum_{\substack{(a,q)=1\\ 0\le a<q}} \int_{-\frac{Q(N)}{N}}^{\frac{Q(N)}{N}} S^k\left(\frac{a}{q}+z\right) e^{-2\pi i(\frac{a}{q}+z)N}\,\mathrm{d}z. \tag{2.7}$$

Estudiemos a $S(a/q+z)$. Haciendo $x = qt+s$ con $1\le s\le q$ se obtiene

$$S\left(\frac{a}{q}+z\right) = \sum_{x\le P} e^{2\pi i\left(\frac{a}{q}+z\right)x^n} = \sum_{s=1}^{q} e^{2\pi i\frac{a}{q}s^n} \sum_{t=\frac{1-s}{q}}^{\frac{P-s}{q}} e^{2\pi i z(qt+s)^n}.$$

Apliquemos el Teorema de *Van der Corput* (Teorema 1.2.2) a la suma

$$\sum_{t=\frac{1-s}{q}}^{\frac{P-s}{q}} e^{2\pi iz(qt+s)^n}.$$

Para ello es preciso que se cumpla

$$\left|\frac{\mathrm{d}}{\mathrm{d}t} z(qt+s)^n\right| \leq \frac{1}{2}.$$

La elección de $Q(N)$ garantiza la desigualdad, para satisfacer esta condición se ha elegido $Q(N) = \frac{1}{n}P^{1/2}$.
Así, aplicando el Teorema de *Van der Corput* resulta

$$\begin{aligned}
S\left(\frac{a}{q}+z\right) &= \sum_{s=1}^{q} e^{2\pi i\frac{a}{q}s^n}\left\{\int\limits_{\frac{1-s}{q}}^{\frac{P-s}{q}} e^{2\pi iz(qt+s)^n}\,\mathrm{d}t \;+\; O(1)\right\} \\
&= \sum_{s=1}^{q} e^{2\pi i\frac{a}{q}s^n}\left\{\frac{P}{q}\int\limits_0^1 e^{2\pi izNx^n}\,\mathrm{d}x \;+\; O(1)\right\} \\
&= \frac{P}{q}\sum_{s=1}^{q} e^{2\pi i\frac{a}{q}s^n}\int\limits_0^1 e^{2\pi izNx^n}\,\mathrm{d}x \;+\; O(q) \\
&= P\frac{S(a,q)}{q}\int\limits_0^1 e^{2\pi izNx^n}\,\mathrm{d}x + O(q).
\end{aligned}$$

Ahora elevemos a la k-ésima potencia para obtener

$$\begin{aligned}
S^k\left(\frac{a}{q}+z\right) = P^k\left(\frac{S(a,q)}{q}\right)^k\left\{\int\limits_0^1 e^{2\pi izNx^n}\,\mathrm{d}x\right\}^k \;+\; O\left(q^k\right) \;+ \\
+\,O\left(P^{k-1}\left(\frac{S(a,q)}{q}\right)^{k-1}\left\{\int\limits_0^1 e^{2\pi izNx^n}\,\mathrm{d}x\right\}^{k-1} q\right).
\end{aligned}$$

Sustituyendo esta expresión en (2.7) y haciendo el cambio $z' = Nz$ obtenemos

$$\begin{aligned}
J_1 &= P^k \sum_{q\le Q(N)} \sum_{\substack{(a,q)=1\\0\le a<q}} \left(\frac{S(a,q)}{q}\right)^k e^{-2\pi i \frac{a}{q}N} \times \\
&\quad \times \int_{-\frac{Q(N)}{N}}^{\frac{Q(N)}{N}} \left\{\int_0^1 e^{2\pi i z N x^n}\,\mathrm{d}x\right\}^k e^{-2\pi i N z}\,\mathrm{d}z \;+\; {R_1}', \\
&= P^{k-n} \sum_{q\le Q(N)} \sum_{\substack{(a,q)=1\\0\le a<q}} \left(\frac{S(a,q)}{q}\right)^k e^{-2\pi i \frac{a}{q}N} \times \\
&\quad \times \int_{-Q(N)}^{Q(N)} \left\{\int_0^1 e^{2\pi i z x^n}\,\mathrm{d}x\right\}^k e^{-2\pi i z}\,\mathrm{d}z \;+\; R_1,
\end{aligned}$$

con

$$\begin{aligned}
R_1 \ll P^{k-n-1} &\sum_{q\le Q(N)} \sum_{\substack{(a,q)=1\\0\le a<q}} \left(\frac{S(a,q)}{q}\right)^{k-1} q \int_0^{Q(N)} \left\{\int_0^1 e^{2\pi i z x^n}\,\mathrm{d}x\right\}^{k-1} \mathrm{d}z \\
&+ \frac{Q(N)^{k+3}}{P^n}.
\end{aligned}$$

El Lema 1.2.3 establece que

$$\int_0^1 e^{2\pi i z x^n}\,\mathrm{d}x \ll \text{mín}(1, |z|^{-1/n})$$

y además $|z|^{-1/n} \le 1$ sí $|z| \ge 1$. Por esta razón:

$$\int_0^1 e^{2\pi i z x^n}\,\mathrm{d}x \ll \begin{cases} 1 & \text{si } |z| < 1, \\ |z|^{-1/n} & \text{si } |z| \ge 1. \end{cases}$$

De esta manera, junto con la estimación del Lema 1.2.2; $S(a,q) \ll q^{1-1/n}$.

Se tiene

$$\begin{aligned} R_1 \;&\ll\; P^{k-n-1} \sum_{q \le Q(N)} q^{-\frac{k-1}{n}+2} \left(1 \,+\, \int_1^{Q(N)} z^{-\frac{k-1}{n}}\, \mathrm{d}z \right) \,+\, \frac{Q(N)^{k+3}}{P^n} \\ &\ll\; P^{k-n-1} Q(N)^{-\frac{k-1}{n}+3} \Big(1 \,+\, Q(N)^{-\frac{k-1}{n}+1} \Big) \,+\, \frac{Q(N)^{k+3}}{P^n}. \end{aligned}$$

Hasta este punto no hemos usado de la hipótesis $k = 2^n + 1$. Siendo éste el caso obtenemos

$$-\frac{k-1}{n} + 1 = -\frac{2^n}{n} + 1 < 0, \quad \text{sí} \quad n \ge 2$$

luego $Q(N)^{-\frac{k-1}{n}+1} \ll 1$ para cualquier $n \ge 2$. De esta manera

$$\begin{aligned} R_1 \;&\ll\; P^{k-n-1} Q(N)^{-\frac{k-1}{n}+3} \,+\, \frac{Q(N)^{k+3}}{P^n} \\ &\ll\; P^{k-n} P^{-\frac{2^{n-1}}{n}+\frac{1}{2}} \,+\, P^{k-n-(2^{n-1}-1)} \\ &\ll\; P^{k-n-1/n}. \end{aligned} \tag{2.8}$$

Por otra parte,

$$\int_{-Q(N)}^{Q(N)} \left\{ \int_0^1 e^{2\pi i z x^n}\, \mathrm{d}x \right\}^k e^{-2\pi i z}\, \mathrm{d}z \;=\; \gamma \,+\, R_\gamma,$$

con

$$R_\gamma \ll \int_{Q(N)}^{\infty} z^{-k/n}\, \mathrm{d}z \;\ll\; Q(N)^{-k/n+1} \;\ll\; P^{-\frac{1}{2}(k/n-1)}.$$

Además,

$$\sum_{q \le Q(N)} \sum_{\substack{(a,q)=1 \\ 0 \le a < q}} \left(\frac{S(a,q)}{q} \right)^k e^{-2\pi i \frac{a}{q} N} \;=\; \sigma(N) \,+\, R_\sigma,$$

$$R_\sigma \;\ll\; \sum_{q > Q(N)} q^{-k/n+1} \;\ll\; Q(N)^{-k/n+2} \;\ll\; P^{-\frac{1}{2}(k/n-2)}.$$

Así, al retomar (2.8), la estimación de R_1 y nuestras dos últimas igualdades concluimos:

$$\begin{aligned} J_1(N) &= P^{k-n}\left(\sigma(N) + O(P^{-\frac{1}{2}(k/n-2)})\right)\left(\gamma + O(P^{-\frac{1}{2}(k/n-1)})\right) + \\ &\quad + O\left(P^{k-n-1/n}\right) \\ &= P^{k-n}\,\sigma(N)\,\gamma + P^{k-n}O(P^{-\frac{1}{2}(k/n-2)} + P^{-1/n}) \\ &= N^{\frac{k}{n}-1}\left(\sigma(N)\,\gamma + O(N^{-1/2n^2})\right). \ \square \end{aligned}$$

Hemos probado nuestro teorema, pero aún falta saber si $\sigma(N)$ o γ acaso se anulan. Anticipamos que no, para ello los siguentes dos lemas.

Lema 2.1.1. *Para*

$$\sigma(N) = \sum_{q=1}^{\infty} \Phi(q), \qquad \Phi(q) = \sum_{\substack{(a,q)=1 \\ 0\le a<q}} \left(\frac{S(a,q)}{q}\right)^k e^{-2\pi i \frac{a}{q} N} \tag{2.9}$$

existe una constante C_0 tal que $\sigma(N) \geq C_0 > 0$. La serie $\sigma(N)$ es conocida como la serie singular del problema de Waring.

Demostración. Primero probemos que $\Phi(q)$ es una función multiplicativa. Por (2.3) sabemos que, para la fracción $\frac{a}{q}$, tenemos $a = 0$ sólo si $q = 1$. De esta forma $\Phi(1) = 1$.

Sean q_1, q_2 enteros positivos primos relativos tales que $q_1 q_2 = q > 1$, entonces la expresión $s_1\, q_2 + s_2\, q_1$ recorre el sistema completo de residuos módulo q a la vez que s_1 recorre el sistema completo de residuos según q_1 y s_2 el sistema completo de residuos módulo q_2. Luego, utilizando el mismo argumento para obtener (1.1) en el Lema 1.2.2, tenemos

$$S(a,q) = S(aq_2^{n-1}, q_1)\, S(aq_1^{n-1}, q_2).$$

De forma similar, el término $a = a_1\, q_2 + a_2\, q_1$ recorre el sistema reducido de residuos módulo q a la vez que a_1 recorre el sistema reducido de residuos según q_1 y a_2 el sistema reducido de residuos módulo q_2. Así obtenemos:

$$
\begin{aligned}
\Phi(q_1 q_2) &= \sum_{\substack{(a_1,q_1)=1\\ 1\le a_1<q_1}} \sum_{\substack{(a_2,q_2)=1\\ 1\le a_2<q_2}} \left(\frac{S((a_1q_2+a_2q_1)q_2^{n-1},q_1)}{q_1} \frac{S((a_1q_2+a_2q_1)q_1^{n-1},q_2)}{q_2} \right)^k \times \\
&\qquad \times e^{-2\pi i \frac{(a_1 q_2 + a_2 q_1)}{q_1 q_2} N} \\
&= \sum_{\substack{(a_1,q_1)=1\\ 1\le a_1<q_1}} \left(\frac{S(a_1 q_2^n, q_1)}{q_1} \right)^k e^{-2\pi i \frac{a_1}{q_1} N} \sum_{\substack{(a_2,q_2)=1\\ 1\le a_2<q_2}} \left(\frac{S(a_2 q_1^n, q_2)}{q_2} \right)^k e^{-2\pi i \frac{a_2}{q_2} N} \\
&= \sum_{\substack{(a_1,q_1)=1\\ 1\le a_1<q_1}} \frac{1}{q_1^k} \left(\sum_{s_1=1}^{q_1} e^{2\pi i \frac{a_1}{q_1}(s_1 q_2)^n} \right)^k e^{-2\pi i \frac{a_1}{q_1} N} \times \\
&\qquad \times \sum_{\substack{(a_2,q_2)=1\\ 1\le a_2<q_2}} \frac{1}{q_2^k} \left(\sum_{s_2=1}^{q_2} e^{2\pi i \frac{a_2}{q_2}(s_2 q_1)^n} \right)^k e^{-2\pi i \frac{a_2}{q_2} N} \\
&= \Phi(q_1)\, \Phi(q_2).
\end{aligned}
$$

Ahora, utilizando esta propiedad y recordando que $\Phi(q) \ll q^{-k/n+1}$ tenemos

$$\prod_{p\le X} \left(1 + \Phi(p) + \Phi(p^2) + \cdots \right) = \sum_{q\le X} \Phi(q) + R$$

donde

$$R \ll \sum_{q>X} q^{-k/n+1} \ll X^{-k/n+2}.$$

Tomando el límite cuando $X \to \infty$ concluimos

$$\sigma(N) = \sum_{q=1}^{\infty} \Phi(q) = \prod_p \left(1 + \Phi(p) + \Phi(p^2) + \cdots \right).$$

También sucede

$$\left| \sum_{m=1}^{\infty} \Phi(p^m) \right| \le c \sum_{m=1}^{\infty} p^{-(k/n-1)m} \le \frac{2c}{p^{k/n-1}}.$$

En nuestro caso, $k = 2^n + 1$, podemos afirmar que $k/n - 1 \ge 3/2$ y de esto

$$\frac{2c}{p^{k/n-1}} \le \frac{2c}{p^{3/2}}.$$

Luego, para aquellos primos $p \geq (2c)^4$ se tiene

$$\left|\sum_{m=1}^{\infty} \Phi(p^m)\right| \leq p^{-5/4}.$$

Así:

$$1 + \Phi(p) + \Phi(p^2) + \cdots > 1 - \frac{1}{p^{5/4}} > 0,$$

obteniendo

$$\begin{aligned}
\sigma(N) &= \prod_{p \geq (2c)^4} \big(1 + \Phi(p) + \Phi(p^2) + \cdots \big) \times \\
&\quad \times \prod_{p < (2c)^4} \big(1 + \Phi(p) + \Phi(p^2) + \cdots \big) \\
&> \prod_{p \geq (2c)^4} \left(1 - \frac{1}{p^{5/4}} \right) \prod_{p < (2c)^4} \big(1 + \Phi(p) + \Phi(p^2) + \cdots \big) \\
&\geq c_1 \prod_{p < (2c)^4} \big(1 + \Phi(p) + \Phi(p^2) + \cdots \big), \qquad (2.10)
\end{aligned}$$

donde c_1 es alguna constante absoluta mayor que cero.

Para concluir con la prueba de este lema es suficiente probar que para cada primo p, el término $(1 + \Phi(p) + \Phi(p^2) + \cdots)$ es mayor que cero. Para ello denotemos por $T_k(p^m)$ al numero de soluciones de la congruencia

$$x_1^n + \cdots + x_k^n \equiv N \pmod{p^m},$$

y observemos que

$$\begin{aligned}
T_k(p^r) &= \frac{1}{p^r} \sum_{a=1}^{p^r} \left\{ \sum_{s=1}^{p^r} e^{2\pi i \frac{a}{p^r} s^n} \right\}^k e^{-2\pi i \frac{a}{p^r} N} \\
&= \frac{1}{p^r} \left\{ p^{rk} \sum_{(a,p)=1} \frac{1}{p^{kr}} \left\{ \sum_{s=1}^{p^r} e^{2\pi i \frac{a}{p^r} s^n} \right\}^k e^{-2\pi i \frac{a}{p^r} N} + \right. \\
&\quad \left. + \; p^k \sum_{a=1}^{p^{r-1}} \left\{ \sum_{s=1}^{p^{r-1}} e^{2\pi i \frac{a}{p^{r-1}} s^n} \right\}^k e^{-2\pi i \frac{a}{p^{r-1}} N} \right\} \\
&= p^{k(r-1)} \Phi(p^r) + p^{k-1} T_k(p^{r-1}).
\end{aligned}$$

Este hecho implica

$$\Phi(p^r) \,=\, p^{-(k-1)r}T_k(p^r) \,-\, p^{-(k-1)(r-1)}T_k(p^{r-1}),$$

y no es difícil verificar que

$$\Phi(p) \,=\, p^{-(k-1)}T_k(p) \,-\, 1.$$

Por lo tanto

$$1 \,+\, \Phi(p) \,+\, \cdots \,+\, \Phi(p^m) \,=\, p^{-(k-1)m}T_k(p^m). \tag{2.11}$$

Ahora bien, el problema lo hemos reducido al estudio de $T_k(p^m)$.

Comenzaremos analizando $T_k(p^\delta)$ siendo

$$\delta = \begin{cases} \tau + 2, & \text{si } p = 2, \quad n = p^\tau n_1, \quad (n, n_1) = 1, \\ \tau + 1, & \text{si } p > 2, \quad n = p^\tau n_1, \quad (n, n_1) = 1. \end{cases}$$

Deseamos probar que la congruencia

$$x_1^n \,+\, \cdots \,+\, x_k^n \equiv N \pmod{p^\delta} \tag{2.12}$$

admite alguna solución $x_1, \ldots, x_k$ con $(x_1, p) = 1$. Para ello podemos suponer que $(N, p) = 1$.

Si $p = 2$ para los casos $n = 2,\, 3$ se verifica directamente que $T_5(8), T_9(4) > 0$. Cuando $n > 3$, entonces $4n \leq k = 2^n + 1$. Por ello $p^\delta \leq 4n \leq k$ y podemos tomar

$$x_1 = 1, \ldots, x_N = 1, x_{N+1} = 0, \ldots, x_k = 0,$$

para obtener la solución de (2.12) requerida.

Si $p > 2$ sean g una raíz primitiva módulo p^δ,

$$g^\alpha \equiv N \pmod{p^\delta},\ g^\beta \equiv N_1 \pmod{p^\delta} \ \text{ y } \ \alpha \equiv \beta \pmod{n}.$$

Entonces, en caso de existir, la congruencia

$$x_1^n \,+\, \cdots \,+\, x_k^n \equiv N \pmod{p^\delta}, \tag{2.13}$$

admite tantas soluciones como

$$x_1^n \,+\, \cdots \,+\, x_k^n \equiv N_1 \pmod{p^\delta}. \tag{2.14}$$

Efectivamente, sea $x_1, \ldots, x_k$ solución de (2.13). Como $\beta = \alpha + nt$ multipliquemos (2.13) por g^{nt} para obtener

$$(x_1 g^t)^n + \cdots + (x_k g^t)^n \equiv g^\beta \pmod{p^\gamma}.$$

Es decir, una solución de (2.14).

Llamemos $k(N)$ al menor entero con la propiedad de que (2.12) admita alguna solución $x_1, \ldots, x_k$ con $(x_1, p) = 1$. Suponiendo que existen exactamente m $k(N)$'s distintos, lo probado anteriormente muestra que $m \leq n$. Dividamos a todos los N's en m clases; diremos que N_1 y N_2 pertenecen a la misma clase si $k(N_1) = k(N_2)$. De esta forma, tomemos a los representantes más pequeños de cada clase $N_1, \ldots, N_m$ dispuestos en orden creciente $N_1 < \cdots < N_m$.

Probemos que $k(N_t) \leq 2t - 1$. Si $t = 1$ resulta $N_1 = 1$ y se cumple $1 = k(1) \leq 2 \cdot 1 - 1$. Ahora supongamos cierto el resultado para todos los enteros menores o iguales a t y notemos que, de entre los números $N_{t+1} - 1$, $N_{t+1} - 2$, alguno no es divisible por p y éste, por ser menor que N_{t+1}, pertenece a una de las clases ya estudiadas. Luego $k(N_{t+1}) \leq 2t + 1 = 2(t+1) - 1$ y con esto obtenemos $k(N_m) \leq 2m + 1 \leq 2n + 1 \leq k$. Es decir, (2.12) admite alguna solución $x_1, \ldots, x_k$ con $(x_1, p) = 1$.

Ahora deseamos investigar acerca de la extensión de soluciones para ciertas congruencias. De manera más precisa:

Si y_0, con $(y_0, p) = 1$, es solución de

$$y^n \equiv a \pmod{p^\delta},$$

entonces para cada $m \geq \delta$ la congruencia

$$x^n \equiv a \pmod{p^m} \tag{2.15}$$

admite una solución x_0 donde $(x_0, p) = 1$. En efecto note primero que la condición $(y_0, p) = 1$ garantiza que $(a, p) = 1$. Por otra parte, sea g una raíz primitiva módulo p^m cuando $p > 2$. Para $p = 2$ tome $g = 5$ si $m \geq 3$ y $g = 3$ cuando $m = 2$. En cualquier caso elijase β de tal manera que

$$y_0^n \, g^\beta \equiv a \pmod{p^m}.$$

Sin perder generlidad, para $p = 2$ y $m \geq 3$ hemos tomado el signo positivo. De esta forma

$$g^{\beta} \equiv 1 \pmod{p^{\delta}} \quad \text{y} \quad \beta = tp^{\tau}(p-1).$$

Para un natural arbitrario r estudiemos la expresión

$$\beta + rp^{m-1}(p-1) = p^{\tau}(p-1)(t + rp^{m-1-\tau}).$$

Puesto que $n = p^{\tau}n_1$ con $(n_1, p) = 1$ es posible elegir r de tal manera que $n_1 h = t + rp^{m-1-\tau}$. Así $\beta + rp^{m-1}(p-1) = nh(p-1)$ y obtenemos

$$g^{\beta + rp^{m-1}(p-1)} \equiv g^{\beta} \pmod{p^m}, \quad y_0^n g^{\beta + rp^{m-1}(p-1)} \equiv a \pmod{p^m}.$$

Luego, $y_0 g^{h(p-1)}$ es solución de (2.15).

Para cada $y_2, \ldots, y_k$ con $1 \leq y_2, \ldots, y_k \leq p^{m-\delta}$ sabemos que la congruencia

$$x_1^n + (x_2 + p^{\delta}y_2)^n + \cdots + (x_k + p^{\delta}y_k)^n \equiv N \pmod{p^{\delta}}$$

admite alguna solución $x_1^{(0)}, \ldots, x_k^{(0)}$ con $(x_1^{(0)}, p) = 1$ siendo $k = 2^n + 1$. O bien, para cada $y_2, \ldots, y_k$ es soluble la congruencia

$$x_1^n \equiv N - (x_2 + p^{\delta}y_2)^n - \cdots - (x_k + p^{\delta}y_k)^n \pmod{p^{\delta}}$$

y cada solución puede ser extendida, en x_1, a una solución de

$$x_1^n \equiv N - (x_2 + p^{\delta}y_2)^n - \cdots - (x_k + p^{\delta}y_k)^n \pmod{p^m}.$$

Es decir

$$T_k(p^m) \geq p^{(k-1)(m-\delta)}.$$

Retomando (2.11) obtenemos

$$1 + \Phi(p) + \cdots + \Phi(p^m) \geq p^{-(k-1)\delta},$$

donde la cota de la derecha no depende de m. Tomando límite

$$1 + \Phi(p) + \cdots \geq p^{-(k-1)\delta} > 0.$$

En virtud de (2.10)

$$\begin{aligned}
\sigma(N) &= \prod_{p\geq(2c)^4}\left(1+\Phi(p)+\Phi(p^2)+\cdots\right)\prod_{p<(2c)^4}\left(1+\Phi(p)+\Phi(p^2)+\cdots\right)\\
&> c_1\prod_{p<(2c)^4}\left(1+\Phi(p)+\Phi(p^2)+\cdots\right)\\
&\geq c_1\prod_{p<(2c)^4}\left(p^{-(k-1)\delta}\right) = c_2 > 0,
\end{aligned}$$

probando de esta manera que la serie singular no se anula. □

Con el siguiente lema concluimos el estudio de J_1 .

Lema 2.1.2. *Para* $k\geq n+1$ *es válida la igualdad*

$$\gamma(k,n)=\int_{-\infty}^{\infty}\left(\int_0^1 e^{2\pi izx^n}\,\mathrm{d}x\right)^k e^{-2\pi iz}\,\mathrm{d}z = \frac{\left(\Gamma\left(1+\frac{1}{n}\right)\right)^k}{\Gamma\left(\frac{k}{n}\right)}. \tag{2.16}$$

En particular $\gamma > 0$.

Demostración. Consideremos la siguiente función de variable real

$$g(x)=\int_{-\infty}^{\infty}\left(\int_0^1 e^{2\pi izu^n}\,\mathrm{d}u\right)^k e^{-2\pi ixz}\,\mathrm{d}z,$$

note que $g(1)=\gamma(k,n)$. Por el Lema 1.2.3 tenemos

$$\int_0^1 e^{2\pi izu^n}\,\mathrm{d}u \ll \text{mín}\left\{1,\frac{1}{|z|^{1/n}}\right\},$$

por lo que la integral converge absolutamente cuando $k\geq n+1$. Para $0<c\leq 1$, tomemos

$$\begin{aligned}
F(c) &= \int_0^c g(x)\,\mathrm{d}x = \int_{-\infty}^{\infty}\left(\int_0^1 e^{2\pi i z u^n}\,\mathrm{d}u\right)^k \frac{1-e^{-2\pi i c z}}{2\pi i z}\,\mathrm{d}z \\
&= \int_0^1 \cdots \int_0^1 \int_{-\infty}^{\infty} \frac{e^{2\pi i z(u_1^n+\cdots+u_k^n)} - e^{2\pi i z(u_1^n+\cdots+u_k^n-c)}}{2\pi i z}\,\mathrm{d}z\,\mathrm{d}u_1\cdots\mathrm{d}u_k \\
&= \frac{1}{\pi}\int_0^1 \cdots \int_0^1 \int_0^{\infty} \frac{\operatorname{sen} 2\pi z\lambda - \operatorname{sen} 2\pi z(\lambda-c)}{z}\,\mathrm{d}z\,\mathrm{d}u_1\cdots\mathrm{d}u_k,
\end{aligned}$$

siendo $\lambda = u_1^n + \cdots + u_k^n$. Por otra parte, usando el hecho:

$$\int_0^{\infty} \frac{\operatorname{sen} z\alpha}{z}\,\mathrm{d}z = \frac{\pi}{2}\operatorname{sign}\alpha,$$

para $\alpha = 2\pi\lambda$ obtenemos

$$\int_0^{\infty} \frac{\operatorname{sen} 2\pi z\lambda - \operatorname{sen} 2\pi z(\lambda-c)}{z}\,\mathrm{d}z = \frac{\pi}{2}\left(\operatorname{sign}\lambda - \operatorname{sign}(\lambda-c)\right).$$

De esta manera se tiene

$$F(c) = \underbrace{\int\cdots\int}_{0\le u_1^n+\cdots+u_k^n\le c} \mathrm{d}u_1\cdots\mathrm{d}u_k.$$

Ahora bien, al hacer el cambio $u_1 = t_1^{1/n}c^{1/n}, \ldots, u_k = t_k^{1/n}c^{1/n}$, obtenemos

$$F(c) = \frac{1}{n^k}c^{k/n} \underbrace{\int\cdots\int}_{0\le t_1+\cdots+t_k\le 1} t_1^{1/n-1}\cdots t_k^{1/n-1}\,\mathrm{d}t_1\cdots\mathrm{d}t_k,$$

donde $0 \le t_1, \ldots, t_k \le 1$.

Usemos el siguiente resultado de Dirichlet.

Sean $\alpha_1 > 0, \ldots, \alpha_k > 0$, *y f(u) una función continua. Entonces, para*

$$I = \underbrace{\int \cdots \int}_{0 \le t_1 + \cdots + t_k \le 1} f(t_1 + \cdots + t_k) t_1^{\alpha_1 - 1} \cdots t_k^{\alpha_k - 1} \, \mathrm{d}t_1 \cdots \mathrm{d}t_k,$$

donde $0 \le t_1, \ldots, t_k \le 1$, *se cumple la igualdad:*

$$I = \frac{\Gamma(\alpha_1) \cdots \Gamma(\alpha_k)}{\Gamma(\alpha_1 + \cdots + \alpha_k)} \int_0^1 f(u) u^{\alpha_1 + \cdots + \alpha_k - 1} \, \mathrm{d}u. \quad \square$$

Así, por el resultado de Dirichlet, obtenemos

$$F(c) = \frac{1}{n^k} c^{k/n} \frac{\Gamma^k\left(\frac{1}{n}\right)}{\Gamma\left(\frac{k}{n}\right)} \int_0^1 u^{k/n - 1} \, \mathrm{d}u = \frac{n}{k} c^{k/n} \frac{\left(\frac{1}{n}\Gamma\left(\frac{1}{n}\right)\right)^k}{\Gamma\left(\frac{k}{n}\right)}.$$

Derivando respecto de c y usando la identidad $\Gamma(1+s) = s\,\Gamma(s)$, sucede

$$g(c) = c^{k/n - 1} \frac{\Gamma\left(1 + \frac{1}{n}\right)^k}{\Gamma\left(\frac{k}{n}\right)}.$$

Finalmente, al tomar $c = 1$, obtenemos

$$g(1) \; = \; \gamma(k,n) \; = \; \frac{\left(\Gamma\left(1 + \frac{1}{n}\right)\right)^k}{\Gamma\left(\frac{k}{n}\right)}. \qquad \square$$

2.2. Acerca de J_2

Hemos concluido el estudio de J_1. Para el estudio de J_2 será de gran importancia que el número de sumandos, en el problema de Waring, sea precisamente $2^n + 1$. Son el Lema de Hua y una estimación no trivial para $S(\alpha)$ los resultados principales de esta sección.

Ahora deseamos verificar que efectivamente J_1 es un término que pondera sobre J_2, o bien $J_2 = o(N^{\frac{k}{n} - 1})$. Para justificar esto, el esquema a seguir es:

hallar una estimación no trivial para $S(\alpha)$, digamos $S(\alpha) \ll P^{1-\delta}$; para algún $\delta = \delta(n) > 0$. Posteriormente, para hacer uso de la desigualdad

$$|J_2| \leq \left| \int\limits_{E_2} S^k(\alpha) e^{-2\pi i \alpha N} \, \mathrm{d}\alpha \right| \leq \sup_{\alpha \in E_2} \{|S(\alpha)|\} \int\limits_0^1 |S(\alpha)|^{2^n} \, \mathrm{d}\alpha,$$

nos daremos a la tarea de probar que para $\varepsilon > 0$ tenemos:

$$\int\limits_0^1 |S(\alpha)|^{2^n} \, \mathrm{d}\alpha \ \ll \ P^{2^n - n + \varepsilon}$$

y así obtener

$$J_2 \ \ll \ P^{2^n + 1 - n - \delta + \varepsilon},$$

o bien

$$J_2 \ \ll \ N^{\frac{k}{n} - 1 - \delta/n + \varepsilon} \ = \ o(N^{\frac{k}{n} - 1}).$$

Comenzemos con la estimación de $S(\alpha)$. Si $n = 2$ tomemos $|S(\alpha)|^2$. Al hacer el cambio $y = x + h$ se obtiene

$$\begin{aligned} |S(\alpha)|^2 &= \left| \sum_{1 \leq y, x \leq P} e^{2\pi i (y^2 - x^2)} \right| \\ &\leq \sum_{|h| \leq P-1} \left| \sum_{A_h \leq x \leq B_h} e^{2\pi i 2hx} \right| \\ &\ll P + \sum_{h \leq P-1} \text{mín}\left(P, \frac{1}{\|\alpha h\|} \right), \end{aligned}$$

con $A_h = \text{máx}\{1, 1-h\}$, $B_h = \text{mín}\{P, P-h\}$.

Bajo la misma idea, para $n = 3$ resulta

$$
\begin{aligned}
|S(\alpha)|^4 &= \left|\sum_{1\le x,y\le P} e^{2\pi i\alpha(y^3-x^3)}\right|^2 \\
&\le \left\{\sum_{|h_1|\le P-1}\left|\sum_{A_1\le x\le B_1} e^{2\pi i\alpha 3z(x^2+xz)}\right|\right\}^2 \\
&\ll P\sum_{|h_1|\le P-1}\left|\sum_{A_1\le x\le B_1} e^{2\pi i\alpha 3z(x^2+xz)}\right|^2 \\
&\ll P\sum_{|h_1|\le P-1}\ \sum_{|h_2|\le B_1-A_1}\left|\sum_{A_2\le x\le B_2} e^{2\pi i\alpha 6zwx}\right| \\
&\ll P^3 + P\sum_{1\le h_1\le P-1}\ \sum_{1\le h_2\le B_1-A_1}\left|\sum_{A_2\le x\le B_2} e^{2\pi i\alpha 6zwx}\right| \\
&\ll P^3 + P^{1+\varepsilon}\sum_{h=1}^{P^2}\left|\sum_{x=1}^{P} e^{2\pi i\alpha hx}\right| \\
&\ll P^3 + P^{1+\varepsilon}\sum_{h=1}^{P^2}\text{mín}\left(P, \frac{1}{\|\alpha h\|}\right),
\end{aligned}
$$

donde $A_1 = \text{máx}\{1, 1-h_1\}$, $B_1 = \text{mín}\{P, P-h_1\}$, $A_2 = \text{máx}\{A_1, A_1-h_2\}$, $B_2 = \text{mín}\{B_1, B_1-h_2\}$.

Antes de hacer el mismo análisis para el caso $n > 3$ estudiaremos un poco más la idea planteada. Sea $f(x)$ un polinomio de grado $n > 1$ con coeficientes enteros y término lider a_n. Entonces para x dado, haciendo el cambio $y = x+h$, obtenemos

$$
\begin{aligned}
\left|\sum_{x\le P} e^{2\pi i\alpha f(x)}\right|^2 &= \left|\sum_{x\le P}\ \sum_{1-x\le h\le P-x} e^{2\pi i\alpha((x+h)^n-x^n)}\right| \\
&\le \sum_{|h|\le P-1}\left|\sum_{A_h\le x\le\ B_h} e^{2\pi i\alpha h f_h(x)}\right|,
\end{aligned}
$$

donde $f_h(x)$ es un polinomio con coeficientes polinomiales en h, de grado $n-1$ en la variable x, término principal na_n y además $A_h = \text{máx}(1, 1-h)$,

$B_h = \text{mín}(P, P-h)$. Suponiendo que $n > 2$, para $2 < j \leq n$, tiene lugar la siguiente desigualdad

$$\left|\sum_{x\leq P} e^{2\pi i\alpha f(x)}\right|^{2^{j-1}} \leq (2P-1)^{2^{j-2}-1} \sum_{1-P\leq h_1\leq P-1} \left|\sum_{A_1\leq x\leq B_1} e^{2\pi i\alpha h_1 f_1(x)}\right|^{2^{j-2}}.$$

Bajo el mismo razonamiento obtenemos:

$$\left|\sum_{x\leq P} e^{2\pi i\alpha f(x)}\right|^{2^{j-1}} \ll P^{2^{j-2}-1} P^{2^{j-3}-1} \times$$

$$\times \sum_{|h_1|\leq P-1} \sum_{|h_2|\leq B_1-A_1} \left|\sum_{A_2\leq x\leq B_2} e^{2\pi i\alpha h_1 h_2 f_2(x)}\right|^{2^{j-3}}.$$

Si $n > 3$ apliquemos el mismo argumento, un total de $j-2$ veces para obtener:

$$\left|\sum_{x\leq P} e^{2\pi i\alpha f(x)}\right|^{2^{j-1}} \ll P^{(2^{j-2}-1)+\cdots+(2-1)} \times$$

$$\sum_{|h_1|\leq P-1} \cdots \sum_{|h_{j-2}|\leq B_{j-3}-A_{j-3}} \left|\sum_{A_{j-2}\leq x\leq B_{j-2}} e^{2\pi i\alpha h_1\cdots h_{j-2} f_{j-2}(x)}\right|^2,$$

donde $f_{j-2}(x)$ es un polinomio con coeficientes polinomiales en $h_1, \cdots, h_{j-2}$ de grado $n-(j-2)$ en la variable x y término lider $n(n-1)\cdots(n-(j-3))a_n$. En resumen, tiene lugar el siguiente lema.

Lema 2.2.1. *Sea $f(x)$ un polinomio de grado $n > 2$ con coeficientes enteros y término lider a_n. Entonces si $j \leq n$ es válida la siguiente estimación:*

$$\left|\sum_{x\leq P} e^{2\pi i\alpha f(x)}\right|^{2^{j-1}} \ll P^{2^{j-1}-j} \times$$

$$\sum_{|h_1|\leq P-1} \cdots \sum_{|h_{j-2}|\leq B_{j-3}-A_{j-3}} \left|\sum_{A_{j-2}\leq x\leq B_{j-2}} e^{2\pi i\alpha h_1\cdots h_{j-2} f_{j-2}(x)}\right|^2,$$

con $f_{j-2}(x)$ *un polinomio con coeficientes polinomiales en* $h_1,\ldots,h_{j-2}$ *de grado* $n-(j-2)$ *en* x*, término lider* $n(n-1)\cdots(n-(j-3))a_n$ *y* $1\le A_k< B_k\le P$ *para* $k=1,\ldots,j-2$. $\square$

Ahora bien, utilizando este lema para el caso $j=n$ con $n>3$, el polinomio f_{n-2} será cuadrático en la variable x. Entonces, haciendo un último cambio, $y=x+h_{j-1}$, obtenemos

$$\left|\sum_{A_{n-2}\le x\le\ B_{n-2}} e^{2\pi i\alpha h_1\cdots h_{n-2}f_{n-2}(x)}\right|^2 = \sum_{A_{n-2}\le x,y\le\ B_{n-2}} e^{2\pi i\alpha h_1\cdots h_{n-2}(f_{n-2}(y)-f_{n-2}(x))}$$

$$\le \sum_{|h_{n-1}|\le B_{n-2}-A_{n-2}} \left|\sum_{A_{n-1}\le x\le\ B_{n-1}} e^{2\pi i\alpha h_1\cdots h_{n-1}f_{n-1}(x)}\right|.$$

Resulta que $f_{n-1}(x)$ es de grado uno en la varible x con coeficiente principal $n!$. Luego, usando la estimación del Lema 1.2.4

$$\begin{aligned}
\left|\sum_{x\le P} e^{2\pi i\alpha f(x)}\right|^{2^{n-1}} &\ll P^{2^{n-1}-n}\times \\
&\sum_{|h_1|\le P-1}\cdots\sum_{|h_{n-1}|\le B_{n-2}-A_{n-2}} \left|\sum_{A_{n-1}\le x\le\ B_{n-1}} e^{2\pi i\alpha\, n!\, h_1\cdots h_{n-1}x}\right|^2 \\
&\ll P^{2^{n-1}-1}+P^{2^{n-1}-n}\sum_{h_1=1}^{P}\cdots\sum_{h_{n-1}}^{P}\left|\sum_{x=1}^{n!P} e^{2\pi i\alpha h_1\cdots h_{n-1}x}\right| \\
&\ll P^{2^{n-1}-1}+P^{2^{n-1}-n+\varepsilon}\sum_{h=1}^{P^{n-1}}\left|\sum_{x=1}^{P} e^{2\pi i\alpha h\, x}\right| \\
&\ll P^{2^{n-1}-1}+P^{2^{n-1}-n+\varepsilon}\sum_{h=1}^{P^{n-1}}\text{mín}\left\{P,\frac{1}{\|\alpha h\|}\right\}. \qquad (2.17)
\end{aligned}$$

De esta forma, incluyendo los casos $n=2,3$ ya estudiados, podemos concluir

Lema 2.2.2. *Sea $f(x)$ es un polinimio mónico de grado mayor o igual a dos. Entonces para $\varepsilon > 0$ se tiene la siguiente estimación*

$$\left|\sum_{x\le P} e^{2\pi i\alpha f(x)}\right|^{2^{n-1}} \ll P^{2^{n-1}-1} + P^{2^{n-1}-n+\varepsilon} \sum_{h=1}^{P^{n-1}} \text{mín}\left\{P, \frac{1}{\|\alpha h\|}\right\}.$$

Más aún, en el caso $n=2$ podemos tomar $\varepsilon = 0$. □

Ahora bien, recordando el Teorema de Dirichlet (Teorema 1.2.1), para $\alpha \in E_2$ y $\tau = P^{n-3/4}$ dados, existen enteros a, q tales que

$$\alpha = \frac{a}{q} + \frac{\theta}{q\tau},$$

con $(a,q) = 1$, $|\theta| \le 1$, $q \le \tau$.

Bajo esta representación de α y usando el Lema 1.2.5, tenemos

$$\sum_{h=1}^{P^{n-1}} \text{mín}\left\{P, \frac{1}{\|\alpha h\|}\right\} \le \left(\frac{P^{n-1}}{q} + 1\right)(P + q\log q).$$

Puesto que $\alpha \in E_2$, debemos notar

$$Q(N) < q \le \tau.$$

Además, la elección $Q(N) = \frac{1}{n}P^{1/2}$ garantiza

$$\frac{1}{q} \ll P^{-1/2}.$$

Finalmente, utilizando el Lema 2.2.2 resulta:

$$\begin{aligned} |S(\alpha)|^{2^{n-1}} &\ll P^{2^{n-1}-1} + P^{2^{n-1}-n+\varepsilon}\left(\frac{P^n}{q} + P^{n-1}\log q + P + q\log q\right) \\ &\ll P^{2^{n-1}-1} + P^{2^{n-1}-n+\varepsilon}P^{n-1/2} \\ &\ll P^{2^{n-1}-1/2+\varepsilon}. \end{aligned}$$

Para concluir

$$S(\alpha) \ll P^{1-\frac{1}{2^n}+\varepsilon}, \tag{2.18}$$

que es efectivamente una estimación no trivial de $S(\alpha)$. $\square$

Siguiendo la idea trazada, ahora necesitamos estimar

$$I_j = \int_0^1 |S(\alpha)|^{2^j} \, d\alpha, \quad \text{con} \quad S(\alpha) = \sum_{x \le P} e^{2\pi i \alpha x^n}.$$

Para ello, utilizaremos el hecho que I_j representa al número de soluciones de la ecuación

$$x_1^n + \cdots + x_{2^{j-1}}^n = y_1^n + \cdots + y_{2^{j-1}}^n, \qquad 1 \le x_i, y_i \le P, \quad 2 \le j \le n.$$

Probaremos:

Lema 2.2.3. (*Lema de Hua*) *Para* $j \ge 2$ *dado y cualquier* $n \ge j$ *es efectiva la fórmula*

$$I_j \ll P^{2^j - j + \varepsilon},$$

para todo $\varepsilon > 0$.

Demostración. Procedamos por inducción.
Supongamos que $j = 2$ y recuerde que por I_2 entendemos al número de soluciones de

$$x_1^n + x_2^n = y_1^n + y_2^n \qquad 1 \le x_1, x_2, y_1, y_2 \le P.$$

Entonces, reescribiendo la expresión como

$$(x_1 - y_1)(x_1^{n-1} + \cdots + y_1^{n-1}) = (y_2 - x_2)(y_2^{n-1} + \cdots + x_2^{n-1})$$

observemos que esta expresión se anula si, y sólo si $x_1 = y_1$ a la vez que $y_2 = x_2$; lo anterior sucede en total P^2 veces. Por otra parte, la ecuación anterior no tiene más que $P^{2+\varepsilon}$ soluciones no nulas. Por lo tanto, $I_2 \ll P^{2+\varepsilon}$.

Con $j = 3$ se exhibirá la idea a extender para resolver el caso general. Siendo así, usando el Lema 2.2.1, bajo el supuesto $j = 3$, se afirma

$$\left| \sum_{x \le P} e^{2\pi i \alpha x^n} \right|^{2^2} \ll P \sum_{|h_1| \le P-1} \left| \sum_{A_1 \le w \le B_1} e^{2\pi i \alpha h_1 f_1(w)} \right|^2.$$

De esta forma

$$\begin{aligned}
I_3 &= \int_0^1 \left|\sum_{x\le P} e^{2\pi i\alpha x^n}\right|^{2^3} \mathrm{d}\alpha = \int_0^1 \left|\sum_{x\le P} e^{2\pi i\alpha x^n}\right|^{2^2} \left|\sum_{x\le P} e^{2\pi i\alpha x^n}\right|^{2^2} \mathrm{d}\alpha \\
&\ll P \sum_{|h_1|\le P-1} \sum_{A_1\le w_2, w_1\le B_1} \int_0^1 e^{2\pi i\alpha h_1(f_1(w_2)-f_1(w_1))} \left|\sum_{x\le P} e^{2\pi i\alpha x^n}\right|^{2^2} \mathrm{d}\alpha \\
&= P \sum_{|h_1|\le P-1} \sum_{A_1\le w_1, w_2\le B_1} \sum_{1\le x_1,x_2,y_1,y_2\le P} \times \\
&\quad \times \int_0^1 e^{2\pi i\alpha(h_1(f_1(w_2)-f_1(w_1))-x_1^n-x_2^n+y_1^n+y_2^n)} \mathrm{d}\alpha \\
&\ll P\,J', \qquad (2.19)
\end{aligned}$$

donde J' es el número de soluciones de

$$h_1(f_1(w_2)-f_1(w_1)) = x_1^n + x_2^n - y_1^n - y_2^n,$$

para $h_1, w_1, w_2 \ll P$, $1 \le x_1, x_2, y_1, y_2 \le P$. Haciendo el cambio $w_2 = h_2 + w_1$, notamos que J' ahora representa al número de soluciones de

$$h_1 h_2 f_2(w_1) = x_1^n + x_2^n - y_1^n - y_2^n, \qquad (2.20)$$

con $h_1, h_2, w_1 \ll P$, $1 \le x_1, x_2, y_1, y_2 \le P$ y $f_2(w_1)$ un polinomio con coeficientes en h_1, h_2 de grado $n-2$ en la variable w_1.
Para estimar J', es preciso conocer el número de soluciones, digamos J'', de

$$x_1^n + x_2^n = y_1^n + y_2^n,$$

el cual es el problema ya estudiado para el caso $j = 2$, por lo que $J'' \ll P^{2+\varepsilon}$. Retomamos la expresión (2.20), si $h_1 = 0$ o $h_2 = 0$, no hay más que $P^{4+\varepsilon}$ soluciones. De manera similar si $f_2(w_2)$ se anula, recordando que no tiene más que $n-2$ raíces, las soluciones no son más que $P^{4+\varepsilon}$. Por último, si la expresión (2.20) es distinta de cero no hay más que $P^{4+\varepsilon}$ soluciones. De esta forma se obtiene $J' \ll P^{4+\varepsilon}$, y al sustituir en la estimación (2.19) concluimos que $I_3 \ll P^{2^3-3+\varepsilon}$.

Supongamos ahora que $j > 3$ y para cada $2 \le l < j$ se cumple $I_l \ll P^{2^l-l+\varepsilon}$.

Siendo así, el Lema 2.2.1 garantiza:

$$\begin{aligned}\left|\sum_{x\le P} e^{2\pi i\alpha x^n}\right|^{2^{j-1}} &\ll P^{2^{j-1}-j} \times \\ &\times \sum_{|h_1|\le P-1}\cdots\sum_{|h_{j-2}|\le B_{j-3}-A_{j-3}}\left|\sum_{A_{j-2}\le x\le B_{j-2}} e^{2\pi i\alpha h_1\cdots h_{j-2} f_{j-2}(x)}\right|^2 .\end{aligned}$$

De esta forma:

$$\begin{aligned}I_j &= \int_0^1 |S(\alpha)|^{2^j}\,\mathrm{d}\alpha = \int_0^1 \left|\sum_{x\le P} e^{2\pi i\alpha x^n}\right|^{2^{j-1}} \left|\sum_{x\le P} e^{2\pi i\alpha x^n}\right|^{2^{2-1}} \mathrm{d}\alpha \\ &\ll P^{2^{j-1}-j}\sum_{|h_1|\le P-1}\cdots\sum_{|h_{j-2}|\le B_{j-3}-A_{j-3}}\ \sum_{A_{j-2}\le w_1,w_2\le B_{j-2}} \times \\ &\quad\times\int_0^1 e^{2\pi i\alpha h_1\cdots h_{j-2}(f_{j-2}(w_2)-f_{j-2}(w_1))}\left|\sum_{x\le P} e^{2\pi i x^n}\right|^{2^{j-1}} \mathrm{d}\alpha \\ &= P^{2^{j-1}-j}\sum_{|h_1|\le P-1}\cdots\sum_{|h_{j-2}|\le B_{j-3}-A_{j-3}}\ \sum_{A_{j-2}\le w_1,w_2\le B_{j-2}} \times \\ &\quad\times\sum_{x_1\le P-1}\cdots\sum_{x_{2^{j-2}}\le P}\ \sum_{y_1\le P-1}\cdots\sum_{y_{2^{j-2}}\le P} \times \\ &\quad\times\int_0^1 e^{2\pi i\alpha(h_1\cdots h_{j-2}(f_{j-2}(w_2)-f_{j-2}(w_1))-(x_1^n-y_1^n)-\cdots-(x_{2^{j-2}}^n-y_{2^{j-2}}^n))}\,\mathrm{d}\alpha \\ &= P^{2^{j-1}-j}\,J'',\end{aligned}$$

con J'' el número de soluciones de

$$h_1\cdots h_{j-2}(f_{j-2}(w_2)-f_{j-2}(w_1)) = (x_1^n-y_1^n)+\cdots+(x_{2^{j-2}}^n-y_{2^{j-2}}^n)$$

para $h_1\cdots h_{j-2}, w_1, w_2 \ll P,\ \ 1\le x_i, y_i\le P$ $(i=1,\dots,2^{j-2})$. Haciendo el cambio $w_2 = h_{j-1}+w_1$, obtenemos que J'' es el número de soluciones para

$$h_1\cdots h_{j-1} f_{j-1}(w_1) = (x_1^n-y_1^n)+\cdots+(x_{2^{j-2}}^n-y_{2^{j-2}}^n),$$

donde $h_1 \cdots h_{j-1}, w_1 \ll P,\ 1 \leq x_i, y_i \leq P\ (i = 1, \ldots, 2^{j-2})$. Si alguno de los $h's$ o el polinimio f_{j-1} se anula, entonces

$$(x_1^n - y_1^n) + \cdots + (x_{2^{j-2}}^n - y_{2^{j-2}}^n) \ = \ 0$$

y la hipótesis de inducción garantiza que esta expresión no admite más soluciones que $P^{2^{j-1}-(j-1)+\varepsilon}$. Luego, nuestra ecuación admite $P^{2^{j-1}+\varepsilon}$ soluciones nulas. Por otra, parte tenemos $P^{2^{j-1}+\varepsilon}$ soluciones no nulas.
Así $J'' \ll P^{2^{j-1}+\varepsilon}$, y con esto podemos concluir que

$$I_j \ \ll \ P^{2^{j-1}-j}\, J'' \ \ll \ P^{2^j - j + \varepsilon}. \ \square$$

Podemos concluir respecto a J_2, el siguiente resultado:

Teorema 2.2.1. *Para* J_2 *es válida la estimación*

$$J_2 \ \ll \ N^{\frac{k}{n} - 1 - \frac{1}{n2^n} + \varepsilon}.$$

Demostración. De la expresión

$$J_2 \ \leq \ \sup_{\alpha \in E_2} \{|S(\alpha)|\} \int_0^1 |S(\alpha)|^{2^n} \ \mathrm{d}\alpha,$$

el resultado es inmediato retomando las estimaciones para $S(\alpha)$ e I_n de (2.18) y el Lema 2.2.3, respectivamente. $\square$

Por otra parte, es fácil verificar que la estimación obtenida para I_n en el Lema 2.2.3 es muy fina, es decir

$$I_n \ \geq \ 2^{-n} P^{2^n - n}.$$

Efectivamente, dado λ, considere a $I_n(\lambda)$ como el número de soluciones de la ecuación

$$x_1^n + \ \cdots \ - x_{2^n}^n = \lambda,$$

para $1 \leq x_1, \ldots, x_{2^n} \leq P$. Es claro que

$$I_n(\lambda) = \int_0^1 \left| \sum_{x \leq P} e^{2\pi i \alpha x^n} \right|^{2^n} e^{-2\pi i \alpha \lambda}\, \mathrm{d}\alpha,$$

luego

$$I_n(\lambda) \leq I_n. \tag{2.21}$$

Por otra parte, $|\lambda| < 2^{n-1}P^n$ y además

$$\sum_{\lambda} I_n(\lambda) \; = \; P^{2^n}.$$

Tomando la sumatoria en (2.21) sobre λ tenemos

$$I_n \; \geq \; 2^{-n}P^{2^n-n}.$$

2.3. Conclusión

Finalmente, en virtud de los Teoremas 2.1.1 y 2.2.1 podemos deducir una fórmula asintótica para el problema de *Waring* y en base a los Lemas 2.1.1 y 2.1.2, afirmar que el término principal de dicha fórmula no es cero.

Teorema 2.3.1. *Sean* $n \geq 2$ *y* $k = 2^n + 1$. *Si* $J(n,k,N)$ *representa el número de soluciones de la igualdad*

$$x_1^n + \cdots + x_k^n \; = \; N,$$

entonces la expresión asintótica

$$J(n,k,N) = N^{\frac{k}{n}-1}\left(\gamma\,\sigma(N) \; + \; O(N^{-1/n2^n+\varepsilon})\right)$$

se cumple, donde $\sigma(N)$ *es la serie singular del problema de Waring*

$$\sigma(N) \; = \sum_{q=1}^{\infty} \sum_{\substack{(a,q)=1 \\ 0\leq a<q}} \left(\frac{S(a,q)}{q}\right)^k e^{-2\pi i \frac{a}{q} N}, \quad S(a,q) = \sum_{s=1}^{q} e^{2\pi i \frac{a}{q} s^n}$$

para la cual existe una constante absoluta $C_0 > 0$ *tal que* $\sigma(N) \geq C_0$. *Además,*

$$\gamma(k,n) = \frac{\left(\Gamma\left(1+\frac{1}{n}\right)\right)^k}{\Gamma\left(\frac{k}{n}\right)}$$

y existe una constante absoluta $C_1 > 1$ *con* $\gamma \geq C_1 > \; 0.$ $\square$

2.4. Observaciones finales

Diferentes métodos se han empleado para mejorar la cota $G(n) \leq 2^n + 1$. Para $n = 3$ el resultado de Linnik [9] muestra que $G(n) \leq 7$, no obstante dicho resultado carece de una fórmula asintótica para el número de representaciones de $N \geq N_0$ como suma de siete cubos. Vaughan logró hayar una expresión asintótica para la suma de ocho cubos [10]. Para el caso general los resultados de Vinogradov (puede consultarse [7], Cap. XI Sec. §3) muestran que

$$n \ \leq \ G(n) \ \leq \ c\, n \log n.$$

De manera más precisa, Vinogradov [13] probó que para $n > 170000$ se tiene

$$G(n) \ \leq \ n\,(2\log n \ + \ 4\log\log n \ + \ 2\log\log\log n \ + \ 13).$$

Posteriormente, en 1985 [8], Karatsuba introdujo nuevas ideas basadas en su método p-ádico para lograr en particular la estimación

$$G(n) \ \leq \ n\,(2\log n \ + \ 2\log\log n \ + \ 12),$$

cuando $n \geq 4000$. Fué hasta 1992 cuando Wooley [15] mejoró dicha estimación. Su resultado

$$G(n) \ \leq \ n\,(\log n \ + \ \log\log n \ + \ O(1)).$$

Bibliografía

[1] Davenport, Harold. *On Waring's Problem for fourth powers.* Ann. Math., **40** :731–747, (1939).

[2] Hardy, Godfrey Harold and Littlewood, John Edensor. *Some problems of 'Partitio Numerorum'; I: A new solution of Waring's problem.* (English). Gött. Nachr., :33–54, (1920).

[3] Hardy, Godfrey Harold and Littlewood, John Edensor. *Some problems of "Partitio Numerorum": III. On the expression of a number as a sum of primes.* Acta Math., **44** :1–70, (1922).

[4] Hardy, Godfrey Harold and Littlewood, John Edensor. *Some problems of "Partitio Numerorum" (V): A further contribution to the study of Goldbach's problem.* Proc. Lond. Math. Soc.,(2) , **22** :46–56, (1923).

[5] Hilbert, David. *Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n^{ter} Potenzen (Waringsches Problem). Dem Andenken an Hermann Minkowski gewidmet.* (German). Gött. Nachr., :17–36, (1909).

[6] Hua, Loo-Keng. *Introduction to number theory.* Springer-Verlag, Berlin, Heidelberg, New York, first edition, 1982.

[7] Karatsuba, Anatolii Alexeevich. *Fundamentos de la Teoría Analítica de los Números.* Mir Moscú, Moscú, primera edition, 1979.

[8] Karatsuba, Anatolii Alexeevich. *The function $G(n)$ in Waring's problem.* (Russian). Izv. Akad. Nauk SSSR. Ser. Mat., **49**, no. **5** :935–947, 1119, (1985).

[9] Linnik, Yuri Vladimirovich. *On the representation of large numbers as sums of seven cubes.* Mat. Sbornik., **12** :218–224, (1943).

[10] Vaughan, Robert C. *On Waring's Problem for cubes.* J. reine angew. Math., **365** :122–170, (1986).

[11] Vinogradov, Ivan Matveevich. *Sur le théoremè de Waring.* C.R. Acad. Sci. URSS, :393–400, (1928).

[12] Vinogradov, Ivan Matveevich. *Representation of an odd number as a sum of three primes.* C.R. Acad. Sci. URSS, **15** :393–400, (1937).

[13] Vinogradov, Ivan Matveevich. *On an upper bound for $G(n)$.* (Russian). Izv. Akad. Nauk SSSR. Ser. Mat. , **23** :637–642, (1959).

[14] Vinogradov, Ivan Matveevich. *Fundamentos de la Teoría de los Números.* Mir Moscú, Moscú, segunda edition, 1977.

[15] Wooley, Trevor. *Large improvements in Waring's problem.* Ann. of Math. (2), **135**, no. **1** :131–164, (1992).