UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO

FACULTAD DE CIENCIAS

El método del círculo de Hardy-Littlewood

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

Matemático

PRESENTA:

Lorenzo Antonio Alvarado Cabrera

TUTOR

Dr. Jorge Jiménez Urroz

Ciudad Universitaria, CDMX. 2026.

Índice general

Agradecimientos

Cuando uno empieza el viaje en una carrera de ciencias, no se imagina todas las cosas buenas y malas que pasarán. Muchas veces se cree que será un camino sencillo o directo —claro que es posible—, sin embargo, no llegamos a dimensionar todo lo que la vida nos puede deparar en cuatro años. Espero que este trabajo sirva para futuras personas que lo encuentren; si le ayuda a alguien a entender alguna parte del método del círculo o del trabajo realizado por Ramanujan, Hardy, Littlewood o Vinogradov, estaré más que contento. Este trabajo contiene no solo horas de esfuerzo, desveladas, sueños y esperanzas, sino también gran parte de mi esencia por enseñar. Mi pasión por la docencia se forjó a lo largo de los años, y la forma en que me gusta desarrollar los temas fue floreciendo con cada semestre, cada materia y cada alumno. Este trabajo también guarda los anhelos de aquel joven que recién entraba a la carrera. Por ello, quiero dejar constancia y agradecerme a mí mismo por llegar hasta aquí: un camino largo, con tropiezos, callejones sin salida, días nublados y soleados, pero que finalmente encuentra su meta. Empezaré a creer en mí mismo.

Gracias a mi madre, Juana Cabrera Ríos, por tantos años cuidando de mí, por esos días en los que dejó su plato vacío para dárnoslo a mis hermanos y a mí. Fue por ella que quería sacar 10 en todo, y así lo logré durante todo el tiempo que viví con ella en mi ciudad natal; su alegría era lo que endulzaba mi corazón. Pero todo tiene un camino a seguir, y a pesar de su tristeza por mi partida para estudiar la carrera de Matemáticas, siempre estuvo de acuerdo en que estudiara lo que yo quisiera, siendo tan resiliente que a veces olvidaba cuidar de sí misma con tal de ofrecerme su apoyo. Siempre recordaré los días trabajando en el parque: fue un año de risas, pláticas y diversión, pasando casi todo el día a su lado. Fue ahí donde dejé de verla solo como mi madre y empecé a conocer a Juana Cabrera como la persona que es, con miedos, sueños, problemas, defectos y virtudes. Agradezco profundamente haber compartido todo ese año con ella antes de irme. A pesar de mi partida, siempre estuvo apoyándome a 2,700 kilómetros de distancia, con ayuda económica en la medida de sus posibilidades, y con palabras de alegría y preocupación al saber que estaba en una ciudad tan grande y lejana. A ella le debo mi segunda pasión: la cocina. Esos días en los que intentaba replicar su sazón, esas llamadas preguntando por ingredientes y recetas, fueron lo que me alimentó durante todo un año, hasta que aprendí y le tomé un verdadero amor a cocinar. Todo esto es gracias a ella, siempre dispuesta a enseñarme y a emocionarse con lo que yo preparaba. Con el tiempo, la vida adulta te consume y te quita tiempo; llegan los problemas personales en los que uno tiene que ver por sí mismo para superarlos, caídas y momentos difíciles. Lamentablemente, eso hizo que mi interacción con ella disminuyera, pero quiero que sepa que la amo y le agradezco de todo corazón por ser mi madre y haberme enseñado el amor incondicional. Esta tesis es para ella.

A mi hermano Víctor Alvarado, le agradezco por haberme formado mis gustos musica-

les y por enseñarme el valor de seguir adelante a pesar de la adversidad. Su perseverancia al estudiar una carrera me inspiró, y su apoyo durante mis primeros semestres fue lo que sostuvo mi vida de foráneo, asegurándose de que nunca me faltara alimento. Siempre ha sido un motivo de enorme gratitud tenerlo cerca, así como su ayuda en cada visita a mi ciudad; un poco gruñón a veces, pero siempre amable. Te agradezco por pensar siempre en nosotros: aunque no seamos los más sentimentales, sabemos que contamos el uno con el otro. Gracias, hermano.

A mis hermanas, Juana Alvarado y Marta Alvarado: gracias por estar ahí siempre, por cuidarme cuando era pequeño y por soportar los momentos difíciles que, aunque yo no recuerdo del todo, sé que sucedieron. Las tengo siempre presentes y siempre es un gusto verlas para compartir pláticas, bromas y ponernos al día.

A mi hermano Francisco Alvarado: gracias por ser parte de mi inspiración para mejorar mi salud. Siempre hemos vivido persiguiendo la sombra el uno del otro; sé que, al igual que yo, viviste momentos difíciles y el camino no siempre es claro, pero sé que puedes encontrar la paz, porque tener esperanza es la mejor forma de vivir. Gracias por ser mi hermano del alma (casi literalmente). Podría decir que fuimos uno solo por mucho tiempo y, aunque cada quien va tomando su propio rumbo, me siento profundamente orgulloso de decir que eres mi gemelo. A pesar de nuestros problemas o discusiones, siempre terminamos ayudándonos. Estar contigo durante la carrera fue lo que la hizo mejor; nuestro equipo de dos nunca falló, y espero que pueda seguir siendo así.

A mi padre, Víctor Alvarado, sin quien no estaría aquí, de una u otra forma. Tal vez nunca nos llegamos a entender en vida, y no fue hasta tiempo después de su partida que comprendí la profunda tristeza en la que vivía, y cómo su forma de ser era, quizá, la única manera que conocía para demostrar su afecto. Le perdono las cosas, aunque no las olvido, y desde aquí le pido disculpas por no habernos entendido.

A mi tío Julio Cabrera, le agradezco haber estado ahí siempre. Era muy grato para mí ir a vender globos, acompañándolo en cada plaza, estar en su casa, en cualquier fiesta a la que nos invitara; los regalos y la ayuda que nos brindó a toda mi familia desde que éramos niños, y su apoyo incondicional a su hermana. No podría pensar en mi infancia sin recordarlo a él: sus invitaciones y su amabilidad siempre me daban alegría. Gracias por cada comida a la que me invitó de niño, gracias por llevarme con usted, gracias por cada encuentro familiar que organizó con tanto esmero, y gracias por su apoyo y palabras de afecto en cada momento de mi vida. Me dio trabajo y respaldo para poder estudiar mi carrera, y a pesar de que tal vez el negocio no daba para mi sueldo, sé que en el fondo era su manera de apoyarnos a todos, como siempre lo ha hecho. Este logro también es por usted, alguien que nunca ha faltado a pesar de la adversidad y de los problemas que ha enfrentado en su propia vida. Por todo esto, siempre lo consideraré un segundo padre para mí.

Finalmente, agradezco a todos mis amigos y amigas que conocí a lo largo de mi tiempo en la facultad (sin un orden específico): Isaac, Emmanuel, Alan, Pedro, Mariana, Carlos, Sandra, Fernando, Eduardo, Miguel, Paulina, Bruno, Ninive y Hugo. Gracias a todos por su amistad, por los momentos y las reuniones compartidas. Estar con ustedes y acompañarlos en sus vidas le dio sentido a la mía en muchísimos momentos. Sobre todo a

mis compañeros de desveladas y sueños, quienes siempre estuvieron ahí más que nadie: Isaac, Emmanuel y Pedro. Espero que esta amistad sea para toda la vida, sin importar que en un futuro nuestros caminos se separen por los estudios. A Ninive, por haberme apoyado durante gran parte de mi carrera mientras luchaba su propia batalla; uno está formado de lo que comparte con los demás, y ella fue parte de mi carrera con mucho cariño.

A mi asesor de tesis, el Dr. Jorge Jiménez Urroz, por su extrema paciencia cada vez que me tardaba en entregarle avances, por su apoyo en los momentos difíciles que pasé escribiendo la tesis y por su amabilidad infinita al acompañarme en todo este proceso sin desistir. Y a todos los sinodales: Gerónimo Uribe, Juan José Alba, Adrián Zenteno y Fidencio Galicia, por la revisión de este trabajo.

Notación y definiciones

- Sea $R \subseteq \mathbb{R}$, denotaremos por $R_{\geq 0} = \{r : r \in R \text{ y } r \geq 0\}$.
- Sea $R \subseteq \mathbb{R}$, denotaremos por $R_{>0} = \{r : r \in R \text{ y } r > 0\}$.
- p denotara números primos. Se entenderá entonces que la notación

$$\sum_{p}, \sum_{p \leq x}, \prod_{p}, \prod_{p \leq x}$$

como sumas y productos sobre números primos.

- $\mathbb{P}$ denotara al conjunto de los números primos.
- Decimos que f es del orden de g, denotado por $f = O(g)$, si existe una constante $C > 0$ y un numero real x_0 tal que

$$|f(x)| \leq C\,|g(x)| \quad \text{para todo} \quad x > x_0$$

- Denotamos por $f \ll g$ para decir que $f = O(g)$.
- Decimos que f es proporcional a g, denotado por $f \asymp g$, si

$$f \ll g \quad \text{y} \quad g \ll f$$

- Decimos que $f$es asintoticamente equivalente a g, denotado por $f \sim g$, si:

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1$$

- Denotaremos para $\alpha \in \mathbb{R}$

$$\binom{\alpha}{k} := \frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!}, \quad \binom{\alpha}{k} = 0 \text{ si } k > \alpha$$

- Dada una serie de potencias

$$f(z) = \sum_{n=0}^{\infty} a_n z^n$$

denotaremos por $[z^n]f(z) = a_n$el coeficiente de z^n.

- Decimos que f es multiplicativa si $f(nm) = f(n)f(m)$ para toda $(n, m) = 1$.

- La **función Phi de Euler** se define como:

$$\varphi(n) = \#\{m : 1 \leq m \leq n,\ (m,n) = 1)\}$$

- La **función divisor** se define como:

$$\sigma_k(n) = \sum_{d|n} d^k$$

- La **función de von Mangoldt** se define como:

$$\Lambda(n) = \begin{cases} \log p & \text{si } n = p^k \text{ para alguna } k \\ 0 & \text{en otro caso} \end{cases}$$

- La **función de Möbius** se define como:

$$\mu(n) = \begin{cases} (-1)^k & \text{si } n = p_1 p_2 \cdots p_k \text{ para alguna } k \\ 0 & \text{en otro caso} \end{cases}$$

- Se define a la sucesión de Fibonacci por $F_0 = 0$, $F_1 = 1$ y $F_{n+2} = F_{n+1} + F_n$ para toda $n \geq 2$.

Introducción

La matemática suele esconder sus misterios más profundos en las operaciones más elementales. La suma, el concepto aritmético más primitivo, da origen a una de las áreas más ricas y complejas de la teoría de números: **la teoría aditiva**. El problema central de esta disciplina puede formularse con asombrosa simplicidad: dado un subconjunto de los números enteros A (como pueden ser los números primos, los cuadrados perfectos o las potencias k-ésimas), **¿Es posible expresar un entero arbitrario n como la suma de elementos de A?** Y, de ser así, **¿De cuántas formas distintas puede lograrse?**

Históricamente, el estudio de este tipo de cuestiones comenzó con una naturaleza fuertemente intuitiva. Las investigaciones clásicas se centraban en garantizar la mera existencia de soluciones para estas ecuaciones aditivas, motivando el trabajo en problemas fundamentales que han guiado el desarrollo del área durante siglos, tales como el estudio de las particiones de un entero, el problema de Waring para potencias o la conjetura de Goldbach. Sin embargo, conforme la teoría fue madurando, la pregunta sobre la existencia de soluciones fue complementada por la necesidad de una comprensión mas exacta. El objetivo analítico pasó a ser entonces la determinación del comportamiento asintótico de la cantidad de representaciones a medida que n crece hacia el infinito, y ya no solo la existencia de estas representaciones.

Este salto hacia la precisión asintótica exige abandonar los métodos estrictamente algebraicos o de conteo elemental. Intentar contar soluciones de manera combinatoria directa se vuelve rápidamente una tarea inmanejable debido al crecimiento exponencial de las formas de representar un numero. Es precisamente en este punto donde la teoría aditiva revela una de sus características más elegantes: la profunda interconexión entre la naturaleza discreta de la aritmética y las herramientas continuas del análisis matemático. Al codificar de los conjuntos de enteros en series de potencias, productos infinitos o sumas exponenciales, las preguntas sobre la suma de números naturales se traducen en problemas sobre el comportamiento de funciones en el plano complejo o el estudio de integrales oscilatorias.

El presente trabajo tiene como propósito explorar esta transición metodológica y conceptual. A lo largo del texto, se examinará cómo el desafío de estimar con precisión el número de representaciones forzó la creación de una maquinaria analítica cada vez más sofisticada. Este recorrido trazará el camino desde los cimientos de la combinatoria formal y algebraica, hasta llegar a la invención y consolidación de herramientas geométricas y trigonométricas finas mediante el Método del Circulo.

En el **primer capítulo** de este trabajo se establecen los fundamentos formales de la teoría aditiva de números, abordándola desde el estudio de las soluciones enteras de ecuaciones aditivas sobre subconjuntos infinitos de los enteros positivos, denotados como $A \subseteq \mathbb{Z}^+$. El desarrollo comienza introduciendo las nociones de representaciones y particiones de un entero n en k partes. La diferencia crucial entre ambos conceptos radica en el

orden de los sumandos: mientras que las representaciones se consideran distintas mediante permutaciones, las particiones se tratan como multiconjuntos donde las permutaciones son consideradas iguales. Para estudiar estas definiciones, nos centramos en su estudio mediante el uso de funciones generadoras:

- **Representaciones:** Su análisis resulta manejable gracias a las propiedades del producto de Cauchy. Se demuestra que la función generadora para el número de representaciones se puede expresar de forma cerrada como $R_{k,A}(z) = f_A^k(z)$, donde $f_A(z)$ es la función de representación del conjunto A, lo que permite obtener identidades y relaciones de recurrencia lineales de manera natural.

- **Particiones:** Al ignorar el orden de los sumandos, la potencia algebraica de las series geométricas se pierde, obligando a emplear funciones generadoras dobles y productos infinitos. Aunque no es factible hallar fórmulas cerradas elementales en el caso general, se deducen expresiones para particiones en 2 y 3 partes, y se construyen relaciones de recurrencia complejas haciendo uso de una generalización de la función divisor, $\sigma_A(n)$, aplicable a conjuntos multiplicativamente cerrados.

Para ilustrar el contraste entre la teoría general y las identidades clásicas, la sección final del capítulo se enfoca en el caso particular $A = \mathbb{Z}^+$. Se obtienen las fórmulas exactas para las representaciones de los enteros, como $r(n) = 2^{n-1}$. En el estudio de las particiones, se revisan los resultados analíticos formulados por Euler, incluyendo la descripción algebraica mediante productos infinitos y el teorema del número pentagonal, del cual se extraen recurrencias explícitas.

El capítulo concluye exponiendo una limitación intrínseca de este método: tratar a las funciones generadoras únicamente como series formales encapsula la información aritmética, pero no ofrece las herramientas necesarias para determinar el comportamiento asintótico del número de representaciones o particiones. Esta barrera histórica es la que justifica la transición hacia el Método del Círculo, trabajado por Hardy y Ramanujan, donde estas series se re interpretan como funciones de variable compleja.

El **segundo capítulo** está dedicado al desarrollo histórico y formal del Método del Círculo, la herramienta analítica central de este trabajo. Se expone cómo este método evolucionó desde un enfoque fundamentado en el análisis complejo hasta convertirse en una técnica puramente aritmética y geométrica basada en sumas trigonométricas.

El capítulo se estructura en tres grandes etapas, reflejando como fue madurando el Método del Circulo históricamente:

- **La introducción de Hardy y Ramanujan:** En esta sección, discutimos como, ante la insuficiencia de los métodos puramente algebraicos, la colaboración entre G. H. Hardy y S. Ramanujan llevó a reinterpretar la función generadora de las particiones, $P(z)$, como una función analítica en el disco unitario. Apoyados en los cálculos empíricos de P. A. MacMahon, desarrollaron una estrategia basada en la fórmula integral de Cauchy y en la "disección de Farey" de la frontera del disco para aislar las singularidades de mayor peso (las raíces de la unidad con denominador pequeño). Esto les permitió formular una célebre aproximación asintótica para $p(n)$, la cual posteriormente fue refinada por H. Rademacher, quien utilizó círculos de Ford para transformar dicha aproximación en una serie convergente al valor exacto.

- **Los trabajos de Hardy y Littlewood:** A continuación, se detalla cómo J. E. Littlewood y Hardy abstrajeron esta idea para abordar el Problema de Waring. En

esta etapa, el método deja de aplicarse a productos infinitos (como en las particiones) y pasa a centrarse en las funciones generadoras de representaciones $R_{k,A}(z)$. Se formaliza aquí la partición del dominio de integración en **Arcos Mayores** —vecindades alrededor de racionales con denominador pequeño donde ocurre interferencia constructiva— y **Arcos Menores** —donde las sumas exponenciales presentan grandes cancelaciones—. Esto permitió establecer asintóticas para la cantidad de representaciones de un entero como suma de potencias k-ésimas, brindando estimaciones precisas para la función $G(k)$.

- **La simplificación de Vinográdov:** Finalmente, se analiza la profunda modificación introducida por I. M. Vinográdov, quien observó las complicaciones técnicas de lidiar con series infinitas y límites cerca del borde del disco unitario. Vinográdov propuso truncar la función de representación, transformando el problema analítico en el estudio de sumas exponenciales finitas $F_A(\alpha, x) = \sum_{a\in A, a\leq x} e(\alpha a)$ evaluadas mediante integrales reales en el intervalo $[0, 1]$.

El trabajo concluye consolidando esta visión moderna, demostrando que la eficacia del método del círculo radica en la dicotomía entre arcos mayores y menores, la cual depende íntimamente de la distribución aritmética del conjunto A en clases de residuos módulo q.

Capítulo 1

Teoría aditiva de números

1.1. Nociones generales

Comencemos con las definiciones básicas de suma aditiva de conjuntos.

Definición 1.1.1

Consideremos A, $B \subset \mathbb{Z}$, definimos el **conjunto suma** $A + B$ como

$$A + B := \{a + b : a \in A,\, b \in B\}$$

similarmente, definimos el **conjunto suma iterada** kA para $k \in \mathbb{Z}^+$ como

$$kA := \{a_1 + a_2 + \cdots + a_k : a_1,\, a_2, ...,\, a_k \in A\}$$

Observación. Para evitar confusiones, utilizaremos un punto $\cdot$ para denotar el producto natural $k \cdot A := \{ka : a \in A\}$.

Algunas preguntas naturales que surgen de dichas definiciones, y que son las que se trabajan en esta área de estudio, son las siguientes:

1. Dado un conjunto $C \subset \mathbb{Z}$, ¿Existen conjuntos A, $B \subset \mathbb{Z}$ tales que $C = A + B$?
2. Dados conjuntos A, $B \subset \mathbb{Z}$, ¿Podemos dar una descripción exacta del conjunto $A + B$?
3. Dados A, $B \subset \mathbb{Z}$, podemos determinar cuando es que $A + B = \mathbb{Z}$? O en su defecto ¿Existirá algún $n_0 \in \mathbb{Z}$ tal que $A + B = \mathbb{Z}_{\geq n_0}$?
4. Dado $n \in A + B$. ¿Cuantas distintas representaciones tiene n como suma de elementos de A y B? ¿Son infinitas o finitas? ¿Como crecen respecto al valor de n?

Todas preguntas totalmente naturales de cuestionarse, por ejemplo, consideremos $A = 2 \cdot \mathbb{Z}$ y $B = 4 \cdot \mathbb{Z}$, entonces

$$A + B = 2 \cdot \mathbb{Z} + 4 \cdot \mathbb{Z} = \{a + b : a \in 2 \cdot \mathbb{Z},\, b \in 4 \cdot \mathbb{Z}\} = \{2x + 4y : x, y \in \mathbb{Z}\}$$

podemos observar que $A + B \neq \mathbb{Z}$ ya que cada elemento del conjunto suma es par, así que $1 \notin A + B$, más aun, dado la infinitud de los números impares tampoco existirá un $n_0 \in \mathbb{Z}$ tal que $A + B = \mathbb{Z}_{\geq n_0}$. Por otro lado, $n \in A + B$ si, y solo si, $n = 2x + 4y$

tiene solución, siendo una ecuación diofantina sabemos que tendrá solución si, y solo si, $(2,4) \mid n$, es decir solo si n es un numero par y, en tal caso, las soluciones serán $y \in \mathbb{Z}$ y $x = {}^{n}/_{2} - 2y$ por lo que todo entero par se puede escribir de esa forma. Estas preguntas se hacen mas interesantes cuando consideramos conjuntos mas elaborados o la suma de varios conjuntos.

La teoría aditiva se divide en el estudio de subconjuntos finitos y dar estimaciones para el tamaño de la suma aditiva de estos o, por otro extremo, el estudio de subconjuntos infinitos de los enteros positivos y estudiar bajo que condiciones la suma aditiva de estos forman a todo $\mathbb{Z}^+$ o a todos a partir de un punto. En este trabajo nos concentraremos unicamente en este segundo caso, aun mas, nos centraremos unicamente en el caso en que los subconjuntos elegidos **son todos el mismo**. Los ejemplos clásicos de esto seria considerar $A = \{k^2 : k \in \mathbb{Z}^+\}$, $B = \mathbb{P}$ de donde, por ejemplo, el teorema de los tres cuadrados de Legendre nos dice que

$$3A = A + A + A = \{n : n \neq 4^a(8b+7),\ a, b \in \mathbb{Z}_{\geq 0}\}$$

es decir, todo numero que no sea de la forma $4^a(8b+7)$ es suma de tres cuadrados, y donde la conjetura fuerte de Goldbach (de la que retomaremos en capítulos posteriores) afirma que

$$2\mathbb{P} = \mathbb{P} + \mathbb{P} = 2 \cdot \mathbb{Z}_{\geq 2}$$

en otras palabras, todo numero par mayor o igual a 4 es suma de dos primos.

Esta manera en que veremos a la teoría aditiva se puede interpretar como la búsqueda de soluciones de ecuaciones en los enteros, pues el teorema de los tres cuadrado de Legendre es equivalente a preguntarse: ¿Para cuales $n \in \mathbb{Z}^+$ existe solución para la ecuación $x_1^2 + x_2^2 + x_3^2 = n$? Es por ello que daremos la siguiente re interpretación a la teoría aditiva de números como el estudio de soluciones enteras de ecuaciones. Para simplificar todo a partir de este momento consideraremos $A \subseteq \mathbb{Z}^+$ infinito y no vació.

Definición 1.1.2

Sean $n, k \in \mathbb{Z}^+$. Llamaremos **ecuación aditiva** en A a una ecuación de la forma:

$$x_1 + x_2 + \cdots + x_k = n$$

donde $x_i \in A$.

Particularmente (como es natural), nos interesaremos en saber cuando es que estas ecuaciones aditivas tienen solución, cuantas soluciones tienen para cada $n \in \mathbb{Z}^+$ fijo, y cuantas tiene con ciertas restricciones. Para ello haremos uso de la siguiente notación.

Definición 1.1.3

Sea $n, k \in \mathbb{Z}^+$. Una **representación** de n en k partes de A es una $k-$eada $(x_1, x_2, ..., x_k) \in A^k$ tal que es solución de la ecuación aditiva $x_1 + x_2 + \cdots + x_k = n$. A la cantidad total de representaciones de n en k partes de A la denotaremos por

$$r_{k,A}(n) := |\{(x_1, x_2, ..., x_k) : x_1 + x_2 + \cdots + x_k = n,\ x_i \in A\}|$$

Ejemplo. $(1, 1, 3, 5)$ es una representación de 10 en 4 partes de impares pues $1+1+3+5 = 10$.

Observación. Podemos notar que el numero de representaciones es sensible a las permutaciones de las soluciones, pues en el ejemplo anterior $(1,1,3,5) \neq (5,3,1,1)$. Sin embargo esto podría considerarse "repetitivo" pues en la practica considerar que $1+1+3+5=10$ es algo diferente a $5+3+1+1=10$ no parece algo muy lógico de hacer, pues unicamente permutamos los sumandos por lo que deberíamos considerarla como la misma. Hacer esto es lo que llamaremos una "Partición".

Definición 1.1.4

Sea $n,k \in \mathbb{Z}^+$. Una **partición** de n en k partes de A es un multiconjunto $[x_1,x_2,...,x_k]$ con $x_i \in A$ tal que es solución de la ecuación aditiva $x_1+x_2+\cdots+x_k = n$. A la cantidad total de particiones de n en k partes de A la denotaremos por

$$p_{k,A}(n) := |\{[x_1,x_2,...,x_k] : x_1+x_2+\cdots+x_k = n,\ x_i \in A\}|$$

La ventaja de usar multiconjuntos es que estos son iguales bajo permutaciones de los elementos. Regresando al ejemplo anterior tendremos que $[1,1,3,5] = [5,3,1,1]$ son la misma partición de 10 en impares.

Ejemplo. $[1,1,2,3,3]$ es una partición de 10 en 5 partes de $\mathbb{Z}^+$.

Observación. Algo claro es que dada una ecuación aditiva $x_1+x_2+\cdots+x_k = n$ con $n,k \in \mathbb{Z}^+$ y $x_i \in A \subseteq \mathbb{Z}^+$ necesariamente se tendrá que entonces $1 \leq x_i < n$ pues en caso contrario el lado izquierdo seria mayor a n, esto también me dice que $r_{k,A}(n) = p_{k,A}(n) = 0$ si $k > n$.

Dadas estas observaciones podemos decidir dos cosas, la primera es que tomaremos la convención:

Para $k=0$, $r_{0,A}(0) = p_{0,A}(0) = 1$ y para $k \geq 1$, definimos $r_{k,A}(0) = p_{k,A}(0) = 0$

Pues la única representación o partición del cero como suma de cero enteros positivos es la vaciá, y para $k \geq 1$ no hay forma de sumar enteros positivos que den cero, lo cual nos sera de utilidad al estudiar funciones generadoras y lo segundo es que hay un numero finito de valores de k tales que $r_{k,A}(n) > 0$ para una n fija, entonces tiene sentido preguntarnos por el numero total de representaciones u particiones de un entero n, a las cuales denotaremos por $r_A(n)$ y $p_A(n)$, es decir para $n \geq 1$,

$$r_A(n) = \sum_{k=1}^{n} r_{k,A}(n) \quad \text{y} \quad p_A(n) = \sum_{k=1}^{n} p_{k,A}(n)$$

y en el caso extremo

$$r_A(0) = p_A(0) = 1$$

En la mayor parte de este documento consideraremos $k,n \geq 1$ pero cuando estudiemos funciones generadoras en la Sección 1.2 y 1.3 sera importante recordar estas definiciones. Con todo esto definido, podemos dar resultados elementales respecto al numero de representaciones y particiones sobre un subconjunto A de los enteros positivos. Dado que cada $1 \leq x_i < n$, tendremos las estimaciones directas (pero muy ineficaces)

$$r_{k,A}(n) < n^k \quad \text{y} \quad p_{k,A}(n) < \frac{n^k}{k!}$$

la primera se da, pues para cada x_i hay a lo mas n posibles elecciones y esto para cada una de las k variables, y la segunda se da pues en cada elección de los x_i estamos contando también las permutaciones de estas soluciones las cuales son $k!$. Pero como se menciono, esta cota superior es muy grande, podemos notarlo considerando $A = 2 \cdot \mathbb{Z}^+$, de donde $r_{3,A}(10) = 6$ y $p_{3,A}(10) = 2$ pues

$$10 = \begin{cases} 2+2+6 \\ 2+6+2 \\ 6+2+2 \\ 2+4+4 \\ 4+2+4 \\ 4+4+2 \end{cases}$$

y nuestra cota superior nos da $r_{3,A}(10) < 10^3 = 1000$ y $p_{3,A}(10) < {}^{10^3}/_{3!} = 166.\overline{6}$ las cuales son muy grandes a comparación del valor real, por lo que necesitaremos refinar mas esta cota superior. La "ventaja" de esta cota es que no depende del conjunto A que escojamos, pero como vemos esto no nos es de mucha ayuda. Para estimar o dar una cota superior mas refinada necesitaremos saber las propiedades aritméticas del conjunto A, sin embargo en el caso general esto no es posible. Pero lo que si podemos hacer es dar una estimación considerando el valor general de los posibles valores que pueden tomar las variables x_i.

Definición 1.1.5

Definimos a la función contadora de A como

$$\pi_A(x) := |\{n \leq x : n \in A\}| = \sum_{\substack{n \leq x \\ n \in A}} 1 = \sum_{n \leq x} \delta_A(n)$$

donde

$$\delta_A(n) := \begin{cases} 1 & \text{si } n \in A \\ 0 & \text{si } n \notin A \end{cases}$$

Con esto podemos dar una mejor cota superior para el numero de representaciones y particiones ya que dada una representación $(x_1, ..., x_k)$ de n de elementos de A, tenemos que cada x_i tiene $\pi_A(n)$ posibles valores a escoger, y como esto es para cada una de las variables, tendremos que

$$r_{k,A}(n) < \pi_A(n)^k \quad \text{y} \quad p_{k,A}(n) < \frac{\pi_A(n)^k}{k!}$$

en el caso en que $A = 2 \cdot \mathbb{Z}^+$ podemos dar una formula exacta para $\pi_A(n)$, pues la cantidad de números pares menores que un entero positivo n no es mas que $\lfloor \frac{n}{2} \rfloor$, es decir, $\pi_A(n) = \lfloor \frac{n}{2} \rfloor$ por lo que nuestra nueva estimación nos queda

$$r_{3,A}(10) < \left\lfloor \frac{10}{2} \right\rfloor^3 = 125 \quad \text{y} \quad p_{3,A}(10) < \frac{\lfloor \frac{10}{2} \rfloor^3}{3!} = 20.8\overline{3}$$

para la cual es de discusión afirmar si es mejor o no, pero si obtenemos valores mas "cercanos" al valor real. Este alejamiento de nuestra cota superior al valor real nos refleja algo que no hemos considerado, es el hecho de la delicadeza que tiene el numero de

representaciones o particiones a la cantidad de partes, por ejemplo, es bien conocido el teorema de los tres cuadrados de Legendre y el de los cuatro cuadrados de Legendre los cuales establecen que dado $n \in \mathbb{Z}^+$:

$$\begin{array}{cc} n = x^2 + y^2 + z^2 & \text{si y solo si } n \neq 4^a(8b+7),\ a, b \in \mathbb{Z}_{\geq 0} \\ n = x^2 + y^2 + z^2 + w^2 & \text{valido para toda } n \end{array}$$

por lo que en ese sentido si consideramos $B = \{n^2 : n \in \mathbb{Z}_{\geq 0}\}$ entonces afirman que

$$\begin{array}{c} r_{3,B}(n) > 0 \text{ si y solo si } n \neq 4^a(8b+7),\ a, b \in \mathbb{Z}^+ \\ r_{4,B}(n) > 0 \text{ para toda } n \end{array}$$

siendo evidente el cambio drástico de considerar 3 partes a 4 partes. También el numero de partes nos da información sobre la cantidad de valores posibles para las variables x_i, pues dada una representación u partición en 2 partes, el valor de x_1 me determinara de manera completa el valor de x_2, pues $x_1 + x_2 = n \Rightarrow x_2 = n - x_1$, por lo que concluimos que

$$r_{2,A}(n) \leq \pi_A(n) \quad \text{y} \quad p_{2,A}(n) \leq \frac{\pi_A(n)}{2!}$$

y con el mismo argumento dada una representación u partición en 3 partes, una vez elegido el valor de x_1 tendremos que $x_2 + x_3 = n - x_1$ y como x_1 es al menos 1, entonces escoger un valor para x_2 entre los primeros $n-1$ números me determinara el valor de x_3,de donde

$$r_{3,A}(n) \leq \pi_A(n)\pi_A(n-1) \quad \text{y} \quad p_{3,A}(n) \leq \frac{\pi_A(n)\pi_A(n-1)}{3!}$$

comparando nuevamente con nuestro caso $A = 2 \cdot \mathbb{Z}^+$ obtenemos

$$r_{3,A}(10) \leq \left\lfloor \frac{10}{2} \right\rfloor \left\lfloor \frac{9}{2} \right\rfloor = 20 \quad \text{y} \quad p_{3,A}(10) \leq \frac{\left\lfloor \frac{10}{2} \right\rfloor \left\lfloor \frac{9}{2} \right\rfloor}{3!} = 3.\overline{3}$$

siendo una clara mejoría a los dos anteriores.

Si bien podemos hacer cálculos mas detallados para obtener cotas superiores mas exactas, esto no es en lo que nos enfocaremos en este documento.

1.2. Representaciones

Otra forma muy usual en combinatoria de trabajar con sucesiones de números enteros (pues el numero de representaciones u particiones lo son), son las **funciones generadoras**. En las dos próximas secciones, trataremos las funciones generadoras como series formales de potencias. Esto significa que los resultados obtenidos serán una identidad sobre los coeficientes, la cual se justifica por la definición del producto de series, sin necesidad de analizar su convergencia. En el capitulo siguiente, al trabajar con el Método del Circulo, sera necesario re interpretar estas series como funciones analíticas, cuya convergencia sera analizada formalmente.

¿Como las funciones generadores nos ayudaran? Esto es, sencillamente, porque hay una forma de extraer los coeficientes de una función generadora. Si $f(z) = \sum_{n=0}^{\infty} a_n z^n$ entonces

$$a_n = [z^n]f(z) = \frac{f^{(n)}(0)}{n!}$$

de esta manera, poder encontrar una expresión cerrada para la función generadora nos dará una forma de obtener nuestra sucesión buscada.

La función generadora para el numero de representaciones lo podremos obtener de forma sencilla usando un resultado clásico en series, el llamado **producto de Cauchy**.

$$\left(\sum_{n=0}^{\infty} a_n\right)\left(\sum_{n=0}^{\infty} b_n\right) = \sum_{n=0}^{\infty}\left(\sum_{\substack{k+m=n\\ k,m\geq 0}} a_k b_m\right) = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} a_k b_{n-k}\right)$$

de donde es fácil generalizar, obteniendo

$$\left(\sum_{n=0}^{\infty} a_n^{(1)}\right)\left(\sum_{n=0}^{\infty} a_n^{(2)}\right)\cdots\left(\sum_{n=0}^{\infty} a_n^{(k)}\right) = \sum_{n=0}^{\infty}\left(\sum_{\substack{x_1+x_2+\cdots+x_k=n\\ x_i\geq 0}} a_{x_1}^{(1)} a_{x_2}^{(2)}\cdots a_{x_k}^{(k)}\right)$$

Esto es suficiente para poder encontrar las función generadora de $r_{k,A}(n)$ y $r_A(n)$.

Teorema 1.2.1

Para el numero de representaciones en k partes y totales de A, sus funciones generadoras vienen dadas por

$$R_{k,A}(z) := \sum_{n=0}^{\infty} r_{k,A}(n) z^n = \left(\sum_{a\in A} z^a\right)^k$$
$$R_A(z) := \sum_{n=0}^{\infty} r_A(n) z^n = \frac{\sum_{a\in A} z^a}{1-\sum_{a\in A} z^a}$$

Demostración. Considerando la suma $\sum_{a\in A} z^a = \sum_{n=0}^{\infty} \delta_A(n) z^n$, tendremos por el producto de Cauchy

$$\left(\sum_{a\in A} z^a\right)^k = \left(\sum_{n=0}^{\infty} \delta_A(n) z^n\right)^k = \sum_{n=0}^{\infty}\left(\sum_{\substack{x_1+x_2+\cdots+x_k=n\\ x_i\geq 0}} \delta_A(x_1)\delta_A(x_2)\cdots\delta_A(x_k)\right) z^n$$

y notando que el sumando interior no es cero unicamente si tenemos una solución de la ecuación $x_1+x_2+\cdots+x_k = n$ donde $x_i \geq 0$ y $x_i \in A$, tenemos pues que nos da el numero de representaciones de n en k partes de A, por lo que

$$\left(\sum_{n=0}^{\infty} \delta_A(n) z^n\right)^k = \sum_{n=0}^{\infty} r_{k,A}(n) z^n$$

por lo tanto

$$R_{k,A}(z) = \sum_{n=0}^{\infty} r_{k,A}(n) z^n = \left(\sum_{a\in A} z^a\right)^k$$

Por otro lado, dado que

$$R_A(z) := \sum_{n=0}^{\infty} r_A(n) z^n = \sum_{n=0}^{\infty} \left(\sum_{k=1}^{n} r_{k,A}(n) \right) z^n = \sum_{n=0}^{\infty} \left(\sum_{k=1}^{\infty} r_{k,A}(n) \right) z^n$$
$$= \sum_{k=1}^{\infty} \sum_{n=0}^{\infty} r_{k,A}(n) z^n = \sum_{k=1}^{\infty} \left(\sum_{a \in A} z^a \right)^k = \frac{\sum_{a \in A} z^a}{1 - \left(\sum_{a \in A} z^a \right)}$$

□

Observación. Unos valores especiales a tener en cuenta en las cuentas son: $R_{0,A}(0) = 1$ y para $k \geq 1$, $R_{k,A}(0) = 0$. Igualmente $R_A(0) = 1$.

Como vemos, para el caso del numero de representaciones todo se basara en poder encontrar una expresión cerrada para la suma $\sum_{a \in A} z^a$, la cual (nuevamente) dependerá de las propiedades aritméticas del conjunto A. Esta función sera usada múltiples veces en los próximos capítulos, es por ello que la definiremos formalmente.

Definición 1.2.1

Sea $A \subseteq \mathbb{Z}^+$ infinito, definimos la **función de representación** de A como

$$f_A(z) := \sum_{a \in A} z^a$$

Donde el resultado anterior lo podremos reescribir como

$$R_{k,A}(z) = f_A^k(z) \tag{1.2.1}$$

$$R_A(z) = \frac{f_A(z)}{1 - f_A(z)} \tag{1.2.2}$$

Observación. Dependiendo del conjunto podemos obtener su función de representación en forma cerrada o no, por ejemplo, si $A = \mathbb{Z}^+$y $B = \mathbb{P}$ entonces fácilmente,

$$f_A(z) = \sum_{n \in \mathbb{Z}^+} z^n = \frac{z}{1 - z}$$

pero de manera contraria $f_B(z)$ no tiene una formula cerrada elemental[1].

Ejemplo. Un ejemplo interesante es el caso en que $\mathscr{A} = 2 \cdot \mathbb{Z}_{\geq 0} + \{1\}$, es decir, el conjunto de impares. ¿Cual es el numero de representaciones de un $n \in \mathbb{Z}^+$ como suma de impares? La función de representación de los impares sera

$$f_{\mathscr{A}}(z) = \sum_{n=0}^{\infty} z^{2n+1} = z \sum_{n=0}^{\infty} (z^2)^n = \frac{z}{1 - z^2}$$

[1]Con métodos más avanzados, como la fórmula de suma de Abel, es posible expresar $f_B(z)$ mediante una integral de Riemann-Stieltjes respecto a la función contadora de primos $\pi(x)$. Sin embargo, dicha representación no resulta práctica en este contexto. Para una discusión sobre la formula de sumación y funciones aritméticas, véase el capitulo 4 de [20].

así, por 1.2.1 y 1.2.2

$$R_{k,\mathscr{A}}(z) = f^k_{\mathscr{A}}(z) = \left(\frac{z}{1-z^2}\right)^k = \frac{z^k}{(1-z^2)^k}$$

$$R_{\mathscr{A}}(z) = \frac{\frac{z}{1-z^2}}{1-\frac{z}{1-z^2}} = \frac{z}{1-z-z^2}$$

de donde, para el numero de representaciones obtenemos la bien conocida función generadora de los números de Fibonacci

$$\sum_{m=0}^{\infty} F_m z^m = \frac{z}{1-z-z^2}$$

entonces,

$$r_{\mathscr{A}}(n) = [z^n]R_{\mathscr{A}}(z) = [z^n]\frac{z}{1-z-z^2} = [z^n]\sum_{m=0}^{\infty} F_m z^m = F_n$$

es decir, el numero de representaciones de n como suma de impares es F_n. Por ejemplo para $n = 6$ tenemos que $r_{\mathscr{A}}(6) = F_6 = 8$ y efectivamente

$$\begin{aligned} 6 &= 1+1+1+1+1+1 \\ &= 3+1+1+1 \\ &= 1+3+1+1 \\ &= 1+1+3+1 \\ &= 1+1+1+3 \\ &= 3+3 \\ &= 5+1 \\ &= 1+5 \end{aligned}$$

Para el numero de representaciones en k partes, se necesita un análisis mas especifico, tenemos por el teorema del binomio generalizado

$$\begin{aligned} R_{k,\mathscr{A}}(z) &= \frac{z^k}{(1-z^2)^k} = z^k(1-z^2)^{-k} = z^k\sum_{m=0}^{\infty}\binom{-k}{m}(-1)^m z^{2m} \\ &= z^k\sum_{m=0}^{\infty}(-1)^m\binom{m+k-1}{m}(-1)^m z^{2m} = z^k\sum_{m=0}^{\infty}\binom{m+k-1}{m}z^{2m} \end{aligned}$$

entonces,

$$\begin{aligned} r_{k,\mathscr{A}}(n) &= [z^n]R_{k,\mathscr{A}}(z) = [z^n]\left(z^k\sum_{m=0}^{\infty}\binom{m+k-1}{m}z^{2m}\right) \\ &= [z^{n-k}]\sum_{m=0}^{\infty}\binom{m+k-1}{m}z^{2m} = \begin{cases}\binom{(n-k)/2+k-1}{(n-k)/2} & \text{si } n-k=2m \text{ para alguna } m\in\mathbb{Z} \\ 0 & \text{en otro caso}\end{cases} \\ &= \begin{cases}\binom{m+k-1}{k-1} & \text{si } n-k=2m \text{ para alguna } m\in\mathbb{Z} \\ 0 & \text{en otro caso}\end{cases} \end{aligned}$$

por ejemplo, si $n = 6$ y $k = 2$, entonces $n - k = 4$, por lo que $r_{2,A}(6) = \binom{2+2-1}{2-1} = 3$ y efectivamente

$$6 = 3 + 3 = 1 + 5 = 5 + 1$$

Para valores particulares obtenemos relaciones interesantes, por ejemplo, para $k = 2$ las representaciones serán no cero sobre los pares,

$$r_{2,\mathscr{A}}(n) = \frac{n}{2}\delta_{\mathbb{Z}}\left(\frac{n}{2}\right)$$

Para $k = 3$ obtenemos que la suma sera no cero siempre que n sea impar, y la formula nos da que

$$r_{3,\mathscr{A}}(n) = \binom{(n-3)/2 + 2}{(n-3)/2}\delta_{\mathbb{Z}}\left(\frac{n-1}{2}\right) = \binom{(n-1)/2}{2}\delta_{\mathbb{Z}}\left(\frac{n-1}{2}\right) = T_{(n-1)/2}\delta_{\mathbb{Z}}\left(\frac{n-1}{2}\right)$$

siendo $T_m = \binom{m}{2}$ los llamados **números triangulares** para n impar. Pero con la formula obtenida podemos entender quien es en general $r_{k,\mathscr{A}}(n)$. Para $n \equiv k \pmod 2$, $r_{k,\mathscr{A}}(n)$ son los **números poliédricos**[2] definidos mediante $P_q(m) = \binom{m+q}{q}$, de forma mas exacta obtenemos que si $n \equiv k \pmod 2$ entonces

$$\boxed{r_{k,\mathscr{A}}(n) = P_{k-1}\left(\frac{n-k}{2}\right)}$$

Más aún, este último resultado también nos da una equivalencia interesante, entre los números de Fibonacci y los números poliédricos

$$F_n = r_{\mathscr{A}}(n) = \sum_{k=1}^{n} r_{k,\mathscr{A}}(n) = \sum_{\substack{1\le k\le n \\ n-k=2m}} \binom{m+k-1}{k-1} = \sum_{\substack{1\le k\le n \\ n-k=2m}} P_{k-1}(m)$$

Las funciones generadoras también nos ayudan a encontrar relaciones de recurrencia entre sus coeficientes, en nuestro caso podemos obtener algunas muy generales.

Proposición 1.2.1

El numero de representaciones cumple las siguientes relaciones de recurrencia

$$r_{k+1,A}(n) = \sum_{a\in A,\, a\le n} r_{k,A}(n-a) \tag{1.2.3}$$

$$r_A(n) = \delta_A(n) + \sum_{a\in A,\, a\le n} r_A(n-a) \tag{1.2.4}$$

Demostración. Por 1.2.1 tenemos

$$R_{k+1,A}(z) = f_A^{k+1}(z) = f_A(z)f_A^k(z) = f_A(z)R_{k,A}(z)$$

[2]En la literatura tienen distintos nombres, entre ellos; Números Simples, Números Figurativos, Números Politópicos. Pero es mas usual encontrarlos como Figurate Numbers.

entonces por el producto de Cauchy

$$r_{k+1,A}(n) = [z^n]R_{k+1,A}(z) = [z^n]f_A(z)R_{k,A}(z) = \sum_{i+j=n} \delta_A(i)r_{k,A}(j) = \sum_{a\in A,\, a<n} r_{k,A}(n-a)$$

De forma similar por 1.2.2

$$R_A(z) = \frac{f_A(z)}{1-f_A(z)} \;\Rightarrow\; f_A(z) = (1-f_A(z))R_A(z) \;\Rightarrow\; R_A(z) = f_A(z) + f_A(z)R_A(z)$$

por lo cual

$$\begin{aligned} r_A(n) = [z^n]R_A(z) &= [z^n]\left[f_A(z) + f_A(z)R_A(z)\right]) = \delta_A(n) + \sum_{i+j=n} \delta_A(i)r_A(j) \\ &= \delta_A(n) + \sum_{a\in A,\, a<n} r_A(n-a) \end{aligned}$$

□

Regresando a nuestro ejemplo de los impares. De la relación 1.2.4 obtenemos

$$\begin{aligned} F_n = r_{\mathscr{A}}(n) &= \delta_{\mathscr{A}}(n) + \sum_{a\in\mathscr{A},\, a\le n} r_{\mathscr{A}}(n-a) = \delta_{\mathscr{A}}(n) + \sum_{a\in\mathscr{A},\, a\le n} F_{n-a} \\ &= \begin{cases} F_1 + F_3 + \cdots + F_{n-3} + F_{n-1} & \text{si } n \text{ par} \\ 1 + F_2 + F_4 + \cdots + F_{n-3} + F_{n-1} & \text{si } n \text{ impar} \end{cases} \end{aligned}$$

Escribir la relación para el numero de representaciones en k partes se vuelve mas complicado.

A partir de los resultados anteriores podría parecer que, al tomar como ejemplo el conjunto de los enteros impares, deberíamos obtener de forma inmediata la conocida relación de recurrencia que satisface la sucesión de Fibonacci ($F_{n+2} = F_{n+1} + F_n$). Sin embargo, esto no ocurre. La razón es que la fórmula general que obtuvimos expresa $r_A(n)$ como una suma que depende de toda la estructura del conjunto A. Por lo tanto, la posibilidad de simplificarla y obtener una recurrencia explícita depende de propiedades aritméticas particulares del conjunto que estemos considerando. Esto se hace evidente cuando retomamos el caso concreto de los impares. Utilizando que $R_{\mathscr{A}}(z) = \frac{z}{1-z-z^2}$ de donde

$$R_{\mathscr{A}}(z)(1-z-z^2) = z \;\Rightarrow\; R_{\mathscr{A}}(z) - zR_{\mathscr{A}}(z) - z^2R_{\mathscr{A}}(z) = z$$

y entonces para $n \le 2$,

$$\begin{aligned} [z^n]\left[R_{\mathscr{A}}(z) - zR_{\mathscr{A}}(z) - z^2R_{\mathscr{A}}(z) = z\right] &= [z^n]z \\ \Rightarrow\; r_{\mathscr{A}}(n) - r_{\mathscr{A}}(n-1) - r_{\mathscr{A}}(n-2) &= 0 \end{aligned}$$

obteniendo la formula de recurrencia usual.

En conclusión, hemos visto como el estudiar las series formales del número de representaciones nos permite dar relaciones directas como $R_{k,A}(z) = f_A^k(z)$ y recurrencias lineales manejables. Esta "simplicidad" algebraica surge precisamente de distinguir el orden de los sumandos, lo que alinea perfectamente la combinatoria con el producto de Cauchy. Sin embargo, veremos que al considerar el orden de los sumandos importante (particiones) perderemos esta potencia algebraica que nos daban las series geométricas y la función de representación de A, y nos orillara a hacer uso de productos infinitos, aumentando considerablemente la complejidad del análisis y requiriendo nuevas herramientas para extraer información sobre sus coeficientes.

1.3. Particiones

Para el caso de particiones la situación cambia bastante al querer obtener "formulas cerradas" para sus funciones generadoras, pues sera necesario hacer uso del conteo y de una función generadora doble en el caso de las particiones en k partes. .

Teorema 1.3.1

Las funciones generadora del numero de particiones en k partes de A, vienen dadas por

$$P_{k,A}(z) := \sum_{n=0}^{\infty} p_{k,A}(n) z^n = [t^k] \prod_{a \in A} \left(\frac{1}{1 - tz^a} \right)$$

$$P_A(z) := \sum_{n=0}^{\infty} p_A(n) z^n = \prod_{a \in A} \left(\frac{1}{1 - z^a} \right)$$

Demostración. Procediendo de forma general para $p_A(n)$. Consideramos cuantas veces usamos cada elemento del conjunto A en nuestra partición, dado que cada termino z^a nos dará un sumando de nuestra partición para cada producto que hagamos tendremos que, si el elemento a aparece cero veces contribuirá con un factor de 1 $(z^{0 \cdot a})$, si aparece una vez con un factor de z^a, si aparece dos veces con un factor de z^{2a} y así sucesivamente, entonces la serie que me representa todas las posibles opciones para un único elemento $a \in A$ es:

$$1 + z^a + z^{2a} + \cdots = \sum_{n=0}^{\infty} z^{na} = \frac{1}{1 - z^a}$$

De esta manera, como nuestra partición estará formada por todos los posibles sumandos del conjunto A y una elección de un elemento es independiente de otro, tendremos que la función generadora vendrá dada por el producto de cada serie geométrica, siendo pues

$$P_A(z) := \sum_{n=0}^{\infty} p_A(n) z^n = \prod_{a \in A} \left(\frac{1}{1 - z^a} \right)$$

Para la función generadora del numero de particiones en k partes de A haremos uso de un marcador, el cual nos contara la cantidad de partes utilizadas en cada partición. Esto lo lograremos utilizando una doble función generadora, donde

$$P_A(t, z) := \sum_{k=0}^{\infty} \sum_{n=0}^{\infty} p_{k,A}(n) z^n t^k \Rightarrow P_{k,A}(z) = [t^k] P_A(t, z)$$

Aquí, el razonamiento es similar, notemos que si queremos contar a la vez la cantidad de veces que aparece un sumando a en la partición y las veces que lo usamos vasta agregar el factor de t correspondiente, siendo que si a aparece cero veces contribuirá con un factor de 1 $(t^0 z^{0 \cdot a})$, si aparece una vez con un factor de tz^a, si aparece dos veces con un factor de $t^2 z^{2a}$ y así sucesivamente, donde t nos va marcando la cantidad de veces que fue usando el elemento a. Entonces para cada elemento a la serie que me representa todas sus posibles opciones y veces usadas es

$$1 + tz^a + t^2 z^{2a} + \cdots = \sum_{n=0}^{\infty} t^n z^{na} = \frac{1}{1 - tz^a}$$

multiplicando todos estos factores para cada $a \in A$, el exponente de z es la suma de las partes, y el exponente de t es la suma de cuantas partes se usaron, por lo tanto

$$P_A(t,z) = \prod_{a\in A}\left(\frac{1}{1-tz^a}\right) \Rightarrow P_{k,A}(z) = [t^k]\prod_{a\in A}\left(\frac{1}{1-tz^a}\right)$$

□

Observación. Similarmente para el caso de representaciones, valores especiales a tener en cuenta en las cuentas son: $P_{0,A}(0) = 1$ y para $k \geq 1$, $P_{k,A}(0) = 0$. Igualmente $P_A(0) = 1$.

Las particiones totales constituyen un problema extremadamente complejo: no contamos con ningún caso verdaderamente sencillo del cual podamos extraer una fórmula cerrada para la función generadora. Por ello (a diferencia de las representaciones), este método algebraico basado en funciones generadoras, que en un principio parece prometedor, se vuelve rápidamente inútil para obtener estimaciones del número de particiones en la mayoría de los casos. En esta misma línea, también resulta algo desalentador el hecho de que, incluso cuando intentamos obtener una fórmula para el número de particiones en k partes, esta termina dependiendo del coeficiente en la variable t dentro de una función generadora doble. Si bien es cierto que dicho coeficiente podría determinarse derivando sucesivamente k veces y luego evaluando en $t = 0$, esto conduciría a una expresión general cuyo valor práctico sería casi nulo o sumamente complicada.

No obstante, sí es posible obtener formas explícitas de las funciones generadoras para particiones en pequeñas partes, especialmente en 2 y 3 partes, las cuales serán de utilidad en secciones posteriores. Es por ello que haremos una breve revisión de esos casos específicos que nos interesan, junto con una mirada preliminar al caso general, notando que los resultados obtenidos dependerán de nuestra función de representación $f_A(z)$, lo cual nos vuelve a decir que dicha función (de cierta manera) nos encapsula la información aritmética del conjunto A.

Proposición 1.3.1

El numero de particiones en 2 y 3 partes tienen como función generadora

$$P_{2,A}(z) = \frac{1}{2}\left(f_A^2(z) + f_A(z^2)\right) \tag{1.3.1}$$

$$P_{3,A}(z) = \frac{1}{6}\left(f_A^3(z) + 3f_A(z)f_A(z^2) + 2f_A(z^3)\right) \tag{1.3.2}$$

Demostración. Por el **Teorema 1.3.1**

$$P_{2,A}(z) = [t^2]\prod_{a\in A}\left(\frac{1}{1-tz^a}\right) = [t^2]P_A(t,z)$$

Llamemos $G(t,z) = \log P_A(t,z)$, entonces

$$G(t,z) = -\sum_{a\in A}\log\left(1-tz^a\right)$$

de donde derivando respecto a t

$$G'(t,z) = \sum_{a\in A}\frac{z^a}{1-tz^a}, \quad G''(t,z) = \sum_{a\in A}\frac{z^{2a}}{(1-tz^a)^2}, \quad G'''(t,z) = 2\sum_{a\in A}\frac{z^{3a}}{(1-tz^a)^2}$$

y evaluando en $t = 0$ se obtiene

$$G'(0,z) = \sum_{a\in A} z^a = f_A(z), \quad G''(0,z) = \sum_{a\in A} z^{2a} = f_A(z^2)$$

$$G'''(0,z) = 2\sum_{a\in A} z^{3a} = 2f_A(z^3)$$

Ahora, como $P_A(t,z) = \exp\left(G(t,z)\right)$ tendremos

$$\begin{aligned} P'_A &= P_A \cdot G' \\ P''_A &= P_A \cdot \left((G')^2 + G''\right) \\ P'''_A &= P_A \cdot \left((G')^3 + 3G'G'' + G'''\right) \end{aligned}$$

de donde, para las particiones en dos partes

$$\begin{aligned} P_A(z) = [t^2]P_A(t,z) &= \frac{P_A^{(2)}(0,z)}{2!} \\ &= \frac{P_A(0,z)\left((G'(0,z))^2 + G''(0,z)\right)}{2!} \\ &= \frac{1}{2}\left(f_A^2(z) + f_A(z^2)\right) \end{aligned}$$

y para las particiones en tres partes

$$\begin{aligned} P_A(z) = [t^3]P_A(t,z) &= \frac{P_A^{(3)}(0,z)}{3!} \\ &= \frac{P_A(0,z)\left((G'(0,z))^3 + 3G'(0,z)G''(0,z) + G'''(0,z)\right)}{3!} \\ &= \frac{1}{6}\left(f_A^3(z) + 3f_A(z)f_A(z^2) + 2f_A(z^3)\right) \end{aligned}$$

□

Este es un resultado sumamente interesante, para poder ver su eficacia regresemos a nuestro ejemplo con los números impares donde obtendremos las formulas para particiones en dos y tres partes.

Ejemplo. Para el caso de impares, retomando

$$f_{\mathscr{A}}(z) = \frac{z}{1-z^2}$$

entonces por 1.3.1

$$\begin{aligned} p_{2,\mathscr{A}}(n) = [z^n]P_{2,\mathscr{A}}(z) &= [z^n]\left[\frac{1}{2}\left(f_{\mathscr{A}}^2(z) + f_{\mathscr{A}}(z^2)\right)\right] \\ &= \frac{1}{2}\left([z^n]f_{\mathscr{A}}^2(z) + [z^n]f_{\mathscr{A}}(z^2)\right) \\ &= \frac{1}{2}\left(r_{2,\mathscr{A}}(n) + \delta_{\mathscr{A}}(\frac{n}{2})\right) \\ &= \frac{1}{2}\left(\frac{n}{2}\delta_{\mathbb{Z}}(\frac{n}{2}) + \delta_{\mathscr{A}}(\frac{n}{2})\delta_{\mathbb{Z}}(\frac{n}{2})\right) \\ &= \frac{1}{2}\left(\frac{n}{2} + \delta_{\mathscr{A}}(\frac{n}{2})\right)\delta_{\mathbb{Z}}(\frac{n}{2}) \end{aligned}$$

pero podemos notar que para $n = 2k$ tendremos $p_{2,\mathscr{A}}(2k) = \frac{1}{2}(k + \delta_{\mathscr{A}}(k))$ por lo que unicamente le sumamos 0 o $\frac{1}{2}$dependiendo si k es impar o no, pero esto es justamente $\lceil \frac{k}{2} \rceil$, pero al ser $n = 2k$ obtenemos

$$\boxed{p_{2,\mathscr{A}}(n) = \left\lceil \frac{n}{4} \right\rceil \delta_{\mathbb{Z}}(\frac{n}{2})}$$

Podemos ver algunos valores, para $n = 4, 6, 8$, sus particiones en dos partes de impares serán:

$$\begin{aligned} 4 &= 1 + 3 \\ 6 &= 1 + 5 = 3 + 3 \\ 8 &= 1 + 7 = 3 + 5 \end{aligned}$$

y siendo que, efectivamente, $\lceil \frac{4}{4} \rceil = 1, \lceil \frac{6}{4} \rceil = 2, \lceil \frac{8}{4} \rceil = 2$.

Para las particiones en tres partes, por 1.3.2 tendremos

$$\begin{aligned} p_{3,\mathscr{A}}(n) &= [z^n]P_{3,\mathscr{A}}(z) = [z^n]\left[\frac{1}{6}\left(f^3_{\mathscr{A}}(z) + 3f_{\mathscr{A}}(z)f_{\mathscr{A}}(z^2) + 2f_{\mathscr{A}}(z^3)\right)\right] \\ &= \frac{1}{6}\left([z^n]f^3_{\mathscr{A}}(z) + 3[z^n]f_{\mathscr{A}}(z)f_{\mathscr{A}}(z^2) + 2[z^n]f_{\mathscr{A}}(z^3)\right) \\ &= \frac{1}{6}\left(r_{3,\mathscr{A}}(n) + 3[z^n]f_{\mathscr{A}}(z)f_{\mathscr{A}}(z^2) + 2\delta_{\mathscr{A}}(\frac{n}{3})\right) \end{aligned}$$

en la parte central hacemos uso del producto de Cauchy,

$$\begin{aligned} p_{3,\mathscr{A}}(n) &= \frac{1}{6}\left(r_{3,\mathscr{A}}(n) + 3\left(\sum_{k=0}^{n} \delta_{\mathscr{A}}(n)\delta_{\mathscr{A}}(\frac{n-k}{2})\right) + 2\delta_{\mathscr{A}}(\frac{n}{3})\right) \\ &= \frac{1}{6}T_{(n-1)/2}\delta_{\mathbb{Z}}(\frac{n-1}{2}) + \frac{1}{2}\left(\sum_{k=0}^{n} \delta_{\mathscr{A}}(k)\delta_{\mathscr{A}}(\frac{n-k}{2})\right) + \frac{1}{3}\delta_{\mathscr{A}}(\frac{n}{3}) \end{aligned}$$

simplificando la suma interna, considerando solo las m tales que $\frac{n-k}{2} = m \in \mathbb{Z}^+$

$$p_{3,\mathscr{A}}(n) = \frac{1}{6}T_{(n-1)/2}\delta_{\mathbb{Z}}(\frac{n-1}{2}) + \frac{1}{2}\left(\sum_{0 \le m \le \frac{n}{2}} \delta_{\mathscr{A}}(n-2m)\delta_{\mathscr{A}}(m)\right) + \frac{1}{3}\delta_{\mathscr{A}}(\frac{n}{3})$$

mas aun, notemos que la suma central es sobre los impares entre 0 y $\frac{n}{2}$, pero la paridad de $n - 2m$ unicamente depende de n, por lo cual si n es par, $n - 2m$ es par y cada sumando sera 0, en cambio si n es impar, $n - 2m$ es impar y entonces cada sumando sera 1 obteniendo entonces la cantidad de impares entre 0 y $\frac{n}{2}$ lo cual es $\lceil \frac{n-1}{4} \rceil$, por lo tanto

$$\boxed{p_{3,\mathscr{A}}(n) = \frac{1}{6}T_{(n-1)/2}\delta_{\mathbb{Z}}(\frac{n-1}{2}) + \frac{1}{2}\left\lceil \frac{n-1}{4} \right\rceil \delta_{\mathbb{Z}}(\frac{n-1}{2}) + \frac{1}{3}\delta_{\mathscr{A}}(\frac{n}{3})}$$

Podemos notar como esta ultima es, significativamente mas complicada que el caso de representaciones en tres partes. Evaluando para $n = 15$, obtenemos

$$\begin{aligned} p_{3,\mathscr{A}}(15) &= \frac{1}{6}T_7\delta_{\mathbb{Z}}(7) + \frac{1}{2}\left\lceil\frac{7}{2}\right\rceil\delta_{\mathbb{Z}}(7) + \frac{1}{3}\delta_{\mathscr{A}}(5) \\ &= \frac{1}{6}T_7 + \frac{1}{2}(4) + \frac{1}{3} = \frac{28}{6} + 2 + \frac{1}{3} = 7 \end{aligned}$$

que coincide con el conteo, pues

$$\begin{aligned} 15 &= 1+1+13 \\ &= 1+3+11 \\ &= 1+5+9 \\ &= 1+7+7 \\ &= 3+3+9 \\ &= 3+5+7 \\ &= 5+5+5 \end{aligned}$$

De forma general, podemos notar que se tienen las siguientes relaciones

Lema 1.3.1

Las particiones en dos y tres partes vienen dadas por

$$p_{2,A}(n) = \frac{1}{2}(r_{2,A}(n) + \delta_A(\frac{n}{2})) \tag{1.3.3}$$

$$p_{3,A}(n) = \frac{1}{6}\left(r_{3,A}(n) + 3\left(\sum_{0\leq m\leq\frac{n}{2}}\delta_A(n-2m)\delta_A(m)\right) + 2\delta_A(\frac{n}{3})\right) \tag{1.3.4}$$

¿Que sentido tienen estas formulas? Dar una interpretación combinatoria de estas relaciones es sumamente alentador en nuestro camino al estudiar las funciones de representación, pues muchas veces dar formulas complicadas puede llegar a ser confuso y llegar a parecer innecesario o carente de sentido combinatorio, pero en este caso veremos que no sera así. Para esto nos enfocaremos en el caso de particiones en tres partes. Primeramente ¿Como podemos contar las representaciones en tres partes?

Podemos clasificar cualquier partición en uno de los siguientes conjuntos (los cuales serán disjuntos) según la forma en que están creados

- A_1 : El conjunto de particiones donde los tres sumandos son distintos $[a, b, c]$
- A_2 : El conjunto de particiones donde exactamente solo dos sumandos son iguales $[a, a, b]$
- A_3: El conjunto de particiones donde los tres sumandos son iguales $[a, a, a]$

Con ello tendremos que el numero de particiones en tres partes es

$$p_{3,A}(n) = |A_1| + |A_2| + |A_3|$$

Por otro lado, el numero de representaciones $r_{3,A}(n)$ cuenta las permutaciones de estos elementos, cada partición de A_1 tiene la forma $[a,b,c]$ entonces la cantidad de permutaciones de tres elementos donde consideramos los tres distintos es el coeficiente multinomial siendo $\binom{3}{1,1,1} = \frac{3!}{1!\cdot 1!\cdot 1!} = 6$, cada partición de A_2 tiene la forma $[a,a,b]$ entonces la cantidad de permutaciones tres elementos donde consideramos dos iguales y otro distintos es $\binom{3}{1,2} = \frac{3!}{1!\cdot 2!} = 3$ y para A_3similarmente, serán $\binom{3}{3} = \frac{3!}{3!} = 1$.

Por lo tanto, tendremos que

$$r_{3,A}(n) = 6\,|A_1| + 3\,|A_2| + |A_3|$$

Ahora, consideraremos otra forma de contar particiones, para ello definiremos conjuntos B_i con condiciones menos restrictivas.

- B_1 : El conjunto de todas las representaciones de n como suma de tres elementos de A (es decir $|B_1| = r_{3,A}(n)$)
- B_2 : El conjunto de representaciones de n donde dos de los sumandos son iguales y el otro puede ser cualquier otro (incluso repetir a los primeros)
- B_3: El conjunto de representaciones donde los tres sumandos son iguales.

Con esto tendremos las siguientes relaciones: por su definición, $|B_1| = 6\,|A_1| + 3\,|A_2| + 2\,|A_3|$, cualquier representación en B_2 es del tipo A_2 o del tipo A_3, por lo que $|B_2| = |A_2| + |A_3|$ y directamente $|B_3| = |A_3|$ por lo que tendemos el sistema lineal:

$$\begin{aligned} |B_1| &= 6\,|A_1| + 3\,|A_2| + |A_3| \\ |B_2| &= |A_2| + |A_3| \\ |B_3| &= |A_3| \end{aligned}$$

Resolviendo para los $|A_i|$ obtenemos

$$\begin{aligned} & |A_3| = |B_3| \\ \Rightarrow\ & |A_2| = |B_2| - |B_3| \\ \Rightarrow\ & |A_1| = \frac{1}{6}(|B_1| - 3\,|B_2| + 2\,|B_3|) \end{aligned}$$

Sumando, obtenemos

$$p_{3,A}(n) = |A_1| + |A_2| + |A_3| = \frac{1}{6}(|B_1| + 3\,|B_2| + 2\,|B_3|)$$

Mas aun, por sus propias definiciones $|B_1| = r_{3,A}(n)$ y $|B_3| = \delta_A(\frac{n}{3})$ de tal forma que, no solo recuperamos la formula 1.3.4, sino que también demostramos que

$$|B_2| = \sum_{0\leq m\leq \frac{n}{2}} \delta_A(n-2m)\delta_A(m) = [z^n] f_A(z) f_A(z^2)$$

Es decir, el coeficiente de la serie $f_A(z)f_A(z^2)$ me cuenta el numero de representaciones de n como suma de tres elementos de A donde dos de ellos son iguales. Esto me da la idea intuitiva del siguiente resultado, el cual se prueba de forma rápida con el producto de Cauchy.

Proposición 1.3.2

El coeficiente $[z^n]$ de la función $f_A^k(z)f_A(z^m)$ es igual al numero de representaciones de n como suma de $k+m$ elementos del conjunto A, donde m de los sumandos son iguales entre sí.

Con el objetivo de generalizar, el método de despejar conjuntos A_i se vuelve tedioso para k grande. Sin embargo, la estructura que emerge para cada B_i es clara, pues estas están indexadas por particiones de enteros positivos de k pues en el caso de $k=3$ obtenemos los coeficientes multinomiales $\binom{3}{1,1,1}$, $\binom{3}{1,2}$ y $\binom{3}{3}$ donde los números de abajo me representan las particiones de $k=3$ como suma de enteros positivos. Esto nos da una idea de la importancia que tendrán las particiones de enteros pues dichas particiones me determinan la cantidad de repeticiones de cada conjunto A_i en el numero de particiones. Con ello en mente, lo hecho con anterioridad puede ser generalizado para poder describir a la función generadora de las particiones en k partes, sin embargo se necesita hacer uso de contar el numero de permutaciones en el grupo cíclico S_k que cumplen cierta restricción, para ello se usa la **formula del indice de ciclos del grupo**, es por ello que no profundizaremos en esta generalización, pues se sale de los parámetros de este documento.

También es preciso aclarar que el procedimiento hecho en la **Proposición 1.3.1** es claramente generalizable, pues todo se baso en obtener formulas de las derivadas de la función $P_A(t,z)=\exp\left(G(t,z)\right)$ respecto a t, por lo que bastaría con encontrar una formula para la derivada k-esima de dicha función en términos de G. Dicha formula es obtenible, pero hace uso de la formula de **Faà di Bruno** la cual generaliza la regla de la cadena para derivadas de orden superior y (como es de esperar) es complicada, agregado a ello su forma mas compacta esta escrita en términos de particiones de enteros como en el caso del método combinatorio[3] por todos estos motivos unicamente nos quedaremos con las formulas obtenidas (y su interpretación) de las particiones en dos y tres partes, y no entraremos en detalle en la formula general.

A pesar de esto y por gusto del buen lector, dejaremos aquí descrita la formula de la función generadora de particiones en cuatro partes, obtenida con el método general y el como me representan los posibles casos de representaciones que hay, por ejemplo, el termino $f_A(z^2)^2=f_A(z^2)f_A(z^2)$ me indica las representaciones en cuatro partes donde dos sumandos son iguales y los otros dos también son iguales pero distintos a los primeros.

$$P_{4,A}(z)=\frac{1}{24}\left(f_A^4(z)+6f_A^2(z)f_A(z^2)+3f_A(z^2)^2+8f_A(z)f_A(z^3)+6f(z^4)\right)$$

Al igual que en el caso de las representaciones, a partir de las funciones generadoras obtenidas en el **Teorema 1.3.1** podemos derivar relaciones de recurrencia para las particiones. Empezaremos con el caso de particiones en k partes.

[3]De hecho la formula de Faà di Bruno se puede probar usando la teoría de indices de ciclos, por lo que usarla directamente seria lo mismo que usar a los ciclos.

Teorema 1.3.2

El numero de particiones en k partes de A, cumple la siguiente relación de recurrencia

$$p_{k,A}(n) = \frac{1}{k}\sum_{m=0}^{k}\left(\sum_{a\in A,\, a\leq \frac{n}{m}} p_{k-m}(n-ma)\right) \tag{1.3.5}$$

Demostración. Retomando la doble función generadora

$$P_A(t,z) = \sum_{n=0}^{\infty}\sum_{k=0}^{\infty} p_{k,A}(n)t^k z^n = \sum_{k=0}^{\infty} P_{k,A}(z)t^k = \prod_{a\in A}\left(\frac{1}{1-tz^a}\right)$$

tomando logaritmo en ambos lados de la expresión y derivando respecto a t

$$\log P_A(t,z) = \sum_{a\in A} -\log(1-tz^a) \;\Rightarrow\; \partial_t P_A(t,z) = P_A(t,z)\cdot\left(\sum_{a\in A}\frac{z^a}{1-tz^a}\right)$$

pero podemos reescribir el sumando de la derecha como una serie geométrica de modo que

$$\begin{aligned}\partial_t P_A(t,z) &= P_A(t,z)\cdot\left(t^{-1}\sum_{a\in A}\sum_{m=1}^{\infty}(tz^a)^m\right) = t^{-1}P_A(t,z)\cdot\left(\sum_{a\in A}\sum_{m=1}^{\infty}t^m z^{ma}\right)\\ &= t^{-1}P_A(t,z)\cdot\left(\sum_{m=1}^{\infty}\left(\sum_{a\in A}z^{ma}\right)t^m\right) = t^{-1}P_A(t,z)\cdot\left(\sum_{m=1}^{\infty}f_A(z^m)t^m\right)\end{aligned}$$

de tal forma que obtenemos la ecuación

$$t\cdot\partial_t P_A(t,z) = P_A(t,z)\cdot\left(\sum_{m=1}^{\infty}f_A(z^m)t^m\right)$$

Con esto, sacamos el coeficiente de $[t^k]$ de ambos lados de la igualdad

$$[t^k]\left[t\cdot\partial_t P_A(t,z)\right] = [t^k]\left[P_A(t,z)\cdot\left(\sum_{m=1}^{\infty}f_A(z^m)t^m\right)\right]$$

$$\Rightarrow\; [t^{k-1}]\left[\sum_{j=1}^{\infty}jP_{j,A}(z)t^{j-1}\right] = [t^k]\left[\left(\sum_{j=0}^{\infty}P_{j,A}(z)t^j\right)\cdot\left(\sum_{m=1}^{\infty}f_A(z^m)t^m\right)\right]$$

$$\Rightarrow\; kP_{k,A}(z) = \sum_{m=1}^{k}f_A(z^m)P_{k-m,A}(z) \;\Rightarrow\; P_{k,A}(z) = \frac{1}{k}\sum_{m=1}^{k}f_A(z^m)P_{k-m,A}(z)$$

y para obtener $p_{k,A}(n)$ extraemos el coeficiente de $[z^n]$en cada lado, donde

$$p_{k,A}(n) = \frac{1}{k}\sum_{m=1}^{k}[z^n]\left[f_A(z^m)P_{k-m,A}(z)\right] = \frac{1}{k}\sum_{m=1}^{k}\left(\sum_{q=0}^{n}p_{k-m}(q)\delta_A(\frac{n-q}{m})\right)$$

finalmente sumando sobre los $a \in A$ tales que $a = \frac{n-q}{m}$

$$p_{k,A}(n) = \frac{1}{k} \sum_{m=1}^{k} \left(\sum_{a \in A,\, a \leq \frac{n}{m}} p_{k-m}(n - ma) \right)$$

□

Esta formula es una relación entre particiones en k partes y particiones en menos partes $(k-m)$. Como en el caso de representaciones poder obtener formulas de recurrencia mas sencillas dependerá del conjunto A como veremos en la próxima sección.

A partir de esta relación de recurrencia podemos dar la relación para el caso $k = 3$ (aunque no muy útil).

$$\begin{aligned} p_{3,A}(n) &= \frac{1}{3} \sum_{m=1}^{3} \left(\sum_{a \in A,\, a \leq \frac{n}{m}} p_{3-m}(n - ma) \right) \\ &= \frac{1}{3} \left(\sum_{a \in A,\, a \leq n} p_2(n-a) + \sum_{a \in A,\, a \leq \frac{n}{2}} p_1(n-2a) + \sum_{a \in A,\, a \leq \frac{n}{3}} p_0(n-3a) \right) \end{aligned}$$

$$p_{3,A}(n) = \frac{1}{3} \left(\sum_{a \in A,\, a \leq n} p_2(n-a) + \sum_{a \in A,\, a \leq \frac{n}{2}} (n-2a)\delta_A(n-2a) \right)$$

Obtener una relación de recurrencia para las particiones en k partes sera totalmente distinto a obtener una relación de recurrencia para las particiones totales, para llegar a este objetivo sera necesario definir una función auxiliar, la cual es una generalización a la **función divisor** $\sigma(n)$ en los enteros.

Definición 1.3.1

Sea $A \subseteq \mathbb{Z}^+$y $n \in \mathbb{Z}^+$. Definimos a la **función divisor de** A como la función

$$\sigma_A(n) := \sum_{d|n,\, d \in A} d$$

Observación. De la expresión

$$\sigma_A(n) = \sum_{d|n,} d\delta_A(d) = (\mathrm{id} * \delta_A)(n)$$

en la convolución de Dirichlet, por tanto σ_A sera multiplicativa si y solo si la función δ_A es multiplicativa. Recordemos que decir que δ_A es multiplicativa significa

$$\text{si } (n,m) = 1 \text{ entonces } \delta_A(n)\delta_A(m) = \delta_A(nm)$$

Pero para que esto siquiera tenga sentido necesitaríamos que dados $n, m \in A$ se cumpla que $nm \in A$, sin embargo, esto no bastara para encapsular los productos en A, pues ademas de ello necesitaremos que se cumpla el inverso

Definición 1.3.2

Llamamos por **conjunto multiplicativamente cerrado**, a un subconjunto $A \subseteq \mathbb{Z}^+$ el cual tiene la propiedad de que para cualesquiera $(n, m) = 1$

$$n \in A \, \text{y} \, m \in A \Leftrightarrow nm \in A$$

Con ello se tiene lo siguiente

Lema 1.3.2

Sea $A \subseteq \mathbb{Z}^+$. Si A es multiplicativamente cerrado entonces, $\sigma_A(n)$ es multiplicativa.

Demostración. En efecto, dados $(n, m) = 1$ tendremos que $\delta_A(nm) = 1$ si y solo si $nm \in A$ y esto es si y solo si $n, m \in A$, por lo que $\delta_A(nm) = \delta_A(n)\delta_A(m)$. De forma similar, $\delta_A(nm) = 0$ si y solo si $nm \notin A$ y esto es si y solo si $n \notin A$ o $m \notin A$ (por ser multiplicativamente cerrado), por lo que $\delta_A(nm) = 0 = \delta_A(n)\delta_A(m)$. De esta forma δ_A es multiplicativa y por tanto el producto de Dirichlet $(\text{id} * \delta_A)(n) = \sigma_A(n)$ lo es. □

Ejemplo. Algunos ejemplos de conjuntos multiplicativamente cerrados son los enteros positivos, el conjunto de potencias de un numero fijo, el conjunto de números libres de cuadrados. En particular nuestro ejemplo usual de los impares $\mathscr{A}$ es un conjunto multiplicativamente cerrado,[4] por lo cual $\sigma_{\mathscr{A}}(n)$ es multiplicativa, de hecho es fácil comprobar que si 2^r es la mayor potencia de 2 que divide a n, entonces $\sigma_{\mathscr{A}}(n) = \sigma(\frac{n}{2^r})$ donde es la función divisor usual en los enteros.

Con esta noción podemos dar la relación de recurrencia para las particiones totales.

Teorema 1.3.3

El numero de particiones totales en partes de A, cumple la siguiente relación de recurrencia

$$p_A(n) = \frac{1}{n} \sum_{k=1}^{n} \sigma_A(k) p_A(n-k)$$

Demostración. Por el Teorema 1.3.1 tenemos

$$P_A(z) = \prod_{a \in A} \left(\frac{1}{1 - z^a} \right)$$

aplicando logaritmo y derivando respecto a z

$$P'_A(z) = P_A(z) \left(\sum_{a \in A} \frac{a z^{a-1}}{1 - z^a} \right) \Rightarrow z P'_A(z) = P_A(z) \left(\sum_{a \in A} a \frac{z^a}{1 - z^a} \right)$$

escribiendo como serie geométrica el segundo sumando

$$z P'_A(z) = P_A(z) \left(\sum_{a \in A} a \sum_{k=1}^{\infty} z^{ak} \right) = P_A(z) \left(\sum_{k=1}^{\infty} \sum_{a \in A} a z^{ak} \right)$$

[4] De hecho los impares no necesitan la hipótesis de producto de elementos coprimos ya que un producto es impar si y solo si ambos son impares.

Notemos que en el segundo sumando tendremos un z^msiempre y cuando exista algún $k \in \mathbb{Z}^+$ y $a \in A$ tal que, $m = ak$. Ademas el termino z^mse repetirá tantas veces como $a \in A$ haya tales que existe algún $k \in \mathbb{Z}^+$ tal que $m = ak$, es decir, para a que divide a n y como cada termino esta multiplicado por el valor de a que divide a n tendremos que el coeficiente que acompaña a z^m sera la suma de cada a que divide a m con $a \in A$, es decir, $\sigma_A(m)$, teniendo

$$zP'_A(z) = P_A(z)\left(\sum_{m=1}^{\infty} \sigma_A(m)z^m\right)$$

extrayendo los coeficientes

$$[z^n]zP'_A(z) = [z^n]P_A(z)\left(\sum_{m=1}^{\infty} \sigma_A(m)z^m\right)$$

$$\Rightarrow\ np_A(n) = \sum_{k=1}^{n} \sigma_A(k)p_A(n-k)$$

□

Nuevamente esta formula de recurrencia es sobre las particiones en menos partes, multiplicadas por una función que captura la estructura de los divisores de n en A. Una cosa a notar de la formula obtenida, es que, el numero de particiones de n se puede pensar como el promedio simple de las particiones en menos partes ponderadas con un peso $\sigma_A(k)$.

Ejemplo. Para nuestro conjunto de impares $\mathscr{A}$ tendremos$p_{\mathscr{A}}(n) = \frac{1}{n}\sum_{k=1}^{n} \sigma_{\mathscr{A}}(k)p_{\mathscr{A}}(n-k)$

$$p_{\mathscr{A}}(1) = 1,\ p_{\mathscr{A}}(2) = 1,\ p_{\mathscr{A}}(3) = 2$$

$$\begin{aligned} p_{\mathscr{A}}(4) &= \frac{1}{4}\left(\sigma_{\mathscr{A}}(1)p_{\mathscr{A}}(3) + \sigma_{\mathscr{A}}(2)p_{\mathscr{A}}(2) + \sigma_{\mathscr{A}}(3)p_{\mathscr{A}}(1) + \sigma_{\mathscr{A}}(4)p_{\mathscr{A}}(0)\right) \\ &= \frac{1}{4}\left(1\cdot 2 + 1\cdot 1 + 4\cdot 1 + 1\cdot 1\right) = 2 \end{aligned}$$

y efectivamente $4 = 1+1+1+1 = 1+3$.

Veamos como las propiedades aritméticas del conjunto A nuevamente nos facilitan las relaciones de recurrencia en el caso de particiones. Consideremos en conjunto $\mathscr{A}$ de impares, primeramente veamos como la función generadora $P_{k,\mathscr{A}}(z)$ es, de hecho, un producto finito. Consideremos

$$P_{\mathscr{A}}(t,z) = \sum_{k=0}^{\infty} P_{k,\mathscr{A}}(z)t^k = \prod_{a\in\mathscr{A}}\left(\frac{1}{1-tz^a}\right) = \prod_{n=0}^{\infty}\left(\frac{1}{1-tz^{2n+1}}\right)$$

quitando el primer producto y re indexando

$$P_{\mathscr{A}}(t,z) = \frac{1}{1-tz}\prod_{n=0}^{\infty}\left(\frac{1}{1-tz^{2n+3}}\right) = \frac{1}{1-tz}\prod_{n=0}^{\infty}\left(\frac{1}{1-(tz^2)z^{2n+1}}\right) = \frac{1}{1-tz}P_{\mathscr{A}}(tz^2,z)$$

de modo que

$$P_{\mathscr{A}}(t,z)(1-tz) = P_{\mathscr{A}}(tz^2,z)$$

$$\Rightarrow \left(\sum_{k=0}^{\infty} P_{k,\mathscr{A}}(z)t^k\right)(1-tz) = \sum_{k=0}^{\infty} P_{k,\mathscr{A}}(z)(tz^2)^k$$

$$\Rightarrow \left(\sum_{k=0}^{\infty} P_{k,\mathscr{A}}(z)t^k\right) - \left(\sum_{k=0}^{\infty} zP_{k,\mathscr{A}}(z)t^{k+1}\right) = \sum_{k=0}^{\infty} z^{2k}P_{k,\mathscr{A}}(z)t^k$$

Por lo que, sacando el coeficiente $[t^k]$ en ambos lados obtenemos una relación de recurrencia para la función generadora de particiones de impares en k partes

$$P_{k,\mathscr{A}}(z) - zP_{k-1,\mathscr{A}}(z) = z^{2k}P_{k,\mathscr{A}}(z) \Rightarrow P_{k,\mathscr{A}}(z) = \frac{z}{1-z^{2k}}P_{k-1,\mathscr{A}}(z)$$

$$\Rightarrow P_{k,\mathscr{A}}(z) = \frac{z}{1-z^{2k}}\frac{z}{1-z^{2k-2}}P_{k-2,\mathscr{A}}(z)$$

$$\Rightarrow P_{k,\mathscr{A}}(z) = \frac{z}{1-z^{2k}}\frac{z}{1-z^{2k-2}}\frac{z}{1-z^{2k-4}}P_{k-3,\mathscr{A}}(z)$$

siguiendo los despejes, obtenemos $(P_{0,\mathscr{A}}(z) = 1)$

$$\boxed{P_{k,\mathscr{A}}(z) = \frac{z^k}{(1-z^2)(1-z^4)\cdots(1-z^{2k})}}$$

Ademas de esto, de la recurrencia en la función generadora $P_{k,\mathscr{A}}(z) = \frac{z}{1-z^{2k}}P_{k-1,\mathscr{A}}(z)$, reordenando, $P_{k,\mathscr{A}}(z)(1-z^{2k}) = zP_{k-1,\mathscr{A}}(z)$ obteniendo el coeficiente $[z^n]$ recuperamos una recurrencia para el numero de particiones en k partes

$$\boxed{p_{k,\mathscr{A}}(n) = p_{k,\mathscr{A}}(n-2k) + p_{k-1,\mathscr{A}}(n-1)}$$

Ademas de la formula de recurrencia obtenida en el **Teorema 1.3.3**, podemos hacer algo más. Pensemos en nuestra función generadora de las particiones de A

$$P_A(z) = \sum_{n=0}^{\infty} p_A(n)z^n = \prod_{a\in A}\left(\frac{1}{1-z^a}\right)$$

y consideremos su reciproco

$$\frac{1}{P_A(z)} = \prod_{a\in A}(1-z^a)$$

el producto de la derecha no es mas que un producto de polinomios cuya expansión sera una serie de potencias en z, llamemosle

$$\prod_{a\in A}(1-z^a) = \sum_{n=0}^{\infty} c_{A,n}z^n$$

donde $c_0 = 1$ siempre. Entonces, dada su propia definición tendremos que

$$P_A(z)\frac{1}{P_A(z)} = 1 \Leftrightarrow \left(\sum_{n=0}^{\infty} p_A(n)z^n\right)\left(\sum_{n=0}^{\infty} c_{A,n}z^n\right) = 1$$

de donde obtendremos una recurrencia en términos de la sucesión c_n:

$$\left(\sum_{n=0}^{\infty} p_A(n)z^n\right)\left(\sum_{n=0}^{\infty} c_{A,n}z^n\right) = 1 \Leftrightarrow p_A(0)c_{A,0} = 1 \text{ y } \sum_{k=0}^{n} c_{A,k}p_A(n-k) = 0, n \geq 1$$

$$\text{Para } n \geq 1,\ p_A(n) = -\sum_{k=1}^{n} c_{A,k} p_A(n-k)$$

Esto me da otra formula de recurrencia del numero de particiones pero en términos de esta sucesión c_n del reciproco de la generadora. Dado un conjunto A en general no es posible determinar el valor exacto de dicha sucesión, pero si seremos capaces de dar una formula de recurrencia que cumple.

Proposición 1.3.3

Sea

$$\prod_{a\in A}(1-z^a) = \sum_{n=0}^{\infty} c_{A,n} z^n$$

entonces la sucesión $c_{A,n}$ cumple que $c_{A,0} = 1$ y, para $n \geq 1$

$$c_{A,n} = -\frac{1}{n}\sum_{k=1}^{n} \sigma_A(k) c_{A,n-k}$$

Demostración. Prosiguiendo como en el **Teorema 1.3.3**, dada

$$Q_A(z) = \prod_{a\in A}(1-z^a) = \sum_{n=0}^{\infty} c_{A,n} z^n$$

aplicando logaritmo y derivando respecto a z

$$Q'_A(z) = Q_A(z)\left(-\sum_{a\in A}\frac{a z^{a-1}}{1-z^a}\right) \Rightarrow zQ'_A(z) = Q_A(z)\left(-\sum_{a\in A} a\frac{z^a}{1-z^a}\right)$$

escribiendo como serie geométrica el segundo sumando

$$\begin{aligned} zQ'_A(z) &= Q_A(z)\left(-\sum_{a\in A} a\sum_{k=1}^{\infty} z^{ak}\right) = Q_A(z)\left(-\sum_{k=1}^{\infty}\sum_{a\in A} a z^{ak}\right) \\ &= Q_A(z)\left(-\sum_{m=1}^{\infty}\sigma_A(m) z^m\right) \end{aligned}$$

de donde el coeficiente $[z^n]$ nos da que

$$n c_{A,n} = -\sum_{k=1}^{n}\sigma_A(k) c_{A,n-k}$$

□

Como podemos notar, esta es exactamente la misma relación de recurrencia del numero de particiones, pero en dicha formula de recurrencia tenemos un signo menos. En resumen,

estos dos últimos resultados me dicen que: Dada la sucesión definida como $c_0 = 1$ y $c_{A,n} = -\frac{1}{n}\sum_{k=1}^{n} \sigma_A(k)c_{A,n-k}$, el numero de particiones de n cumplirá la relación

$$p_A(n) = -\sum_{k=1}^{n} c_{A,k}p_A(n-k) \tag{1.3.6}$$

la posible "ventaja" es que es una suma lineal, sin necesidad de promediar por la cantidad de sumando, siempre y cuando la sucesión $c_{A,n}$se comporte "bien". Pero veremos que este no sera el caso, pues una expresión para $c_{A,n}$ es casi imposible de obtener. En la siguiente sección daremos una formula exacta para $c_{A,n}$ en el caso particular $A = \mathbb{Z}^+$ y mencionaremos la dificultad de su prueba.

Cabe aclarar que es posible hacer análisis mas exhaustivos sobre la sucesión $c_{A,n}$ e incluso darle una interpretación combinatoria con el numero de particiones con cantidad par e impar de sumandos distintos, pero se sale del objetivo de este trabajo.

El análisis desarrollado en esta sección evidencia que, si bien es posible obtener relaciones de recurrencia generales mediante la derivada logarítmica y funciones auxiliares como $\sigma_A(n)$, la naturaleza del problema de las particiones tiene una complejidad mas profunda que el de las representaciones debido a los productos infinitos involucrados. Hemos logrado describir $p_{k,A}(n)$ y $p_A(n)$ en términos de la aritmética del conjunto A, pero estas formulas generales que obtuvimos son tan complejas que el uso puede llegar a no ser practico. Para poder comprender realmente el alcance y las limitaciones de estas funciones generadoras resultara de importancia considerar el caso donde la estructura aritmética es la mas fundamental posible. Es por esta razón que en la siguiente sección nos centraremos en el caso $A = \mathbb{Z}^+$, lo que nos permitirá comparar la teoría general con las identidades clásicas.

1.4. Los enteros

Como bien explicamos, estudiar el caso general de encontrar estimaciones (o formulas) para $r_{k,A}(n)$ y $p_{k,A}(n)$, es en extremo complicado, pues el hecho de haber o no soluciones a las ecuaciones aditivas dependerá de las propiedades aritméticas del conjunto A que tomemos. Es por ello que daremos un repaso en el caso mas conocido y simple, que es cuando consideramos $A = \mathbb{Z}^+$.

Para simplificar denotaremos $\delta_{\mathbb{Z}^+}(n) = \delta(n)$, $r_{k,\mathbb{Z}^+}(n) := r_k(n)$ y $p_{k,\mathbb{Z}^+}(n) := p_k(n)$ así como $r_{\mathbb{Z}^+}(n) := r(n)$ y $p_{\mathbb{Z}^+}(n) := p(n)$ y en el caso de las funciones generadoras $R_{k,\mathbb{Z}^+}(z) := R_k(z)$, $R_{\mathbb{Z}^+}(z) := R(z)$, $P_{k,\mathbb{Z}^+}(z) := P_k(z)$ y $P_{\mathbb{Z}^+}(z) := P(z)$. En este caso lo que estudiaremos es el numero de representaciones y particiones de enteros positivos.

Ejemplo. Tenemos que $r(4) = 8$ pues:

$$4 = \begin{cases} 4 \\ 1+3 \\ 3+1 \\ 2+2 \\ 1+1+2 \\ 1+2+1 \\ 2+1+1 \\ 1+1+1+1 \end{cases}$$

de donde también podemos obtener que $r_1(4) = 1$, $r_2(4) = 3$, $r_3(4) = 3$, $r_4(4) = 1$. Y de forma similar podemos notar que $p(4) = 5$, pues $p_1(4) = 1$, $p_2(4) = 2$, $p_3(4) = 1$, $p_4(4) = 1$.

Quisiéramos atacar el problema de saber si es posible dar una buena expresión para $r_k(n)$ y $p_k(n)$ y por ende para $r(n)$ y $p(n)$, veamos que para el caso del numero de representaciones de un entero positivo si podemos obtenerlo de una manera sencilla usando las herramientas estudiadas en la sección anterior.

Proposición 1.4.1

Sean $n, k \in \mathbb{Z}^+$. Entonces

$$r_k(n) = \binom{n-1}{k-1}$$

y por ende

$$r(n) = 2^{n-1}$$

Demostración. La función de representación de enteros positivos es

$$f_{\mathbb{Z}^+}(z) = \sum_{n=1}^{\infty} z^n = \frac{z}{1-z}$$

así, por el **Teorema 1.2.1**

$$R_k(z) = f^k_{\mathbb{Z}^+}(z) = \left(\frac{z}{1-z}\right)^k = \frac{z^k}{(1-z)^k}$$

$$R(z) = \frac{\frac{z}{1-z}}{1-\frac{z}{1-z}} = \frac{z}{1-2z}$$

de donde, para el numero de representaciones obtenemos

$$R(z) = \frac{z}{1-2z} = z\frac{1}{1-2z} = z\sum_{m=0}^{\infty}(2z)^m = \sum_{m=0}^{\infty} 2^m z^{m+1} = \sum_{m=1}^{\infty} 2^{m-1} z^m$$

entonces $r(n) = [z^n]R(z) = 2^{n-1}$, similarmente usando el teorema del binomio generalizado

$$\begin{aligned} R_k(z) = \frac{z^k}{(1-z)^k} &= z^k \sum_{m=0}^{\infty} \binom{-k}{m} (-1)^m z^m \\ &= \sum_{m=0}^{\infty} \binom{m+k-1}{m} z^{m+k} = \sum_{j=k}^{\infty} \binom{j-1}{j-k} z^j \end{aligned}$$

obteniendo

$$r_k(n) = [z^n]R_k(z) = \binom{n-1}{n-k} = \binom{n-1}{k-1}$$

□

De esta manera identificamos exactamente el numero de representaciones en k partes y el numero de representaciones totales, que, comprobando con nuestro ejemplo, $r_2(4) =$

$\binom{4-1}{2-1} = \binom{3}{1} = 3$ y $r(4) = 2^{4-1} = 8$ efectivamente. Podemos recuperar algunas relaciones de recurrencia con lo obtenido en la **Proposición 1.2.1**

$$\binom{n-1}{k} = r_{k+1}(n) = \sum_{1\leq a\leq n} r_k(n-a) = \sum_{m=1}^{n} \binom{n-m-1}{k-1}$$

$$2^{n-1} = r(n) = 1 + \sum_{1\leq a<n} r(n-a) = 1 + \sum_{m=1}^{n-1} 2^{n-m-1}$$

dichas relaciones ya son bien conocidas e, incluso, claras de ver. Por tanto para el caso de enteros positivos el tema del numero de representaciones queda totalmente determinado.

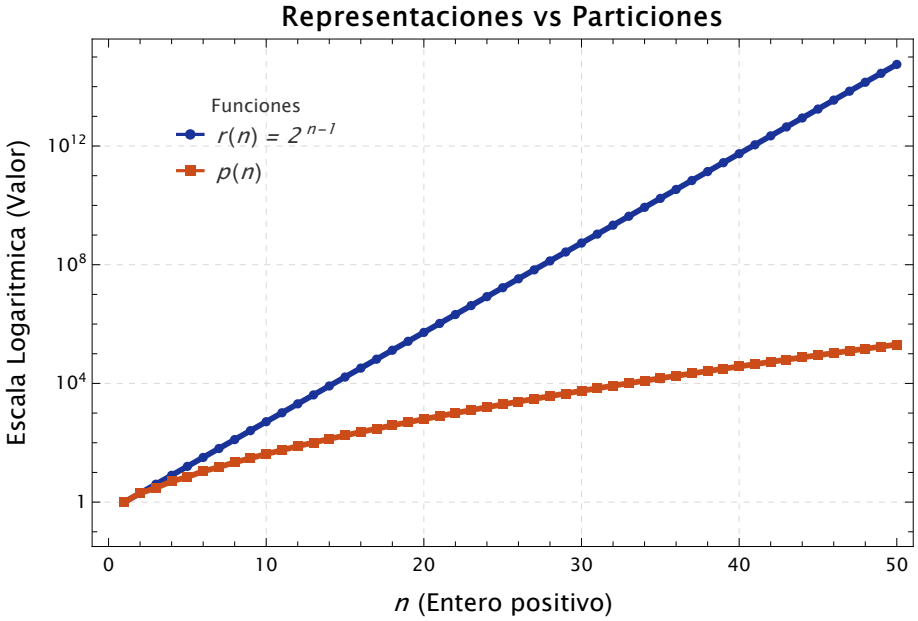

Figura 1.4.1: *Comparación en escala logarítmica del crecimiento del número de representaciones $r(n)$ frente al número de particiones $p(n)$. Nótese el crecimiento exponencial de $r(n)$.*

El estudio formal de las particiones de enteros positivos comenzó a mediados del siglo XVIII por Leonhard Euler. Antes de él, el problema era mas una curiosidad recreativa que un campo de estudio. Euler trabajo con las particiones mediante el uso de su función generadora, de hecho, fue el primero en dar su descripción algebraica, obteniendo que

$$P(z) = \sum_{n=0}^{\infty} p(n)z^n = \prod_{n=1}^{\infty} \left(\frac{1}{1-z^n}\right)$$

cosa que coincide con lo que obtenemos al aplicar el **Teorema 1.3.1** a $\mathbb{Z}^+$. Es importante notar que Euler trataba a estas funciones como series formales de potencias, con lo cual no se preocupaba por la convergencia de dichas series u productos. Euler noto que este producto infinito no se podía simplificar a una fracción simple, lo que hace imposible extraer el coeficiente $p(n)$ algebraicamente.

Formulas para las particiones en k partes de un entero n no son sencillas, del **Lema 1.3.1** podemos obtener las formulas para particiones en dos y tres partes

$$p_2(n) = \frac{1}{2}(r_2(n) + \delta(\frac{n}{2})) = \frac{1}{2}\left(\binom{n-1}{1} + \delta(\frac{n}{2})\right) = \frac{1}{2}\left(n - 1 + \delta(\frac{n}{2})\right)$$

donde para n par $p_2(n) = \frac{n}{2}$ y para n impar $p_2(n) = \frac{n-1}{2}$, por lo que

$$\boxed{p_2(n) = \left\lfloor \frac{n}{2} \right\rfloor}$$

En el caso de particiones en tres partes,

$$\begin{aligned} p_3(n) &= \frac{1}{6}\left(r_3(n) + 3\left(\sum_{0\leq m\leq \frac{n}{2}} \delta(n-2m)\delta(m) \right) + 2\delta(\frac{n}{3}) \right) \\ &= \frac{1}{6}\left(\binom{n-1}{3-1} + 3\left(\sum_{0<m\leq \lfloor \frac{n}{2} \rfloor} \delta(n-2m) \right) + 2\delta(\frac{n}{3}) \right) \end{aligned}$$

para el sumando central, notemos que $\delta(n-2m) = 0$ si y solo si $n - 2m = 0$ si y solo si $m = \frac{n}{2}$ y eso solo pasara en el caso en que $\lfloor \frac{n}{2} \rfloor = \frac{n}{2}$, es decir, en caso de que n sea par. Con ello

$$\begin{aligned} p_3(n) &= \frac{1}{6}\left(\binom{n-1}{2} + 3\left(\delta(n-2\left\lfloor \frac{n}{2} \right\rfloor) + \sum_{0<m<\lfloor \frac{n}{2} \rfloor} 1 \right) + 2\delta(\frac{n}{3}) \right) \\ &= \frac{1}{6}\left(\frac{(n-1)(n-2)}{2} + 3\left(1 - \delta(\frac{n}{2}) + \left\lfloor \frac{n}{2} \right\rfloor - 1 \right) + 2\delta(\frac{n}{3}) \right) \\ &= \frac{1}{6}\left(\frac{(n-1)(n-2)}{2} + 3\left(\left\lfloor \frac{n}{2} \right\rfloor - \delta(\frac{n}{2}) \right) + 2\delta(\frac{n}{3}) \right) \end{aligned}$$

Ahora, notemos que el termino $\lfloor \frac{n}{2} \rfloor - \delta(\frac{n}{2})$ comprobando casos pares e impares se simplifica a $\lfloor \frac{n-1}{2} \rfloor$, obteniendo

$$\boxed{p_3(n) = \frac{(n-1)(n-2)}{12} + \frac{1}{2}\left\lfloor \frac{n-1}{2} \right\rfloor + \frac{1}{3}\delta(\frac{n}{3})}$$

Aplicar directamente la formula de recurrencia presentada en 1.3.5 sera en sumo ineficiente. Veamos como, como en el caso de impares, podemos obtener una formula de recurrencia para el numero de particiones en k partes. Mas aun, veamos que el producto infinito de la función generadora de particiones en k partes es finita. Procediendo de forma similar dada

$$P(t,z) = \sum_{k=0}^{\infty} P_k(z)t^k = \prod_{n=0}^{\infty}\left(\frac{1}{1-tz^n} \right)$$

podemos separar el primer producto y llegar a la ecuación

$$P(t,z)(1-tz) = P(tz,z)$$

de donde obtendremos que

$$P_k(z) = \frac{z}{1-z^k}P_{k-1}(z) \tag{1.4.1}$$

y aplicando la formula recursiva

$$P_k(z) = \sum_{n=0}^{\infty} p_k(n) z^n = \frac{z^k}{(1-z)(1-z^2)\cdots(1-z^k)}$$

Extrayendo el coeficiente $[z^n]$ de la ecuación 1.4.1, obtenemos la formula de recurrencia para el numero de particiones en k partes

$$p_k(n) = p_k(n-k) + p_{k-1}(n-1)$$

Ejemplo. Con lo anterior veamos cuales son las particiones en tres partes del 6. Primero usando la formula directa

$$\begin{aligned} p_3(6) &= \frac{(6-1)(6-2)}{12} + \frac{1}{2}\left\lfloor \frac{6-1}{2} \right\rfloor + \frac{1}{3}\delta(\frac{6}{3}) \\ &= \frac{20}{12} + \frac{1}{2}(2) + \frac{1}{3}\cdot 1 = 3 \end{aligned}$$

y con la formula de recurrencia:

$$\begin{aligned} p_3(6) &= p_3(6-3) + p_{3-1}(6-1) = p_3(3) + p_2(5) \\ &= \frac{(3-1)(3-2)}{12} + \frac{1}{2}\left\lfloor \frac{3-1}{2} \right\rfloor + \frac{1}{3}\delta(\frac{3}{3}) + \left\lfloor \frac{5}{2} \right\rfloor \\ &= \frac{2}{12} + \frac{1}{2} + \frac{1}{3} + 2 = 3 \end{aligned}$$

Para las particiones totales, el **Teorema 1.3.3** nos da una relación de recurrencia con la función divisor usual

$$p(n) = \frac{1}{n}\sum_{k=1}^{n} \sigma(k) p(n-k)$$

pero al depender de saber los divisores para cada sumando se vuelve muy ineficiente. Sin embargo usando la segunda relación de recurrencia dada por la ecuación 1.3.6

$$p(n) = -\sum_{k=1}^{n} c_k p(n-k)$$

pero en el caso de enteros positivos, podemos notar algo curioso al calcular los términos de la sucesión c_n. En este sentido la sucesión tiene la relación de recurrencia, con $c_0 = 1$;

$$c_n = -\frac{1}{n}\sum_{k=1}^{n} \sigma(k) c_{n-k}$$

Calculando los primeros valores obtenemos

$$(c_0, c_1, c_2, ..., c_{15}, ...) = (1, -1, -1, 0, 0, 1, 0, 1, 0, 0, 0, 0, -1, 0, 0, -1, ...)$$

Notando que los términos unicamente son 0, 1 o -1. Esto fue algo que Leonhard Euler noto en su momento. Mas específicamente, Euler observo las potencias de z^n que sobrevivían en la expansión en series del reciproco de la función generadora de el numero de particiones

$$\prod_{n=1}^{\infty}(1-z^n) = \sum_{n=0}^{\infty} c_n z^n = 1 - z - z^2 + z^5 + z^7 - z^{12} - z^{15} + z^{22} + \cdots$$

Observando las potencias que sobrevivían dio el llamado Teorema del Numero Pentagonal[5] , el cual usando la notacion de este trabajo nos dice lo siguiente.

Teorema 1.4.1 (Teorema del Numero Pentagonal)

Si

$$\prod_{n=1}^{\infty}(1-z^n) = \sum_{n=0}^{\infty} c_n z^n$$

entonces

$$c_n = \begin{cases} (-1)^k & \text{si } n = \frac{k(3k-1)}{2} \text{ con } k \in \mathbb{Z} \\ 0 & \text{en otro caso} \end{cases}$$

Es posible reescribir la identidad anterior de una forma mas compacta, dado que los términos en los que n no son de la forma dada son cero, podemos re indexar la suma sobre los $n = \frac{k(3k-1)}{2}$ para cada k, obteniendo la celebre identidad de Euler en su forma usual

$$\prod_{n=1}^{\infty}(1-z^n) = \sum_{k=-\infty}^{\infty}(-1)^k z^{\frac{k(3k-1)}{2}}$$

Esta expresión genera explícitamente los términos no nulos de la expansión. El nombre de este teorema hace referencia a los exponentes $n = \frac{k(3k-1)}{2}$, pues, para $k \in \mathbb{Z}^+$, estos valores coinciden con los **números pentagonales** (1, 5, 12, 22,...), los cuales representan la cantidad de puntos necesarios para construir pentágonos anidados con un vértice en común. Para los indices negativos $k \in \mathbb{Z}^{-1}$ obtenemos valores positivos igualmente (2, 7, 15,...), en conjunto (términos con k positivos y negativos) son conocidos como **números pentagonales generalizados** que denotaremos g_k (1, 2, 5, 7, 12, 15, 22, 26, 35,...). Con ello Euler dedujo la formula de recurrencia para el numero de particiones mas conocida, la cual es nuestra ecuación 1.3.6

$$p(n) = -\sum_{k=1}^{n} c_k p(n-k)$$

sumando unicamente sobre los c_k no nulos obtenemos

$$p(n) = \sum_{k=1}^{n}(-1)^{k-1}p(n-g_k) = p(n-1)+p(n-2)-p(n-5)-p(n-7)+\cdots$$

Ademas del Teorema del Numero Pentagonal, Euler encontró diversas propiedades de particiones de enteros que cumplían ciertas condiciones, la mas conocida es la identidad que establece que el número de particiones de un entero n en partes impares es igual al numero de particiones de n en partes distintas. Con estas ideas, Euler sentó las bases de la teoría analítica de las particiones, que más tarde inspiraría a toda una línea de investigación combinatoria y analítica en los siglos XIX y XX.

[5]Euler se baso en evidencia heuristica, lo conjeturo en 1741 pero no pudo probarlo sino hasta 1750. Su articulo fue publicado finalmente en 1760.

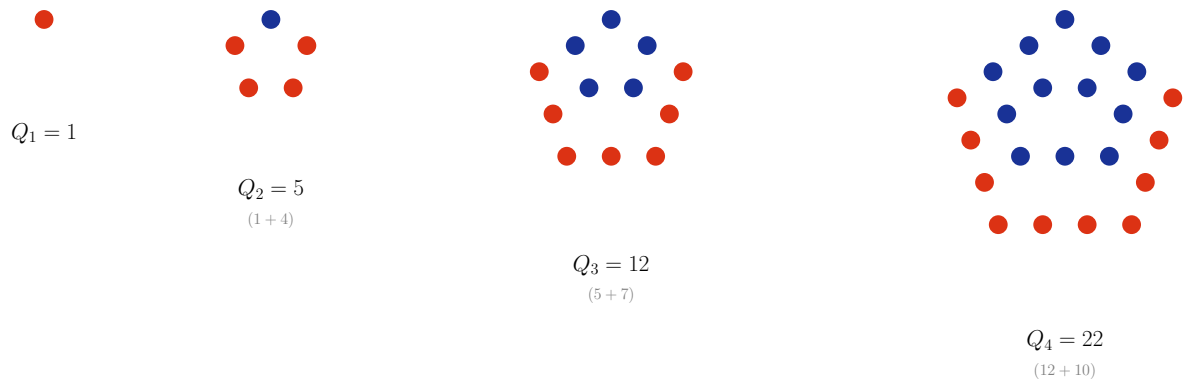

Figura 1.4.2: *Números pentagonales compartiendo un vértice común. En rojo esta el nuevo pentágono agregado en cada iteración. Se puede notar la recurrencia* $Q_n = Q_{n-1} + 3n - 2$.

Sin embargo, tras los trabajos de Euler, el progreso en la búsqueda de una formula explicita para el numero de particiones $p(n)$ fue lento. Durante el siglo XIX, el avance mas significativo vino de la mano de James Joseph Sylvester, quien aplico la teoria de invariantes algebraicos a las particiones restringidas, demostrando que estas se comportan como cuasipolinomios ([10]). Posteriormente , a principios del siglo XX, Percy Alexander MacMahon fue quien dio a la teoría de particiones una estructura combinatoria sistemática en su obra *Combinatory Analysis* [11]. MacMahon no solo estudio las particiones planas y vectoriales (una generalización de particiones con mas coeficientes), sino que utilizo la recurrencia del numero de particiones para calcular el valor de las particiones hasta $n = 200$, obteniendo la monstruosa[6] cantidad:

$$p(200) = 3,972,999,029,388$$

A pesar de estos trabajos, persistía una limitación fundamental: la incapacidad de manejar el verdadero comportamiento asintótico del problema general. Las funciones generadoras se utilizaban unicamente como series formales de potencias, encapsulando la información aritmética del conjunto A de manera algebraica, pero sin herramientas para "desencapsular" dicha información de manera eficiente.

Esta dificultad de manejar los casos generales y los pocos resultados que se obtenían con funciones generadoras llevo a que gran parte de la teoría aditiva clásica se separara en el estudio de casos particulares, aplicando resultados de álgebra y de formas cuadráticas. Dos ejemplos bien conocidos son el teorema de los cuatro cuadrados de Lagrange (1770) y el teorema de los números triangulares de Gauss (1796), los cuales probaban que todo numero es suma de cuatro cuadrados y de tres números triangulares respectivamente. De forma mas especifica, si $B = \{k^2 : k \geq 1\}$ y $C = \left\{\frac{k(k+1)}{2} : k \geq 1\right\}$ entonces $r_{4,B}(n) > 0$ y $r_{3,C}(n) > 0$. Es aquí donde podemos notar una limitación intrínseca desde el punto de vista analítico; pruebas que el numero de representaciones siempre es positivo (es decir siempre hay una representación), pero no dan una respuesta a la pregunta inicial ¿De cuantas formas? o siquiera dar una estimación buena.

Este fue el "muro" que mantuvo estancada a la teoría aditiva general: la falta de un método para estimar el crecimiento del numero de representaciones o particiones. Fue

[6] A pesar de esta afirmación, el valor de $r(200)$ es en escala mucho mayor, al rededor de 2^{199}.

necesario esperar hasta 1918, cuando H. Hardy y S. Ramanujan rompieron este estancamiento mediante una nueva visión. Su idea consistió en dejar de ver a las funciones generadoras como meras series formales y tratarlas como funciones de variable compleja, analizando sus singularidades en el circulo unitario. Las tablas numéricas de MacMahon sirvieron entonces como la evidencia empírica necesaria para validar los resultados asintóticos que obtuvieron. Este nuevo enfoque el cual combina la aritmética con el análisis complejo, es lo que hoy conocemos como el Método del Circulo.

Capítulo 2

El Método del Circulo

2.1. Hardy y Ramanujan

Todo lo detallado en esta sección como los hechos históricos se pueden encontrar en [12, 13, 14, 15], y los análisis modernos así como aclaraciones de lo hecho por Hardy y Ramanujan se pueden encontrar en [18, 19, 21]

La historia moderna de la función de partición, $p(n)$, y el nacimiento del **Método del Círculo**, son dos hechos íntimamente ligados a la colaboración entre G. H. Hardy y Srinivasa Ramanujan. Su encuentro no solo marcó un hito en la teoría analítica de números, sino que representó la convergencia de dos pensamientos opuestos: el rigor analítico de Hardy y la intuición profunda y casi mística de Ramanujan.

G. H. Hardy era ya una figura central de la teoría analítica de números en el Trinity College de Cambridge cuando, el 16 de enero de 1913, recibió una carta proveniente de un joven y prácticamente desconocido contable brahmán de Madrás: Srinivasa Ramanujan. El documento contenía una centena de teoremas y formulas sin demostración, algunos conocidos, otros erróneos, y otros tan extraordinarios que, en palabras de Hardy, **«tenían que ser verdaderos, porque si no lo fueran, nadie tendría la imaginación para inventarlos»**. Junto a su colaborador J. E. Littlewood, Hardy reconoció esa noche que no estaba ante un charlatán, sino ante un genio natural.

Tras superar barreras culturales y religiosas que le impedían dejar su hogar y cruzar el mar, Ramanujan arribó a Inglaterra en abril de 1914, luego de que su madre soñara con su diosa pidiéndole dejar ir a Ramanujan. La colaboración comenzó con un choque de estilos. Hardy se enfrentó a un dilema de enseñanza inesperado: debía guiar a Ramanujan en el rigor del análisis moderno y la teoría de funciones de Cauchy sin fracturar la intuición que le permitía "ver" los resultados. Durante los primeros dos años, mientras la Primera Guerra Mundial vaciaba Cambridge y enviaba a Littlewood al frente, Hardy y Ramanujan se dedicaron a sistematizar los cuadernos de este último, abordando problemas de series hipergeométricas y teoría de números primos. Sin embargo, esto ultimo dificultó enormemente su adaptación. Las fuentes remarcan que pasaba largas horas trabajando en su cuarto, muchas veces aislado por clima, salud o comida sufriendo incluso de racismo en una época de guerra y desprecio hacia los extranjeros.

Pese a esto Ramanujan adoptaba nuevas herramientas analíticas sin perder su creatividad; describía con entusiasmo funciones extrañas que él mismo creaba e inventaba y que no parecían encajar en ninguna teoría existente. En esos primeros años trabajaron

principalmente en series theta, productos infinitos, aproximaciones analíticas y cuestiones generales de teoría de números, no directamente en particiones.

Hacia 1916, el interés de Ramanujan se volcó hacia $p(n)$. Hasta entonces, el estudio de las particiones había sido mayormente algebraico y combinatorio. Ramanujan, sin embargo, estaba convencido de que debía existir una fórmula exacta, o al menos una aproximación asintótica con un error despreciable, para calcular $p(n)$. Ramanujan no parece haber estudiado sistemáticamente la función partición antes de conocer a Hardy, aunque sí había trabajado con productos infinitos y q-series que, de forma implícita, tenían relación profunda con las particiones. Esto se confirma varios años más tarde, cuando él mismo descubre que algunas de sus "identidades nuevas" ya habían sido publicadas en 1894 sin que él lo supiera: había reinventado hechos clásicos desde un angulo diferente. Un hecho importante es que en su primera carta, Ramanujan incluía una fórmula aproximada derivada de una serie theta para obtener ciertos coeficientes. Aunque la fórmula era incorrecta en forma, Hardy diría más tarde que esta "afirmación falsa" de Ramanujan fue lo que los condujo a toda su teoría de particiones.

Ramanujan -como ya mencionamos- sugería que las propiedades de $p(n)$ debían de estar codificadas en su función generatriz, mas específicamente en las singularidades de su función generatriz, una idea que resonaba con su conocimiento de las funciones modulares y elípticas. Ambos elementos llevaron a Hardy a ver que el problema de contar particiones $p(n)$ era ideal para aplicar la teoría analítica que él dominaba, mientras que las ideas previas de Ramanujan ofrecían un camino inesperado hacia una fórmula asintótica.

Un actor crucial en esta etapa fue el Mayor Percy MacMahon, un experto en combinatoria y prodigioso calculista. A petición de Hardy y Ramanujan, MacMahon asumió mostruosa tarea de calcular a mano los valores de $p(n)$ hasta $n = 200$. El resultado, $p(200) = 3,972,999,029,388$, se convirtió en el objetivo a lograr: cualquier fórmula teórica que desarrollaran debía coincidir con este dato empírico con una precisión absoluta. MacMahon entonces se convirtió, en esencia, en la herramienta de validación computacional de su época.

El desarrollo de la prueba coincidió con el periodo más oscuro en la vida de Ramanujan. En la primavera de 1917, contrajo una enfermedad grave (diagnosticada entonces como tuberculosis, aunque análisis modernos sugieren amebiasis hepática) que lo confinó a estar hospitalizado durante largos periodos. La colaboración continuó a menudo al pie de la cama del enfermo con visitas regulares de Hardy para discutir detalles.

El desafío matemático era en sumo difícil. Ramanujan creyó inicialmente haber encontrado una **fórmula exacta** utilizando series asintóticas, pensando que el término de error tendía a cero. Hardy tuvo que demostrarle que la serie no era finita, aunque la aproximación para $p(200)$ arrojaba un error de apenas $0.004\,\%$. Esta tensión entre la visión de Ramanujan sobre qué términos debían dominar la fórmula y la técnica de Hardy para acotar los errores culminó en la creación de una nueva estrategia: deformar el contorno de integración para acercarse a las singularidades "pesadas" de la función generatriz (las raíces de la unidad de orden bajo) y alejarse de las menos significativas. Esta estrategia, publicada en su célebre artículo de 1918 *Asymptotic Formulae in Combinatory Analysis* [2], no solo resolvió el problema de las particiones con una precisión que dejó atónito a MacMahon, sino que inauguró una nueva era en la teoría analítica de números. Había nacido el Método del Círculo.

Lo que sigue a continuación es el corazón técnico de su logro: una explicación de cómo transformaron esta intuición geométrica y modular en una de las fórmulas asintóticas más célebres de la matemática.[1]

El primer paso, encaminado a la prueba de Hardy y Ramanujan, es dejar de considerar a la función generadora de las particiones como meramente una serie formal, y considerarla como una función en variable compleja z. Consideremos la función definida como

$$\phi(z) := \prod_{k=1}^{\infty} (1 - z^k)$$

vamos a probar que dicha función es analítica en el disco unitario $\mathbb{D} = \{z \in \mathbb{C} : |z| < 1\}$, para esto usaremos la teoría de productos infinitos, los resultados utilizados se pueden encontrar en [17]. Dado un producto infinito, podemos determinar cuando este es convergente usando criterios series de números reales.

Lema 2.1.1

Sea $\{a_k\} \subset \mathbb{C}$ sucesión. El producto

$$\prod_{k=1}^{\infty} (1 + a_k) := \lim_{N \to \infty} \prod_{k=1}^{N} (1 + a_k)$$

converge absoluta y uniformemente, si la serie

$$\sum_{k=1}^{\infty} |a_k|$$

converge uniformemente.

Con ello podemos definir para cada $N \in \mathbb{Z}^+$ y $z \in \mathbb{D}$, la sucesión de funciones

$$\phi_N(z) = \prod_{k=1}^{N} (1 - z^k)$$

entonces dado que para cada N, $\phi_N(z)$ es analítica en $\mathbb{D}$ (pues es producto de polinomios) , el **teorema de convergencia de Weierstrass** nos garantiza que si dicha sucesión de funciones converge uniformemente en subconjuntos compactos de $\mathbb{D}$ entonces la función limite $(\phi(z))$ sera analítica en $\mathbb{D}$.

[1] Los detalles aquí mostrados serán una representación lo mas fiel posible a lo hecho originalmente por Hardy y Ramanujan, pero adaptándolo a la notación de este documento y a la actual en las matemáticas.

Proposición 2.1.1

Sea $K \subset \mathbb{D}$ subconjunto compacto, entonces el producto

$$\prod_{k=1}^{\infty}(1-z^k)$$

converge uniformemente para todo $z \in K$.

Demostración. Como K es subconjunto compacto, entonces existe un $0 < r < 1$ tal que $|z| \leq r$ para todo $z \in K$. Sea $z \in K$ y definamos la sucesión $a_k = -z^k$, entonces tendremos

$$\sum_{k=1}^{\infty}|a_k| = \sum_{k=1}^{\infty}|z|^k \leq \sum_{k=1}^{\infty} r^k < \infty$$

Por el **criterio M de Weierstrass**, la serie $\sum_{k=1}^{\infty}|a_k|$ converge absoluta y uniformemente en K. Entonces por el Lema 2.1.1 el producto infinito $\prod_{k=1}^{\infty}(1-z^k)$ converge uniformemente en K. □

De esta manera, dado que $\phi(z) = \prod_{k=1}^{\infty}(1-z^k)$ es analítica en $\mathbb{D}$ y sus ceros son aquellos tales que $1-z^k = 0$, es decir, raíces de la unidad, tendremos que su reciproco $\prod_{k=1}^{\infty}\left(\frac{1}{1-z^k}\right)$ es una función analítica en $\mathbb{D}$, que ademas, como producto es convergente absoluta y uniformemente para cada $z \in \mathbb{D}$. Con ello si consideramos la expansión en series de cada producto

$$\prod_{k=1}^{\infty}\sum_{m=0}^{\infty}(z^k)^m$$

la convergencia absoluta nos garantiza que podremos re ordenar los términos de estas series , por lo cual queda totalmente justificado el análisis hecho en el Teorema 1.3.1 con lo queda demostrado la formula de la función generadora de las particiones, siendo una función analítica y convergente para $|z| < 1$

$$P(z) = \sum_{n=0}^{\infty}p(n)z^n = \prod_{k=1}^{\infty}\left(\frac{1}{1-z^k}\right)$$

Una vez que ya entendemos a nuestra función generadora como una función analítica, podemos hacer uso del análisis complejo. Esto fue algo en lo que Hardy era experto, de esta manera dado $P(z)$ la formula integral de Cauchy nos garantiza que dada γ contorno circular centrado en el origen con radio $\rho < 1$,

$$P^{(n)}(0) := \frac{n!}{2\pi i}\int_{\gamma}\frac{P(z)}{(z-0)^{n+1}}dz$$

desarrollando

$$p(n) = [z^n]P(z) = \frac{P^{(n)}(0)}{n!} = \frac{1}{2\pi i}\int_{\gamma}\frac{P(z)}{z^{n+1}}dz \tag{2.1.1}$$

por lo que el numero de particiones de un entero n queda determinado por una integral de linea sobre el plano complejo de la función generadora. Analizando el integrando, la función $\frac{P(z)}{z^{n+1}}$ tiene un polo de orden $n+1$ en el origen, ademas a esto, el teorema de

Cauchy nos garantiza que el valor de la integral no depende de la curva γ, estos dos hechos intuyeron a Ramanujan a creer que al tomar un contorno γ con radio cercano a 1, las singularidades en la frontera de $\mathbb{D}$ de la función $P(z)$ aportarían la información necesaria para encontrar una formula para la función partición. ¿Cuales son las singularidades de $P(z)$? Teniendo

$$P(z) = \prod_{k=1}^{\infty} \left(\frac{1}{1-z^k} \right)$$

sus singularidades[2] vendrán dadas donde cada producto se indetermina, es decir, los ceros de $1-z^k$ para cada k, los cuales son las raíces k-esima de la unidad.

$$z_{k,m} = \exp\left(2\pi i \frac{m}{k}\right), \text{ con } m = 0, ..., k-1$$

En este sentido, podemos ver que tanto aparece cada singularidad en el producto, viendo las singularidades que aporta cada producto

$$k=1 \Rightarrow 1-z \quad \text{aporta } z_{1,0} = \exp\left(2\pi i \frac{0}{1}\right) \quad 1$$

$$k=2 \Rightarrow 1-z^2 \quad \text{aporta} \begin{cases} z_{2,0} = \exp\left(2\pi i \frac{0}{2}\right) & 1 \\ z_{2,1} = \exp\left(2\pi i \frac{1}{2}\right) & -1 \end{cases}$$

$$k=3 \Rightarrow 1-z^3 \quad \text{aporta} \begin{cases} z_{3,0} = \exp\left(2\pi i \frac{0}{3}\right) & 1 \\ z_{3,1} = \exp\left(2\pi i \frac{1}{3}\right) & -\frac{1}{2} + \frac{\sqrt{3}}{2} i \\ z_{3,2} = \exp\left(2\pi i \frac{2}{3}\right) & -\frac{1}{2} - \frac{\sqrt{3}}{2} i \end{cases}$$

$$k=4 \Rightarrow 1-z^4 \quad \text{aporta} \begin{cases} z_{4,0} = \exp\left(2\pi i \frac{0}{4}\right) & 1 \\ z_{4,1} = \exp\left(2\pi i \frac{1}{4}\right) & i \\ z_{4,2} = \exp\left(2\pi i \frac{2}{4}\right) & -1 \\ z_{4,3} = \exp\left(2\pi i \frac{3}{4}\right) & -i \end{cases}$$

$$k=5 \Rightarrow 1-z^5 \quad \text{aporta} \begin{cases} z_{5,0} = \exp\left(2\pi i \frac{0}{5}\right) & 1 \\ z_{5,1} = \exp\left(2\pi i \frac{1}{5}\right) & * \\ z_{5,2} = \exp\left(2\pi i \frac{2}{5}\right) & * \\ z_{5,3} = \exp\left(2\pi i \frac{3}{5}\right) & * \\ z_{5,4} = \exp\left(2\pi i \frac{4}{5}\right) & * \end{cases}$$

$$k=6 \Rightarrow 1-z^6 \quad \text{aporta} \begin{cases} z_{6,0} = \exp\left(2\pi i \frac{0}{6}\right) & 1 \\ z_{6,1} = \exp\left(2\pi i \frac{1}{6}\right) & * \\ z_{6,2} = \exp\left(2\pi i \frac{2}{6}\right) & -\frac{1}{2} + \frac{\sqrt{3}}{2} i \\ z_{6,3} = \exp\left(2\pi i \frac{3}{6}\right) & -1 \\ z_{6,4} = \exp\left(2\pi i \frac{4}{6}\right) & -\frac{1}{2} - \frac{\sqrt{3}}{2} i \\ z_{6,5} = \exp\left(2\pi i \frac{5}{6}\right) & * \end{cases}$$

Aquí podemos notar que habrá repeticiones en las singularidades, el caso mas claro es $z=1$, pues para cada $k \in \mathbb{Z}^+$, $z_{k,0} = \exp\left(2\pi i \frac{0}{k}\right) = 1$, por lo que la **singularidad**

[2]En el sentido estricto no son singularidades, pues estas están fuera del dominio en donde definimos a la función, ademas de ser polos de orden "infinito"

mas fuerte se encuentra en $z = 1$ ya que esta presente en todos los productos. Siguiendo podemos notar a $z = -1$, donde $z_{2,1} = z_{4,2} = z_{6,3} = -1$ y esto ocurrirá siempre y cuando $\frac{m}{k} = \frac{1}{2}$ lo que implica $m = \frac{k}{2}$, por lo que para cada k par (por ejemplo 2, 4, 6) el factor $1 - z^k$ aportara la singularidad $z = -1$. Podemos pensar en la siguiente singularidad, pues $z = \exp\left(2\pi i \frac{1}{3}\right)$ aparece siempre que k sea múltiplo de 3 y $m = \frac{k}{2}$ ($z_{3,1} = z_{6,2} = z_{9,3}$) y en el caso de $z = \exp\left(2\pi i \frac{2}{3}\right)$ aparecerá siempre que $\frac{m}{k} = \frac{2}{3}$ y esto es si y solo si $m = 2q$ y $k = 3q$, por ejemplo con $q = 1, 2, 3$, $z_{3,2} = z_{6,4} = z_{9,6}$.

Con el análisis anterior podemos considerar a S_N el conjunto de singularidades de producto truncado $P_N(z) = \prod_{k=1}^{N} \left(\frac{1}{1-z^k}\right)$, de forma que

$$S_N = \left\{ \exp\left(2\pi i \frac{m}{k}\right) : 1 \leq k \leq N,\ 1 \leq m < k \text{ con } (k, m) = 1 \right\}$$

Es decir, las singularidades corresponden a las raíces de la unidad donde la fracción $\frac{m}{k}$ es una fracción reducida, y cualquier otra es una repetición. Ahora cabe preguntarse **¿Que tanto aporta cada singularidad?** o dicho de otro modo **¿De que orden son estos polos en el producto truncado?**

Analicemos los casos puntuales:

- **Para $z = 1$:** Sabemos que $z_{k,0} = 1$ para todo $1 \leq k \leq N$. Por tanto, el factor $1 - z^k$ se anula en cada termino del producto, resultando un polo de orden N. Para $z = -1$ (donde $\frac{m}{k} = \frac{1}{2}$), la singularidad aparece si y solo si el término $(1 - z^j)$ se anula, lo cual ocurre cuando $z^j = 1$. Dado que$(-1)^j = 1$ solo si j es par, contamos cuántos pares existen entre 1 y N. Así, $z = -1$ es un polo de orden $\left\lfloor \frac{N}{2} \right\rfloor$.

- **Para $z = \exp\left(2\pi i \frac{1}{3}\right)$**: La condición para que sea polo es que $z^j = 1$, lo que implica $\frac{j}{3} \in \mathbb{Z}^+$. Esto ocurre si y solo si$j$ es múltiplo de 3. La cantidad de múltiplos de 3 entre 1 y N es $\left\lfloor \frac{N}{3} \right\rfloor$, determinando así su orden. Finalmente, consideremos $z = \exp\left(2\pi i \frac{2}{3}\right)$. Aquí la condición de polo $z^j = 1$ implica $\exp\left(2\pi i \frac{2j}{3}\right) = 1$, es decir, $\frac{2j}{3} \in \mathbb{Z}^+$. Dado que $(2, 3) = 1$, esto fuerza necesariamente a que 3 divida a j. Notamos entonces que la condición es idéntica al caso anterior: no depende del numerador $m = 2$, sino únicamente del denominador $k = 3$. Por tanto, el orden es nuevamente $\left\lfloor \frac{N}{3} \right\rfloor$.

Con esto tendremos en general que dado $z = \exp\left(2\pi i \frac{m}{k}\right)$ con $(m, k) = 1$, su contribución como polo en el producto truncado vendrá dada por la cantidad de veces que $z^j = 1$ para $1 \leq j \leq N$. Debido a que m y k son primos relativos, la condición $\frac{mj}{k} \in \mathbb{Z}^+$ se satisface si y solo si k divide a j. Por lo tanto, el polo es de orden $\left\lfloor \frac{N}{k} \right\rfloor$.

¿Que nos dice todo esto? Todo lo hecho en el párrafo anterior nos da dos propiedades importantes acerca de los polos de mayor aportación, la primera; son unicamente aquellos para los cuales k y m son primos relativos, o dicho de otra manera, aquellos números complejos $\exp\left(2\pi i \frac{m}{k}\right)$ en el disco unitario con angulo una **fracción reducida del circulo** y segunda; los polos de mayor aportación serán aquellos con **denominador pequeño**.

Estos dos hechos fueron los que inspiraron a Hardy y Ramanujan a "diseccionar" el circulo unitario en las partes de "mayor aportación" y de "menor aportación" y para lograr este objetivo hicieron uso de la **secuencia de Farey** de orden N, denotada como $\mathcal{F}_N$. Esta secuencia consiste en todas las fracciones reducidas $\frac{m}{k}$ en [0,1] con denominador $k \leq N$ ordenadas de manera creciente, es decir, las mismas que ya estamos trabajando, pero con la diferencia de que consideramos una sucesión de conjuntos de fracciones reducidas

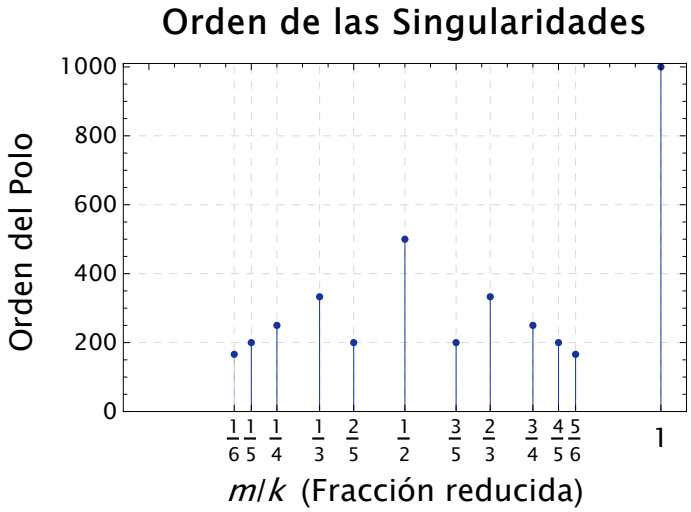

Figura 2.1.1: *Orden de los polos para $N = 1000$. Se observa que las singularidades con denominadores k pequeños poseen los órdenes más altos, dominando el comportamiento asintótico frente a aquellas con k grande.*

donde se agregan cada vez mas fracciones de menor aporte. Los primeros términos de la secuencia son:

$$\mathcal{F}_1 = \left\{\frac{0}{1}, \frac{1}{1}\right\}$$
$$\mathcal{F}_2 = \left\{\frac{0}{1}, \frac{1}{2}, \frac{1}{1}\right\}$$
$$\mathcal{F}_3 = \left\{\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}\right\}$$
$$\mathcal{F}_4 = \left\{\frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}\right\}$$
$$\mathcal{F}_5 = \left\{\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}\right\}$$

Con esto, tomando ρ suficientemente cercano a 1, tendremos que la curva γ en 2.1.1 vendrá parametrizada por $\gamma(\theta) = \rho \exp(2\pi i\theta)$ con $\theta \in [0, 1]$, de forma que

$$p(n) = \frac{1}{2\pi i}\int_\gamma \frac{P(z)}{z^{n+1}}dz = \rho^{-n}\int_0^1 P(\rho e^{2\pi i\theta})e^{-2\pi in\theta}d\theta$$

Entonces el objetivo sera dividir el intervalo $[0, 1]$ en subintervalos que contengan a las fracciones de mayor aportación, es decir, en "arcos" disjuntos $\xi_{m,k}$, cada uno centrado en una fracción de Farey, pero ¿Como lo hacemos?. Para esto podemos ver las propiedades clave de las secuencias de Farey.

Dadas dos fracciones en una secuencia de Farey, diremos que son **vecinos** si una sigue a la otra, por ejemplo, $\frac{1}{4}$ y $\frac{1}{3}$ son vecinos en la secuencia $\mathcal{F}_4$. Esta idea de "vecinos" en una secuencia de Farey nos ayudara a distinguir cuando una fracción reducida sigue de otra, pero para que nos sea de utilidad necesitaremos un criterio que nos asegure cuando es que dos fracciones serán vecinos..

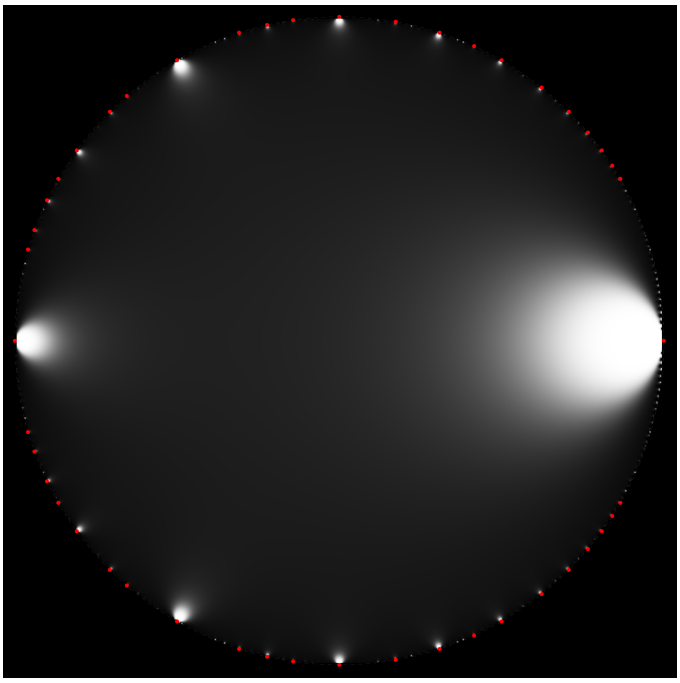

Figura 2.1.2: *Visualización de la magnitud de la función generadora truncada* $P_N(z)$ *con* $N = 300$*, sobre el disco de radio* $\rho = 0.999$*. La figura fue elaborada utilizando* ***Wolfram Mathematica****, implementando computacionalmente la identidad* $P_N(z) = 1/(z;z)_N$*, donde* $(z;z)_N$ *denota el q-Pochhammer symbol, mediante la función* ***QPochhammer****. La representación se realizó con* ***ComplexPlot****, empleando una escala de color basada en la magnitud* $\log(1+|P_N(z)|)$*, de modo que los tonos claros indican regiones donde* $|P_N(z)|$ *crece rápidamente al aproximarse a las singularidades situadas en la frontera del disco unitario, mientras que el interior del disco permanece en niveles de magnitud significativamente menores. Los puntos rojos son las singularidades de* $P_{12}(z)$*. Note como las singularidades con denominador pequeño dominan el crecimiento.*

Lema 2.1.2

Dos fracciones $\frac{a}{b}$ y $\frac{c}{d}$ serán vecinos en una secuencia de Farey si y solo si

$$|ad - bc| = 1 \tag{2.1.2}$$

Dada una fracción de Farey, por definición, esta siempre tendrá vecinos. Ademas de este resultado, podremos obtener "puntos medios" entre dos fracciones de Farey. Dados $\frac{a}{b} < \frac{c}{d}$ definimos su **mediante** como la fracción $\frac{a+c}{b+d}$, esta mediante tendrá la particularidad de ser un un punto entre las fracciones originales, pues resultara que $\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$, pero esta desigualdad es unicamente como fracciones reales ¿Como se comparan como fracciones de Farey? Esta pregunta tiene sentido pues resultara que la mediante siempre es una fracción reducida, por lo que pertenecerá a una secuencia de Farey.

Podemos notar que, en general, dos fracciones arbitrarias de $\mathcal{F}_N$ no serán vecinas, ya que la condición necesaria y suficiente para que $\frac{a}{b}$ y $\frac{c}{d}$ lo sean es que $|ad - bc| = 1$. Por ejemplo, en $\mathcal{F}_4$, tomando $\frac{1}{4}$ y $\frac{2}{3}$, se tiene

$$|1 \cdot 3 - 4 \cdot 2| = 5$$

por lo que no son vecinas. Su mediante es $\frac{3}{7}$, la cual no pertenece a $\mathcal{F}_4$, sino a $\mathcal{F}_7$. Ademas

$$|4 \cdot 3 - 1 \cdot 7| = 5 \quad \text{y} \quad |3 \cdot 3 - 2 \cdot 7| = 5$$

por lo que tampoco es vecina de ninguna de las fracciones originales en $\mathcal{F}_7$. En cambio, si tomamos dos fracciones vecinas, por ejemplo $\frac{1}{4}$ y $\frac{1}{3}$ en $\mathcal{F}_4$, entonces

$$|1 \cdot 3 - 4 \cdot 1| = 1$$

y su mediante en $\frac{2}{7}$ la cual no pertenece a $\mathcal{F}_4$, sino a $\mathcal{F}_7$. En este caso se verifica que

$$|4 \cdot 2 - 1 \cdot 7| = 1 \quad \text{y} \quad |3 \cdot 2 - 1 \cdot 7| = 1$$

por lo que $\frac{2}{7}$ resulta ser vecina de ambas fracciones originales en $\mathcal{F}_7$. En consecuencia, la mediante de dos fracciones vecinas aparece como fracción intermedia y vecina de ambas en alguna sucesión de Farey de orden mayor. Esta propiedad nos dará lo necesario para definir correctamente nuestros arcos.

Definición 2.1.1 Arcos de Farey

Sea $\mathcal{F}_N$ secuencia de Farey de orden N. Para cada $\frac{m}{k} \in \mathcal{F}_N$ consideremos los vecinos $\frac{m_1}{k_1}$ y $\frac{m_2}{k_2}$ de $\frac{m}{k}$, con $\frac{m_1}{k_1} < \frac{m}{k} < \frac{m_2}{k_2}$. Definimos el arco de circunferencia $\xi_{m,k}$ asociado a la fracción $\frac{m}{k}$, como la curva parametrizada como

$$\xi_{m,k}(\theta) = \rho \exp(2\pi i \theta), \quad \rho > 0$$

con θ extendiéndose en el intervalo de las mediantes de cada vecino, es decir,

$$\theta \in \left[\frac{m_1 + m}{k_1 + k}, \frac{m + m_2}{k + k_2} \right]$$

Notemos que en particular $0 = \frac{0}{1}$ no tiene vecino izquierdo en $\mathcal{F}_N$, pero si tiene vecino derecho siendo $\frac{1}{N}$ (que siempre es la segunda fracción), es por ello que para $\xi_{0,1}$ consideramos el intervalo desde 0 hasta la mediante entre $\frac{0}{1}$ y $\frac{1}{N+1}$,

$$\xi_{0,1} \to \left[0, \frac{1}{N+1} \right]$$

similarmente para $1 = \frac{1}{1}$ el único vecino en $\mathcal{F}_N$ es $\frac{N-1}{N}$ (que siempre es la penúltima fracción), entonces consideramos intervalo desde la mediante entre $\frac{N-1}{N}$ y $\frac{1}{1}$ hasta 1,

$$\xi_{1,1} \to \left[\frac{N}{N+1}, 1 \right]$$

Estos arcos nos dan una separación de regiones donde domina cada singularidad $\frac{m}{k} \in \mathcal{F}_N$ (de hecho son el centro) que se extienden hasta las mediantes extremas. La construcción dada por las mediantes nos garantizaran que los extremos del arcos son exactamente los puntos de transición entre el arco $\xi_{m,k}$, y los arcos vecinos.

Lema 2.1.3

Sea $\mathcal{F}_N$ secuencia de Farey de orden N. Los intervalos definidos por las mediantes de cada fracción, forman una partición del intervalo $[0, 1]$. A esta partición se le conoce como **Disección de Farey**.

En la disección de Farey, los arcos $\xi_{0,1}$ y $\xi_{1,1}$ corresponden a los extremos del intervalo $[0,1]$. El punto $\exp(2\pi i) = 1$ queda simultáneamente en la frontera de ambos, pero en la integración sobre el círculo (parametrizada de 0 a 1) este punto pertenece naturalmente al arco final $\xi_{1,1}$. No es necesario que la singularidad 1 quede en el centro del arco: su contribución a la integral proviene de un vecindario pequeño alrededor de ese extremo.

Ejemplo. La disección de Farey correspondiente a $\mathcal{F}_3 = \left\{\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}\right\}$ sera la partición formada por los intervalos que definen a cada sección de arco, esta disección encerrara a cada una de las singularidades de $P_3(z)$ como se muestra en la Figura 2.1.3. La descripción de cada intervalo se hace calculando las mediantes:

$$\begin{aligned}
\exp(2\pi i\tfrac{0}{1}) \to \tfrac{0}{1} \to \xi_{0,1} &\to \left[0, \frac{1}{3+1}\right] &&= \left[0, \frac{1}{4}\right] \\
\exp(2\pi i\tfrac{1}{3}) \to \tfrac{1}{3} \to \xi_{1,3} &\to \left[\frac{0+1}{1+3}, \frac{1+1}{3+2}\right] &&= \left[\frac{1}{4}, \frac{2}{5}\right] \\
\exp(2\pi i\tfrac{1}{2}) \to \tfrac{1}{2} \to \xi_{1,2} &\to \left[\frac{1+1}{3+2}, \frac{1+2}{2+3}\right] &&= \left[\frac{2}{5}, \frac{3}{5}\right] \\
\exp(2\pi i\tfrac{2}{3}) \to \tfrac{2}{3} \to \xi_{2,3} &\to \left[\frac{1+2}{2+3}, \frac{2+1}{3+1}\right] &&= \left[\frac{3}{5}, \frac{3}{4}\right] \\
\exp(2\pi i\tfrac{1}{1}) \to \tfrac{1}{1} \to \xi_{1,1} &\to \left[\frac{3}{3+1}, 1\right] &&= \left[\frac{3}{4}, 1\right]
\end{aligned}$$

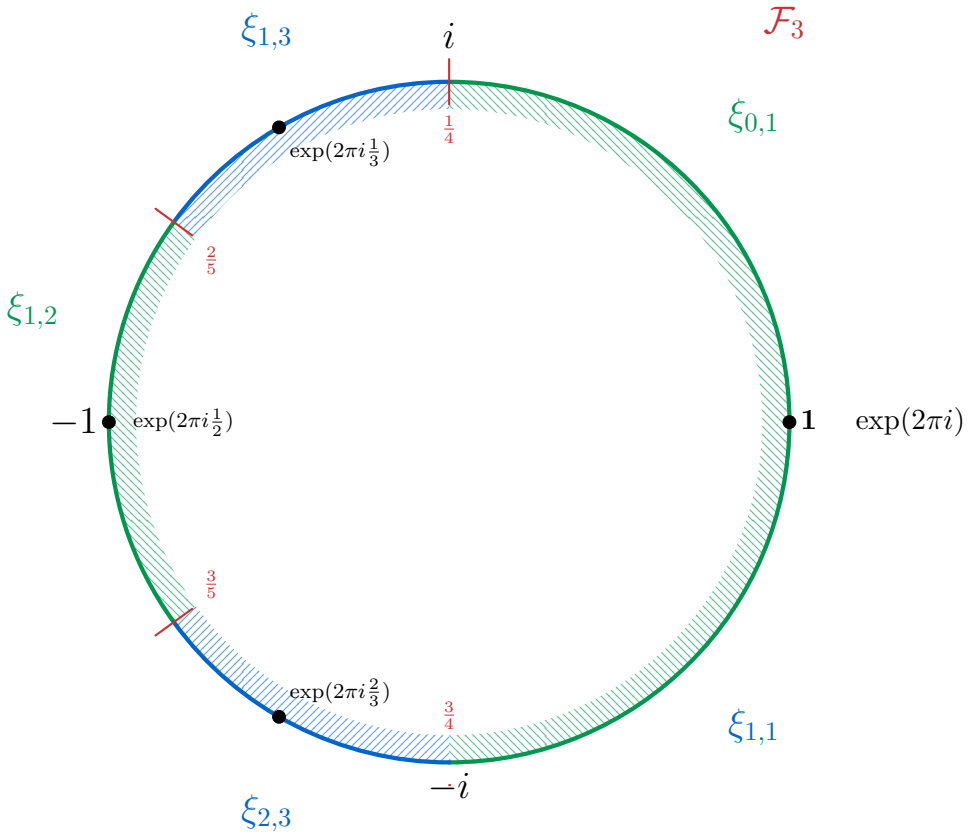

Figura 2.1.3: *Disección de Farey correspondiente a $\mathcal{F}_3$. Los puntos negros representan las singularidades de $P_3(z)$, las lineas rojas representan la sección del disco unitario correspondiente.*

De la misma manera podemos ver la disección de Farey correspondiente a $\mathcal{F}_4$ sobre el disco unitario (Figura 2.1.4). En este caso $\mathcal{F}_4 = \left\{\frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}\right\}$, por lo que calculando las mediantes,

$$\begin{aligned}
\exp(2\pi i\frac{0}{1}) \to \frac{0}{1} \to \xi_{0,1} &\to \left[0, \frac{0+1}{1+4}\right] &&= \left[0, \frac{1}{5}\right] \\
\exp(2\pi i\frac{1}{4}) \to \frac{1}{4} \to \xi_{1,4} &\to \left[\frac{0+1}{1+4}, \frac{1+1}{4+3}\right] &&= \left[\frac{1}{5}, \frac{2}{7}\right] \\
\exp(2\pi i\frac{1}{3}) \to \frac{1}{3} \to \xi_{1,3} &\to \left[\frac{1+1}{4+3}, \frac{1+1}{3+2}\right] &&= \left[\frac{2}{7}, \frac{2}{5}\right] \\
\exp(2\pi i\frac{1}{2}) \to \frac{1}{2} \to \xi_{1,2} &\to \left[\frac{1+1}{3+2}, \frac{1+2}{2+3}\right] &&= \left[\frac{2}{5}, \frac{3}{5}\right] \\
\exp(2\pi i\frac{2}{3}) \to \frac{2}{3} \to \xi_{2,3} &\to \left[\frac{1+2}{2+3}, \frac{2+3}{3+4}\right] &&= \left[\frac{3}{5}, \frac{5}{7}\right] \\
\exp(2\pi i\frac{3}{4}) \to \frac{3}{4} \to \xi_{3,4} &\to \left[\frac{2+3}{3+4}, \frac{3+1}{4+1}\right] &&= \left[\frac{5}{7}, \frac{4}{5}\right] \\
\exp(2\pi i\frac{1}{1}) \to \frac{1}{1} \to \xi_{1,1} &\to \left[\frac{3+1}{4+1}, 1\right] &&= \left[\frac{4}{5}, 1\right]
\end{aligned}$$

Como mencionamos, la disección de Farey captura a las singularidades de la función generadora de particiones, pero esto no es lo único que sera relevante en esta forma de particionar el intervalo $[0, 1]$, pues resultara que también sera la mejor manera de atrapar el aporte "mayor" y "menor" de las singularidades.

Dado un arco $\xi_{m,k}$ en la disección de orden N, tendremos que la longitud de dicho arco vendrá dado por $\mathcal{L}_{m,k} = \beta$ donde β es el angulo de dicho arco desde el centro del disco unitario. Dado que $\xi_{m,k}$ viene parametrizado por $2\pi\theta$, con dicho angulo en el intervalo $\left[\frac{m_1+m}{k_1+k}, \frac{m+m_2}{k+k_2}\right]$, entonces

$$\begin{aligned}
\beta &= 2\pi\frac{m+m_2}{k+k_2} - 2\pi\frac{m_1+m}{k_1+k} = 2\pi\left(\frac{m+m_2}{k+k_2} - \frac{m_1+m}{k_1+k}\right) \\
&= 2\pi\left(\left(\frac{m+m_2}{k+k_2} - \frac{m}{k}\right) + \left(\frac{m}{k} - \frac{m_1+m}{k_1+k}\right)\right) \\
&= 2\pi\left(\frac{km_2 - mk_2}{k(k+k_2)} + \frac{mk_1 - km_1}{k(k+k_1)}\right)
\end{aligned}$$

dado que $\frac{m}{k}$ y los extremos son vecinos, tendremos por 2.1.2, $km_2 - mk_2 = 1$ y $mk_1 - km_1 = 1$, así

$$\mathcal{L}_{m,k} = 2\pi\left(\frac{1}{k(k+k_2)} + \frac{1}{k(k+k_1)}\right)$$

Para establecer el comportamiento asintótico de esta magnitud cuando $N \to \infty$, recurrimos a una propiedad estructural de las sucesiones de Farey: la suma de los denominadores de cualesquiera dos fracciones consecutivas en $\mathcal{F}_N$ siempre excede el orden de la disección, pero no supera el doble del mismo. Es decir, para los vecinos de $\frac{m}{k}$ se satisface que

$$N < k + k_1 \leq 2N \quad \text{y} \quad N < k + k_2 \leq 2N$$

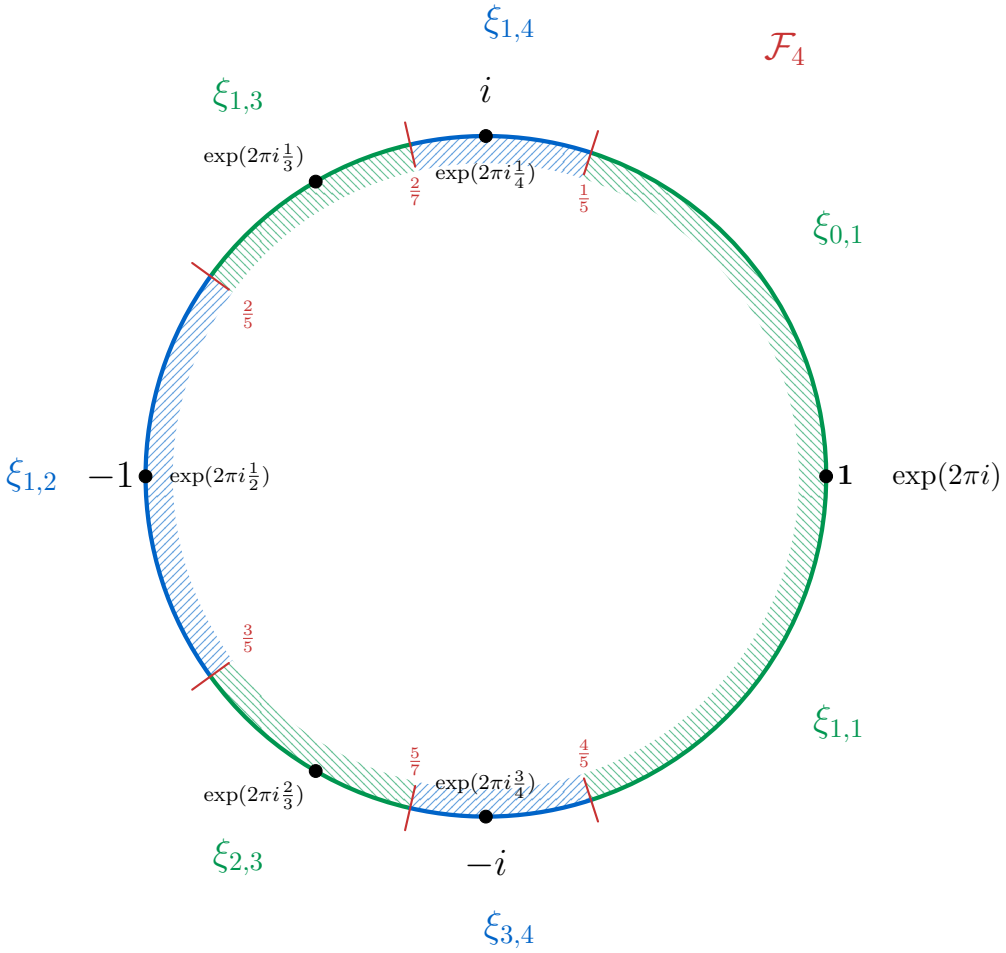

Figura 2.1.4: *Disección de Farey correspondiente a* $\mathcal{F}_4$.

esta desigualdad garantiza que las sumas $k+k_1$ y $k+k_2$ son asintóticamente del orden de N, de donde se deduce que

$$\frac{1}{2kN} \leq \frac{1}{k(k+k_i)} \leq \frac{1}{kN}, \quad i=1,2$$

por lo que

$$\frac{2\pi}{kN} \leq \mathcal{L}_{m,k} \leq \frac{4\pi}{kN}$$

es decir

$$\mathcal{L}_{m,k} \asymp \frac{1}{kN}, \quad \text{cuando } N \to \infty$$

Esta relación revela que la longitud del arco $\xi_{m,k}$ decrece inversamente con el producto del orden de la disección N y el denominador k en cada singularidad de modo que, **para valores de k pequeños, el arco es ancho**. Esto es vital porque necesitamos integrar sobre una región grande para capturar toda la contribución asintótica dominante, mientras que para k grande el arco es muy estrecho por lo que las singularidades mas "debiles" de la función serán de menor aportación en estos arcos (observe figura 2.1.4).

Todo este análisis le dio a Hardy y Ramanujan la forma de descomponer la integral en cada arco. Dado $N \in \mathbb{Z}^+$, se toma la disección de Farey de orden N del intervalo $[0,1]$

por lo que [3]

$$p(n) = \rho^{-n} \int_0^1 P(\rho e^{2\pi i\theta}) e^{-2\pi i n\theta} d\theta = \sum_{k=1}^{N} \sum_{\substack{0\leq m<k \\ (m,k)=1}} \rho^{-n} \int_{\xi_{m,k}} P(\rho e^{2\pi i\theta}) e^{-2\pi i n\theta} d\theta \qquad (2.1.3)$$

El paso más técnico y profundo del método consiste en evaluar el comportamiento de la función generadora $P(z)$ en las vecindades dadas por la diseccion de Farey de la singularidad $\exp(2\pi i\frac{m}{k})$. Para lograrlo, Hardy y Ramanujan aprovecharon la íntima relación entre $P(z)$ y la función **eta de Dedekind**, $\eta(\tau)$, definida como $\eta(\tau) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$ con $q = e^{2\pi i\tau}$. Dado que nuestra función de particiones es esencialmente el recíproco de la función eta:

$$F(e^{2\pi i\tau}) = \frac{e^{\pi i\tau/12}}{\eta(\tau)}$$

La herramienta clave usada por Hardy y Ramanujan fue la ecuación funcional que satisface $\eta(\tau)$ bajo transformaciones modulares. Específicamente, bajo la inversión $\tau \to -1/\tau$ (y sus generalizaciones para m/k), la función eta permite relacionar su valor cerca de una singularidad con su valor cerca del origen o del infinito.

Mediante el cambio de variable $z \to \exp\left(\frac{2\pi im}{k} - \frac{2\pi z}{k}\right)$ se logra poder estudiar el comportamiento de $P(z)$ cerca de la singularidad aproximándonos a m. Mediante la fórmula de transformación de Dedekind, es posible expresar el valor de la función en términos de una nueva variable transformada. A diferencia de una aproximación simple, la transformación modular completa retiene tanto el término dominante como los términos de menor orden, resultando en la expresión:

$$F\left(e^{\frac{2\pi im}{k} - \frac{2\pi z}{k}}\right) \approx \omega_{m,k}\sqrt{z}\exp\left(\frac{\pi}{12z} - \frac{\pi z}{12k^2}\right) \qquad (2.1.4)$$

donde $\omega_{m,k}$ es el llamado **multiplicador de Dedekind** (una raíz de la unidad de orden 24). En esta expresión "aproximada", el primer término exponencial $\exp(\pi/12z)$ captura el crecimiento exponencial de la función cerca de la singularidad, mientras que el segundo término $\exp(-\pi z/12k^2)$ proviene del ajuste modular exacto, el cual, aunque pequeño cuando $z \to 0$, es importante para la precisión teórica.

Sustituyendo la aproximación 2.1.4 en la expresión 2.1.3 se obtiene una expresión para $p(n)$ como una suma de términos tanto aritméticos como analíticos. Al hacer dichas evaluaciones llegaron a la siguiente representación:

$$p(n) = \sum_{k=1}^{N} A_k(n)\phi_k(n) \qquad (2.1.5)$$

y confiaban en que la igualdad se cumpliría al hacer tender $N \to \infty$, es decir, al considerar cada vez disecciones de Farey mas finas. Los componentes de la ecuación 2.1.5 son:

- **La parte aritmética** $A_k(n)$: Una suma trigonométrica (conocida actualmente como suma de Kloosterman) que refleja el comportamiento de oscilación constructiva y destructiva de las raíces de la unidad

$$A_k(n) = \sum_{\substack{0\leq m<k \\ (m,k)=1}} \omega_{m,k} e^{-2\pi i\frac{m}{k}}$$

[3] Aquí la integral $\int_{\xi_{m,k}} ...d\theta$ se entenderá como la integral sobre el intervalo asociado.

- **La parte analítica** $\phi_k(n)$: Una función que representa el crecimiento continuo, expresada por Hardy y Ramanujan mediante derivadas de funciones exponenciales (o hiperbólicas), donde $C = \pi\sqrt{\frac{2}{3}}$ y $\lambda_n = \sqrt{n}$

$$\phi_k(n) \approx \frac{1}{2\pi\sqrt{2}} \frac{d}{dn}\left(\frac{e^{C\cdot\lambda_n/k}}{\lambda_n}\right)$$

A partir de esta representación Hardy y Ramanujan se enfocaron en lo que pasaba al considera $n \to \infty$, notando que el primer termino de 2.1.5 dominaba sobre los demás, atrapando la contribución del arco de mayor aportación (donde se encuentra la singularidad mas fuerte $z = 1$), por tanto

$$p(n) \sim A_1(n)\phi_1(n)$$

por definición,

$$A_1(n) = \sum_{\substack{0\le m<1\\(m,1)=1}} \omega_{m,1} e^{-2\pi i \frac{m}{1}} = \omega_{0,1} e^{-2\pi i \frac{0}{1}} = 1$$

de este modo $p(n) \sim A_1(n)\phi_1(n)$, y por otro lado

$$\begin{aligned}\phi_1(n) &\approx \frac{1}{2\pi\sqrt{2}} \frac{d}{dn}\left(\frac{e^{C\cdot\sqrt{n}}}{\sqrt{n}}\right) = \frac{1}{2\pi\sqrt{2}} e^{C\cdot\sqrt{n}}\left[-\frac{1}{2n^{3/2}} + \frac{C}{2n}\right] \sim \frac{1}{2\pi\sqrt{2}} e^{C\cdot\sqrt{n}} \cdot \frac{C}{2n} \\ &\sim \frac{C}{4\pi n\sqrt{2}} e^{C\cdot\sqrt{n}}\end{aligned}$$

simplificando con el valor de C, obtenemos la formula asintótica de la función partición

$$\boxed{p(n) \sim \frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right)}$$

Este resultado por sí solo represento un avance monumental, proporcionando una precisión numérica asombrosa para valores grandes de n teniendo un error de alrededor del $0.004\,\%$. al compararlo con las tablas de MacMahon y confirmando el crecimiento exponencial de las particiones. Este resultado fue tan extraordinario para Ramanujan que el creía que la serie infinita obtenida al hacer $N \to \infty$ en 2.1.5 representaba el valor exacto de $p(n)$. Sin embargo, Hardy mostró que la serie infinita resultante no es absolutamente convergente cuando se emplea la función original $\phi_k(n)$. Por consiguiente, el método elaborado produce únicamente una expansión asintótica y no una fórmula exacta, pues no es valido intercambiar el límite con la suma infinita sin un control adicional de convergencia. Fue Hans Rademacher quien, años más tarde, logró eliminar este problema y transformar la aproximación asintótica en una igualdad. Para conseguir esta convergencia exacta, Rademacher tuvo que refinar tanto el contorno de integración como la precisión de las funciones analíticas involucradas.

A diferencia de lo hecho por Hardy y Ramanujan que distinguían entre los arcos de "mayor" y "menor" aportación, Rademacher trató a todos los arcos de la disección de Farey con la misma importancia. Utilizó la partición exacta del círculo (la misma que se ilustra en la Figura 2.1.4) para definir nuevos limites de integración $[\vartheta'_{h,k}, \vartheta''_{h,k}]$.

Sin embargo su mayor logro conceptual fue deformar el camino de integración a una forma aun mas detallada. En lugar de integrar sobre un círculo fijo de radio $\rho < 1$, Rademacher desplazó el contorno para que se moviera a través de los llamados **Círculos de Ford**. Estas son circunferencias tangentes al círculo unitario en cada punto racional $\exp(2\pi im/k)$. Al integrar sobre esta nueva curva, pudo sumar las contribuciones de todos los arcos $\xi_{m,k}$ sin despreciar ninguno, capturando así la aportación completa de las singularidades.

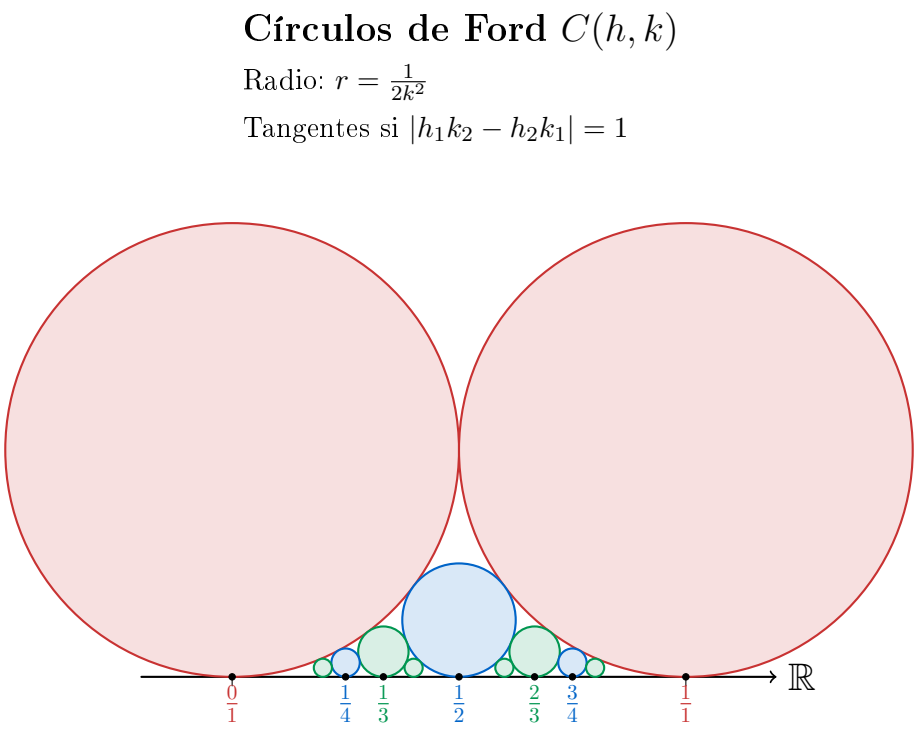

Figura 2.1.5: *Representación de los Círculos de Ford $C(h,k)$ en el semiplano superior. Cada círculo es tangente al eje real en la fracción irreducible h/k y tiene un radio de $r = \frac{1}{2k^2}$. Los colores indican el orden del denominador k: rojo ($k = 1$), azul ($k = 2, 4$) y verde ($k = 3, 5$). Dos círculos $C(h_1, k_1)$ y $C(h_2, k_2)$ son tangentes entre sí, si y solo si, sus fracciones correspondientes son vecinas en alguna sucesión de Farey, cumpliendo la condición $|h_1k_2 - h_2k_1| = 1$*

Para que la suma infinita convergiera absolutamente, Rademacher introdujo dos correcciones cruciales en la fórmula de $\phi_k(n)$. La primera fue incorporar el término $-1/24$ dentro de la raíz cuadrada, definiendo $\lambda_n = \sqrt{n - 1/24}$. Este término surge al considerar la ecuación funcional exacta de la función $\eta(\tau)$, aunque su efecto numérico es despreciable para n muy grande es de importancia para la convergencia. Y lo segundo fue que al evaluar las integrales sobre el contorno de Ford sin aproximaciones, descubrió que estas corresponden a representaciones integrales de las **funciones de Bessel modificadas de primera especie**, denotadas como $I_\nu(z)$ con índice semi-entero $\nu = 3/2$.

El resultado culminante es la célebre fórmula exacta de Rademacher para las particiones

$$p(n) = \frac{1}{\pi\sqrt{2}} \sum_{k=1}^{\infty} A_k(n)\sqrt{k} \left[\frac{d}{dx} \left(\frac{\sinh\left(\frac{\pi}{k}\sqrt{\frac{2}{3}\left(x - \frac{1}{24}\right)}\right)}{\sqrt{x - \frac{1}{24}}} \right) \right]_{x=n}$$

Esta serie no solo converge al valor entero exacto de $p(n)$, sino que lo hace con una rapidez extraordinaria; a menudo, los primeros términos de la suma ya proporcionan el valor entero correcto tras el redondeo. Para mas detalle sobre la prueba y el como se construyen los círculos de Ford se guiá al lector a [20] y [21].

La publicación del artículo *Asymptotic Formulae in Combinatory Analysis* en 1918 marcó el clímax de la colaboración Hardy-Ramanujan y un punto de inflexión en la matemática del siglo XX. La comunidad matemática recibió el trabajo con asombro; no solo habían resuelto un problema clásico de combinatoria, sino que habían forjado una herramienta analítica de potencia aun desconocida.

Ese mismo año, 1918, fue prolífico para Ramanujan a pesar de su salud en deterioro. Descubrió propiedades aritméticas profundas de la función de partición con ayuda de las tablas de MacMahon, conocidas como las congruencias de Ramanujan:

$$p(5m+4) \equiv 0 \pmod 5, \quad p(7m+5) \equiv 0 \pmod 7$$

Estas identidades revelaron que $p(n)$, lejos de ser una mera función de crecimiento exponencial, poseía una estructura interna modular fuerte.

En 1919, con la guerra terminada pero su salud quebrantada, Ramanujan regresó a la India. Lejos de la atmósfera académica de Cambridge, continuó produciendo matemáticas de primer nivel en su lecho de muerte, escribiendo su última carta a Hardy en enero de 1920 sobre las misteriosas "funciones theta falsas" (mock theta functions). Srinivasa Ramanujan falleció el 26 de abril de 1920, a la edad de 32 años.

La muerte de Ramanujan dejó a Hardy con la tarea de editar y publicar sus trabajos restantes, labor que cimentó la leyenda del genio Ramanujan. Sin embargo, la herramienta e ideas que habían creado juntos no murieron con él.

J. E. Littlewood, el colaborador de toda la vida de Hardy, junto con otros matemáticos de alto nivel como G. N. Watson y L. J. Mordell, retomaron el método desarrollado para la función partición. Comprendieron que la técnica de disección de Farey y el análisis de singularidades no se limitaba a las particiones, sino que podía adaptarse para atacar los problemas aditivos aun mas generales de la teoría de números. A esta técnica de considerar el circulo unitario y diseccionar en las partes de mayor y menor aportación, se le conoció entonces como el **Método del Circulo**.

2.2. Hardy y Littlewood

La prematura muerte de Ramanujan en 1920 marcó el fin de una era prolífica en Cambridge, pero no el fin del método que habían desarrollado. Hardy, ahora sin su compañero Ramanujan, se volcó hacia su colaborador más antiguo y constante: John Edensor Littlewood.

Littlewood, era un analista de potencia formidable y experto en desigualdades y teoría de funciones, poseía el rigor técnico necesario para transformar la brillante pero específica maquinaria diseñada para las particiones en una herramienta universal para la teoría aditiva de números. Juntos, emprendieron la monumental tarea de aplicar el Método del Círculo al Problema de Waring y a la Conjetura de Goldbach, en una célebre serie de artículos titulados **Some problems of Partitio Numerorum** publicados entre 1920 y 1928 [22].

Hardy y Littlewood comprendieron que la estructura lógica utilizada para $p(n)$ podía abstraerse para tratar cualquier problema aditivo. Pues la idea principal del método desarrollado consiste en trabajar con la función generadora del numero de particiones como una función analítica en el plano complejo, en ese sentido, podríamos aplicar el mismo análisis si consideramos la función generadora del numero de representaciones u particiones de un entero n como suma de elementos de un conjunto A, que es justo lo que desarrollamos en todo nuestro capitulo anterior. Para poder generalizar este método necesitamos nuevamente, dejar de considerar a las funciones generadoras como series formales y verlas como funciones en variable compleja.

Lema 2.2.1

Sea $A \subseteq \mathbb{Z}^+$ infinito. La función de representación de A, $f_A(z)$ es analítica en $\mathbb{D}$.

Demostración. Tenemos que

$$f_A(z) = \sum_{a\in A} z^a = \sum_{n=0}^{\infty} \delta_A(n) z^n$$

de modo que

$$\limsup_{n\to\infty} |\delta_A(n)|^{\frac{1}{n}} = 1$$

por tanto por el criterio de D´Lambert la serie converge absolutamente con radio de convergencia 1, ademas por ser serie de potencias la convergencia sera uniforme en subconjuntos compactos del disco y por tanto sera analítica para $|z| < 1$. □

De esta manera para cada $k \in \mathbb{Z}^+$ la función $f_A^k(z)$ sera analítica en $\mathbb{D}$ y dada la convergencia absoluta, el resultado del **Teorema 1.2.1** sera valido, de tal forma la funciones generadoras

$$R_{k,A}(z) = \sum_{n=0}^{\infty} r_{k,A}(n) z^n = f_A^k(z) \quad \text{y} \quad R_A(z) = \sum_{n=0}^{\infty} r_A(n) z^n = \frac{f_A(z)}{1 - f_A(z)}$$

serán analíticas en $\mathbb{D}$. A excepción de $R_A(z)$ la cual tendrá una singularidad cuando $f_A(z) = 1$, pero retomaremos este gran detalle mas adelante.

Para el caso de particiones podemos proseguir de forma similar a la **Proposición 2.1.1**, notando que para $a_k = -\delta_A(k) z^k$ se obtiene que

$$\phi_A(z) := \prod_{a\in A} (1 - z^a) = \prod_{k=1}^{\infty} (1 - \delta_A(k) z^k)$$

es analítica en $\mathbb{D}$, y por tanto la función generadora

$$P_A(z) = \sum_{n=0}^{\infty} r_A(n) z^n = \prod_{a\in A} \left(\frac{1}{1 - z^a} \right)$$

es una función analítica en $\mathbb{D}$. Sin embargo, la función generadora de particiones en k partes sera un trabajo mas elaborado. Para justificar la analiticidad procederemos de

manera análoga, pero utilizando herramientas de variable compleja para coeficientes de series de potencias. Teniendo la función generadora bivariada

$$F(z,t)=\prod_{a\in A}\left(\frac{1}{1-tz^a}\right)$$

Fijemos un $z_0\in\mathbb{D}$ arbitrario. Dado que $A\subseteq\mathbb{Z}^+$, tenemos que $|z_0^a|\leq|z_0|<1$ para todo $a\in A$. Consideremos la función $g(t)=F(z_0,t)$ como una función de la variable compleja t.

Las posibles singularidades de este producto infinito ocurren cuando los denominadores se anulan, es decir, cuando $1-tz_0^a=0$, lo que implicat$=z_0^{-a}$. Dado que $|z_0|<1$, se sigue que $|t|=|z_0|^{-a}>1$. Esto garantiza que, para un z fijo en el disco unitario, la función $t\mapsto F(z,t)$ es analítica en un disco abierto que contiene al disco unitario cerrado del plano t (es decir, $|t|\leq 1$).

Debido a la analiticidad respecto a t, podemos usar la formula integral de Cauchy para los coeficientes de la serie de Taylor. El coeficiente k-ésimo, admitirá entonces la siguiente representación integral

$$[t^k]F(z,t)=\frac{1}{2\pi i}\int_\gamma\frac{F(z,t)}{t^{k+1}}\,dt$$

donde γ es, por ejemplo, el círculo unitario $|t|=1$ recorrido en sentido positivo. Ahora bien, consideremos el integrando $H(z,t)=t^{-(k+1)}F(z,t)$, para concluir que $[t^k]F(z,t)$ es analítica, invocamos el siguiente resultado clásico sobre integrales dependientes de un parámetro (ver [23])

Teorema 2.2.1

Si una función $H(z,t)$ es continua en t a lo largo de un contorno γ y es analitica respecto a z en una región D para cada $t\in\gamma$, entonces la función definida por

$$I(z)=\int_\gamma H(z,t)\,dt$$

es analítica en D.

En nuestro caso

- El camino de integración γ es compacto y fijo (independiente de z).
- Para cada $t\in\gamma$ fijo, el factor $(1-tz^a)^{-1}$ es analítico respecto a z en $\mathbb{D}$, pues el denominador $1-tz^a$ no se anula (ya que $|z|<1$ y $|t|=1$ implican $|tz^a|<1$).
- Como se discutió en las proposiciones anteriores para productos infinitos, la convergencia uniforme sobre compactos de los factores implica que el producto infinito $F(z,t)$ es una función analítica de z en $\mathbb{D}$.

Concluyendo entonces que la función definida, $[t^k]F(z,t)$ es analítica en $\mathbb{D}$. Y dada la convergencia absoluta y uniforme, lo hecho en el **Teorema 1.3.1** es valido, por lo que la función generadora de particiones en k partes

$$P_{k,A}(z)=\sum_{n=0}^{\infty}p_{k,A}(n)z^n=[t^k]\prod_{a\in A}\left(\frac{1}{1-z^a}\right)$$

es analítica en $\mathbb{D}$.

Una vez teniendo a nuestras funciones $R_{k,A}(z)$, $R_A(z)$, $P_{k,A}(z)$ y $P_A(z)$, vistas como funciones analíticas. la formula integral de Cauchy nos garantiza que dado un contorno circular γ centrado en el origen con radio $\rho < 1$:

$$p_{k,A}(n) = \frac{1}{2\pi i}\int_\gamma \frac{P_{k,A}(z)}{z^{n+1}}dz, \quad p_A(n) = \frac{1}{2\pi i}\int_\gamma \frac{P_A(z)}{z^{n+1}}dz$$

y usando 1.2.1 y 1.2.2,

$$r_{k,A}(n) = \frac{1}{2\pi i}\int_\gamma \frac{f_A^k(z)}{z^{n+1}}dz, \quad r_A(n) = \frac{1}{2\pi i}\int_\gamma \frac{f_A(z)}{z^{n+1}(1-f_A(z))}dz$$

Esta idea de generalización del método aplicado por Hardy y Ramanujan fue lo que motivo a Hardy y Littlewood a intentar atacar otros problemas aditivos que tenían años escapando de los métodos convencionales. Uno de ellos fue el llamado **Problema de Waring**.

Hacia el año 1621 Claude Gaspard Bachet de Méziriac en su traducción de la *Arithmetica* de Diofanto, conjeturó que todo entero positivo era suma de cuatro cuadrados, esta conjetura se cree que fue por mera heuristica al comprobar que "parecía" que 4 eran suficientes, sin embargo, nadie lo pudo probar en su época.

Pierre de Fermat afirmó haber probado la conjetura. En una carta a Marin Mersenne (1636) y posteriormente en sus notas sobre la obra de Diofanto, Fermat aseguró tener una demostración usando su método del descenso infinito. Pero como era usual, no existe registro escrito de dicha prueba. Por lo que el problema permaneció abierto.

Sin lugar a dudas la figura mas central en atacar el problema de la suma de cuadrados fue Leonhard Euler, quien construyó casi toda la teoría necesaria para la prueba, aunque no logró su objetivo durante 40 años. En 1751 Euler probó rigurosamente que 3 cuadrados no eran suficientes pues, por ejemplo, probo que los números de la forma $8n + 7$ no podían escribirse como suma de tres cuadrados. Entre los distintos intentos de abordar el problema, Euler descubrió una identidad algebraica que muestra que el producto de dos sumas de cuatro cuadrados es, a su vez, una suma de cuatro cuadrados.

$$(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) = A^2 + B^2 + C^2 + D^2$$

con lo que redujo drásticamente el problema, pues bastaba probar que si todo número primo es suma de 4 cuadrados, entonces la identidad de Euler garantiza que cualquier entero (producto de primos) también lo es. Con este gran paso Euler intentó probar que todo primo p es suma de 4 cuadrados usando descenso infinito, pero no pudo demostrar un paso fundamental.

En años posteriores el problema de la suma de cuadrados se extendió hacia potencias mayores, en 1770 Edward Waring, generaliza la vieja conjetura de Bachet (que llevaba 150 años abierta) en su obra *Meditationes Algebraicae*, afirmo (sin demostración) lo siguiente;

> Todo número entero es un cubo o la suma de dos, tres, ..., nueve cubos; todo entero es también el cuadrado de un cuadrado o la suma de dos, tres, ..., diecinueve de tales números, y así sucesivamente.

Afirmando entonces que todo entero positivo era suma de 9 cubos y de 16 potencias cuartas. Como paso con Bachet, la cantidad de sumandos fueron sobre todo ejemplos numéricos, donde dicha cantidad parecían ser suficientes. Debido a la antigüedad del problema y el gran interés por parte de las grandes mentes de la época a esta conjetura se le conoce hoy en día como **Problema de Waring,** su formulación en notación actual seria la siguiente: Para cada entero $k \geq 2$, se busca determinar si existe un mínimo entero positivo s tal que todo $n \in \mathbb{Z}_{\geq 0}$ pueda expresarse como:

$$n = x_1^k + x_2^k + \cdots + x_s^k$$

con $x_i \in \mathbb{Z}_{\geq 0}$. Es decir, ¿Cuantos sumandos se necesitan para que todo numero se puede ver como la suma de potencias k-esimas? Al numero s necesario se le denota como $g(k)$. Con los avances de Euler se prueba que $g(2) \geq 4$, y se conjeturaba que $g(3) = 9$ y $g(4) = 16$.

Aquí es importante hacer una distinción, el problema de Waring hace alusión a la representabilidad de un entero como suma de potencias k-ésimas permitiendo el uso del cero, es decir, considerando sumandos en $\mathbb{Z}_{\geq 0}$. Esta precisión no es meramente formal, pues influye cuando se fija el número de sumandos. Por ejemplo, el entero 1 puede escribirse como suma de cuatro cuadrados si se admite el cero, ya que $1 = 1^2 + 0^2 + 0^2 + 0^2$, mientras que no es posible expresarlo como suma de cuatro cuadrados positivos, dado que el menor valor que puede tomar una suma de cuatro cuadrados positivos es 4. De igual forma, el entero 7 no puede representarse como suma de tres cuadrados, aun permitiendo ceros (pues es de la forma $8n + 7$); sin embargo, sí admite una representación como suma de cuatro cuadrados, por ejemplo $7 = 2^2 + 1^2 + 1^2 + 1^2$. Estos ejemplos nos dan a notar que la inclusión de 0^kamplía la clase de enteros representables con un número fijo de potencias, distinción que debe tenerse presente en la formulación del problema, aunque no altera su comportamiento asintótico para enteros suficientemente grandes.

Continuando, no tardo mucho en que se lograra un primer avance en este tipo de cuestiones, pues ese mismo año de la formulación del problema de Waring, Lagrange pudo probar que efectivamente, $g(2) = 4$. Su demostración en *Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres* de Berlin se titula "*Démonstration d'un théorème d'arithmétique*", la cual consiste en una prueba por descenso infinito, Lagrange tomó las herramientas desarrolladas por Euler (especialmente la identidad y las propiedades de congruencias) y logró probar el lema que le faltaba a Euler. Curiosamente, tres años después de la prueba de Lagrange, Euler publicó una demostración mucho más simple y directa del teorema, basándose en las ideas de Lagrange pero simplificando el argumento del descenso. Esta es la versión que a menudo se enseña hoy en dia. Más aún dados sus propios trabajos y observaciones, Euler conjeturo que

$$p_{k,A}(n) = \frac{1}{2\pi i}\int_\gamma \frac{P_{k,A}(z)}{z^{n+1}}dz, \quad p_A(n) = \frac{1}{2\pi i}\int_\gamma \frac{P_A(z)}{z^{n+1}}dz$$

$$g(k) = 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2$$

esta afirmación surge de intentar representar el número $n = 2^k \cdot \left\lfloor (3/2)^k \right\rfloor - 1$. Como este número es menor que 3^k, solo puede formarse usando sumas de 1^k y 2^k. Y mediante un argumento de conteo se llega a que se necesitan al menos esa cantidad de sumandos, por lo que

$$g(k) \geq 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2$$

entonces la conjetura de Euler era que la desigualdad, de hecho, era exacta para $k > 2$:

$$g(k) = 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2$$

Sin embargo no había pruebas de casos particulares para verificarlo. Se ha verificado que la fórmula es exacta para valores pequeños de k. Por ejemplo, para $k = 3$, $g(3) = 9$; para $k = 4$, $g(4) = 19$; y para $k = 5$, $g(5) = 37$. Todos estos coinciden con la fórmula de Euler. Históricamente, se ha avanzado significativamente en la verificación de esta conjetura. En 1936, Dickson y Pillai demostraron que la igualdad se mantiene para todo $k \geq 7$, siempre que se cumpla la condición

$$2^k\{(3/2)^k\} + \lfloor (3/2)^k \rfloor \leq 2^k$$

y unos años después en 1957 Kurt Mahler utilizó el teorema de Roth para demostrar que solo existe un número finito de valores de k para los cuales la condición podría fallar. Aunque no se ha encontrado ningún contraejemplo y se ha verificado computacionalmente para una vasta cantidad de valores (confirmando, por ejemplo, que $g(5) = 37$), la prueba de que esta condición se cumple para todo k sigue siendo un problema abierto, estrechamente relacionado con la distribución de las partes fraccionarias de las potencias de $3/2$

El avance hacia el problema de Waring fue lento, pues no hubo avances significativos en los próximos 100 años después de su formulación en 1770. Los matemáticos intentaron generalizar el éxito de Euler y Lagrange mediante identidades algebraicas. La idea era encontrar una identidad que expresara una potencia o un múltiplo de una potencia como suma de potencias menores. En ese sentido, hacia 1859, Liouville logró probar la existencia de $g(4)$ aunque con una cota lejana al valor conjeturado por Waring ($g(4) = 19$). Liouville utilizó una identidad basada en el hecho de que

$$6(x_1^2 + x_2^2 + x_3^2 + x_4^2)^2$$

puede expandirse en términos de cuartas potencias. A través del descenso infinito, probo que

$$g(4) \leq 53$$

Esta cota fue mejorada con el tiempo por otros matemáticos mediante métodos elementales, el valor exacto de 19 permaneció sin prueba hasta hace unos años en 1986 por R. Balasubramanian, F. Dress, y J.-M. Deshouillers.

A principios del siglo XX, se sabia que $g(3)$ existía, fue en 1909 cuando Wieferich publico una prueba de que $g(3) = 9$, sin embargo la prueba contenía un error en un caso particular, el cual fue corregido por A.J. Kempner en 1912. Ese mismo año (1909) Landau probo un equivalente al problema, demostró que para enteros suficientemente grandes, bastaban 8 cubos, es decir, existía un N entero positivo, tal que todo $n > N$ se podía ver como suma de 8 cubos, este resultado nos dice que si nos vamos a números mas grandes, nos serán suficientes 8 cubos en vez de 9.

Hasta 1909 ya se tenían pruebas particulares de existencia del problema de Waring para $k = 2, 3, 4$, sin embargo no se sabia si $g(k)$ existía para todo k. David Hilbert resolvió el problema existencial general en 1909. Hilbert probo que existen racionales positivos r_i y enteros a_{ij} tales que:

$$(x_1^2 + \cdots + x_m^2)^k = \sum_{j=1}^{M} r_j(a_{1j}x_1 + \cdots a_{mj}x_m)^{2k}$$

A partir de identidades de este tipo, utilizo argumentos de convexidad y de geometría de números para demostrar que $g(k) < \infty$. La prueba de Hilbert, en principio, era constructiva, pero las cotas para $g(k)$ eran de inmensa magnitud, por lo cual inútiles para hallar el valor exacto.

El terreno que tenían Hardy y Littlewood era nulo, pues para 1920 los avances en el problema de Waring eran la existencia general, los valores exactos para $k = 2, 3$ y para $k = 4$ la cota dada por Liouville. Por lo que adentrarse en querer atacar el problema de Waring mediante el método del circulo era sin duda una tarea atrevida y revolucionaria, entonces ¿Como abordaron el problema de Waring?

Hardy y Littlewood consideraron el conjunto

$$A_k = \left\{m^k : m \in \mathbb{Z}_{\geq 0}\right\}$$

de modo que el número de representaciones de n como suma de s potencias k-ésimas es $r_{s,A_k}(n)$. A primera vista, esto contrasta con la convención del Capítulo 1, donde los conjuntos A están contenidos en $\mathbb{Z}^+$ y no incluyen el 0. Esta inclusión del cero altera el conteo de soluciones, pues permite sumandos nulos. Para establecer la relación exacta, definamos el conjunto de potencias positivas como:

$$A_k^+ := A_k \setminus \{0\}$$

entonces la función de representación correspondiente satisface

$$f_{A_k}(z) = 1 + f_{A_k^+}(z)$$

y al elevar a la potencia s, y aplicando el Teorema del Binomio, obtenemos

$$f_{A_k}^s(z) = \left(1 + f_{A_k^+}(z)\right)^s = \sum_{j=0}^{s} \binom{s}{j} f_{A_k^+}^j(z)$$

Observamos que para $n \geq 1$, el término constante$j = 0$ no aporta al coeficiente de z^n. Por lo tanto, comparando los coeficientes de z^n a ambos lados, llegamos a la identidad:

$$r_{s,A_k}(n) = \sum_{j=1}^{s} \binom{s}{j} r_{j,A_k^+}(n) = r_{s,A_k^+}(n) + \sum_{j=1}^{s-1} \binom{s}{j} r_{j,A_k^+}(n)$$

Así, la función de representación considerando el cero, $r_{s,A_k}(n)$, engloba a la función sin el cero $r_{s,A_k^+}(n)$ (correspondiente al término $j = s$) más una contribución de representaciones que utilizan menos de s sumandos positivos.

En todo lo siguiente, trabajaremos con el conjunto A_k (admitiendo el cero) por dos razones fundamentales: la primera es que la función generadora del numero de representaciones permanece sin cambios siendo $f^s_{A_k}(z)$ y la segunda para mantener la fidelidad histórica al desarrollo original de Hardy y Littlewood.

Con esto aclarado, la formula integral de Cauchy nos garantiza que

$$r_{s,A_k}(n) = \frac{1}{2\pi i}\int_\gamma \frac{f^s_{A_k}(z)}{z^{n+1}}dz$$

escribiendo $e(\alpha) := \exp(2\pi i\alpha)$ y usando la parametrización del contorno,

$$r_{s,A_k}(n) = \rho^{-n}\int_0^1 f_{A_k}(\rho e(\alpha))^s e(-n\alpha)d\alpha$$

Pero, ¿Qué relación existe entre los valores de $r_{s,A_k}(n)$ y la función $g(k)$? La conexión conceptual es inmediata: por definición, $g(k)$ es el menor entero s tal que todo número natural puede escribirse como suma de s potencias k-ésimas. Por lo tanto, si se demostrara que

$$r_{s,A_k}(n) > 0 \qquad \text{para todo } n \geq 1$$

entonces necesariamente $g(k) \leq s$.

Sin embargo, en la práctica analítica (y también en otros problemas aditivos) esta situación es critica. Frecuentemente ocurre que, para un conjunto cualquiera $A \subseteq \mathbb{Z}^+$, la función de representación $r_{s,A}(n)$ puede anularse para algunos valores pequeños de n, aun cuando para todos los números lo suficientemente grandes se tenga la desigualdad

$$r_{s,A}(n) > 0 \qquad \text{para todo } n \geq N$$

Un ejemplo ilustrativo es considerar el conjunto de impares $\mathscr{A}$ del capitulo anterior, donde probamos que

$$r_{2,\mathscr{A}}(n) = \frac{n}{2}\delta_{\mathbb{Z}}\left(\frac{n}{2}\right) \quad \text{y} \quad r_{3,\mathscr{A}}(n) = T_{(n-1)/2}\delta_{\mathbb{Z}}\left(\frac{n-1}{2}\right)$$

Donde, por ejemplo, para n par $r_{2,\mathscr{A}}(n) = 0$, siendo nulo, de hecho, en una infinidad, mientras que para n impar, $r_{3,\mathscr{A}}(n) > 0$ para $n > 3$. Este tipo de fenómenos, la falta de representaciones para algunos n pequeños pero existencia de representaciones para $n \geq N$, es típico en la teoría aditiva y anticipa la necesidad de distinguir dos problemas: el "problema exacto" y el "problema asintótico".

Aplicado al problema de Waring, si se mostrara que existe un N tal que

$$r_{s,A_k}(n) > 0 \qquad \text{para todo } n \geq N$$

no implicaría que $g(k) = s$, pues podría existir un número pequeño que requiera más de s potencias k-ésimas. Lo que sí garantiza es que todo entero suficientemente grande es suma de s potencias k-ésimas. Por esta razón se introduce la función $G(k)$, definida como el menor entero s tal que $r_{s,A_k}(n) > 0$ para todo n suficientemente grande.

Históricamente, esta distinción apareció de manera natural al observar los límites de los métodos puramente algebraicos del siglo XIX. Pues como habíamos mencionado en 1909, Landau en un trabajo precursor del método del círculo, demostró que la representación por siete cubos posee densidad uno: casi todos los enteros pueden escribirse como suma de siete cubos. Como consecuencia inmediata, probó que todo entero suficientemente grande es suma de ocho cubos, por lo que $G(3) \leq 8$ aunque su resultado era puramente asintótico: no proporcionaba un umbral explícito para el "suficientemente grande".

A pesar del resultado de Landau, valor exacto $g(3) = 9$ (validez para todos los enteros) dependía aún de técnicas más finas y correcciones posteriores. Este contraste entre $g(k)$ y $G(k)$ reflejaba precisamente las limitaciones de los métodos clásicos.

Con esta perspectiva, puede verse que la maquinaria desarrollada por Hardy y Littlewood no apunta directamente a determinar $g(k)$, sino a establecer fórmulas asintóticas para $r_{s,A_k}(n)$ y, con ello, valores precisos de $G(k)$. El método del círculo permite dar una estimación explícita de $r_{s,A_k}(n)$, lo cual conduce naturalmente a demostrar que $r_{s,A_k}(n) > 0$ para todo n suficientemente grande. En otras palabras, la teoría analítica trabaja de manera inherente en el régimen asintótico y, por ello, su impacto más directo se refleja en la determinación de $G(k)$.

Al igual que en el caso de las particiones, Hardy y Littlewood empezaron analizando el comportamiento de

$$\frac{f_{A_k}^s(z)}{z^{n+1}}$$

en el circulo de integración con $\rho \to 1^-$. Podemos notar que la singularidad en $z = 0$ y la potencia s no afectaran en un primer análisis asintótico, es por ello que el interés se vuelca en estudiar el comportamiento de la función $f_{A_k}(z)$ al igual que hicimos con la función generadora de particiones $P(z)$. Sin embargo, podemos notar que sera un caso totalmente distinto, pues la estructura de producto de $P(z)$ presenta singularidades en las raíces de la unidad y que, por ello, la transformación modular de la función eta permite explotar esas singularidades para obtener la estimación asintótica de $p(n)$. Cosa contraria en el caso de la función $f_{A_k}(z)$. A simple vista, el contorno crítico sigue siendo el círculo unidad $|z| = 1$ pues el radio de convergencia es 1. No obstante, la naturaleza de los "puntos singulares" cambia radicalmente. Para entender esto, seremos mas específicos con la función a estudiar en este caso, dada la parametrizacion, nos interesa ver el comportamiento de

$$f_{A_k}(\rho e(\alpha)) = \sum_{m=0}^{\infty} (\rho e(\alpha))^{m^k} = \sum_{m=0}^{\infty} \rho^{m^k} e\left(\alpha m^k\right)$$

para $\alpha \in [0, 1]$. Una forma de interpretar esta suma es imaginar a cada termino como un vector unitario en el plano complejo escalado por un factor de ρ^{m^k} y estudiar como se suman o cancelan dichos vectores. Para ello podemos ver que todo dependerá del valor de α, pues si consideramos

$$\left\{e\left(\alpha m^k\right) : m \in \mathbb{Z}_{\geq 0}\right\}$$

este conjunto sera finito si α es un numero racional.

Proposición 2.2.1

Sea $\alpha \in \mathbb{Q}$ tal que $\alpha = a/q$ con $a \in \mathbb{Z}, q \in \mathbb{Z}^+$ y $(a, q) = 1$. El conjunto $\left\{e\left(\alpha m^k\right) : m \in \mathbb{Z}_{\geq 0}\right\}$ es es un conjunto finito formado por raíces q-ésimas de la unidad.

Demostración. Recordemos que la función $e(x) = \exp(2\pi i x)$ es periódica con "periodo 1", es decir, $e(x) = e(x+n)$ para cualquier entero n. Por lo tanto, el valor de $\phi_m := e\left(\alpha m^k\right)$ depende únicamente de la clase de congruencia del argumento módulo 1. Consideremos el exponente

$$\frac{am^k}{q}$$

sabemos que para todo $m \in \mathbb{Z}_{\geq 0}$ existe un único residuo $r_m \in \{0, 1, \ldots, q-1\}$ tal que $m \equiv r_m \pmod{q}$. Dadas las propiedades de las congruencias, esto implica que

$$am^k \equiv ar_m^k \pmod{q}$$

Entonces podemos escribir el numerador como $am^k = h \cdot q + R_m$, donde R_m es el residuo de ar_m^k modulo q. Sustituyendo obtenemos que

$$\phi_m = e\left(\frac{hq + R_m}{q}\right) = e(h) \cdot e\left(\frac{R_m}{q}\right) = e\left(\frac{R_m}{q}\right)$$

Dado que R_m solo puede tomar valores en el conjunto finito $\{0, 1, \ldots, q-1\}$, concluimos que la sucesión $\{\phi_m\}_{m\geq 0}$ solo toma un conjunto finito de puntos sobre la circunferencia unitaria, específicamente un subconjunto de las raíces q-ésimas de la unidad. □

Este resultado tiene una consecuencia geométrica inmediata en la magnitud de la suma $f_{A_k}(\rho e(\alpha))$.

Cuando α es racional ($\alpha = \frac{a}{q}$), la sucesión de vectores unitarios $e(\alpha n^k)$ es periódica con periodo q. A diferencia de lo que ocurriría con una suma sobre todos los enteros (donde los vectores suelen anularse por simetría), en el caso de las potencias k-ésimas, los residuos de $n^k \pmod{q}$ no se distribuyen uniformemente en las clases de residuos. Los valores tienden a concentrarse en ciertos residuos (los residuos k-ésimos) y a evitar otros.

Por el contrario, si α es irracional (o racional con denominador muy grande), el comportamiento es radicalmente distinto. Geométricamente, los vectores unitarios $e(\alpha n^k)$ recorren densamente el círculo unitario sin presentar periodicidad a corto plazo. Al sumar estos vectores, sus direcciones varían de forma "caótica", apuntando en todas direcciones. Esto da lugar a una interferencia destructiva: los vectores tienden a anularse mutuamente, y aunque la serie diverge, la magnitud resultante crece mucho más lentamente que en el caso racional.

Todo el análisis anterior nos intuye que las partes donde la función crece mas rápido sera en vecindades **muy cercadas a fracciones reducidas**, y es justo esto sera la clave del porque no nos sera útil utilizar la disección de Farey directamente como en el caso de particiones, aunque en un primer momento parecería lo obvio. Esta ineficacia vendrá dada por el tamaño de cada arco en la disección de Farey, pues dada una fracción reducida $\frac{a}{q}$ el intervalo asociado con sus vecinos, en algunos casos puede cubrir mucho espacio en el circulo unitario, siendo que dentro de un intervalo de Farey completo, solo una pequeña vecindad de contribuye significativamente mientras la demás no tiene gran magnitud.

Si intentáramos integrar sobre la disección de Farey estaríamos integrando regiones donde; la suma exponencial es pequeña pero el intervalo es largo, esto provocaría que haya términos de error grandes y se destruya el balance principal/error. En otras palabras, **la disección de Farey es demasiado grande** para capturar el comportamiento analítico en el problema de Waring. Por ello, Hardy y Littlewood utilizaron la disección de Farey como guía estructural, pero definieron arcos más pequeños, centrados en $\frac{a}{q}$, adecuados.

Consideremos la disección de Farey de orden N para cada $\frac{a}{q} \in \mathcal{F}_N$ tendremos los arcos asociados por los intervalos centrados en $\frac{a}{q}$:

$$M_{a,q} = \left[\frac{a_1 + a}{q_1 + q}, \frac{a + a_2}{q + q_2}\right]$$

donde $\frac{a_1}{q_1}, \frac{a_2}{q_2}$ son los respectivos vecinos izquierdo y derecho en $\mathcal{F}_N$. Entonces definiremos a los **Arcos Mayores** como los subintervalos

$$\mathfrak{M}_{a,q} := \left\{\alpha \in [0,1] : \left|\alpha - \frac{a}{q}\right| \leq \eta_q\right\}$$

donde η_q sera suficientemente pequeño tal que $\mathfrak{M}_{a,q} \subset M_{a,q}$. Para discernir cual tamaño sera suficiente recordemos los resultados que vimos en la sección anterior sobre la secuencia de Farey. Tendremos que el "radio" de nuestro intervalo $M_{a,q}$ sera:

$$\frac{a + a_2}{q + q_2} - \frac{a}{q} = \frac{qa_2 - q_2 a}{q(q + q_2)} = \frac{1}{q(q + q_2)}$$

y dado que $N < q + q_2 \leq 2N$, entonces el radio del intervalo estará entre $\frac{1}{2qN}$ y $\frac{1}{qN}$. Por conveniencia (y simetría), Hardy y Littlewood tomaron $\eta_q = \frac{1}{qN}$, garantizando así tres cosas a la vez:

1. Los arcos mayores son no vacíos ($\frac{a}{q} \in \mathfrak{M}_{a,q}$).
2. Están contenidos en los intervalos de Farey ($\mathfrak{M}_{a,q} \subset M_{a,q}$).
3. Son disjuntos salvo, eventualmente, en extremos.

Con ello podemos dar una definición formal. Esta definición, salvo constantes intrascendentes, coincide con la definición original introducida por Hardy y Littlewood en su estudio del problema de Waring

Definición 2.2.1 Arcos Mayores (Problema de Waring)

Para cada $\frac{a}{q} \in \mathcal{F}_N$, se define el arco mayor asociado como

$$\mathfrak{M}_{a,q} := \left\{\alpha \in [0,1] : \left|\alpha - \frac{a}{q}\right| \leq \frac{1}{qN}\right\}, \quad 1 \leq q \leq N$$

Al conjunto de arcos mayores lo denotamos por:

$$\mathfrak{M} = \bigcup_{\substack{1 \leq q \leq N \\ (a,q)=1}} \mathfrak{M}_{a,q}$$

Algo inmediato a notar es que, a diferencia de la disección de Farey, estos intervalos por construcción no forman una partición del intervalo $[0,1]$, pues hay huecos entre ellos. Dichos espacios serán justamente los lugares donde el orden de crecimiento de la función generadora sera menor y es por ello que le denominaremos **Arcos Menores**.

Definición 2.2.2 Arcos Menores (Problema de Waring)

Se definen a los arcos menores como:

$$\mathfrak{m} = [0,1] \setminus \mathfrak{M}$$

En conclusión los arcos mayores son el conjunto de $\alpha \in [0,1]$ tales que tienen una **aproximación racional con denominador pequeño** suficientemente buena, mientras que los arcos menores seran aquellos que no la tienen.

La formalización de esta distinción entre arcos mayores y menores constituyó la modificación crucial de Hardy y Littlewood respecto al enfoque utilizado en particiones, estableciendo así el desarrollo estándar del Método del Círculo. A diferencia de la partición usada en particiones, esta nueva estrategia selecciona geométricamente las regiones de contribución dominante. El siguiente gráfico muestra este refinamiento sobre la disección de Farey clásica:

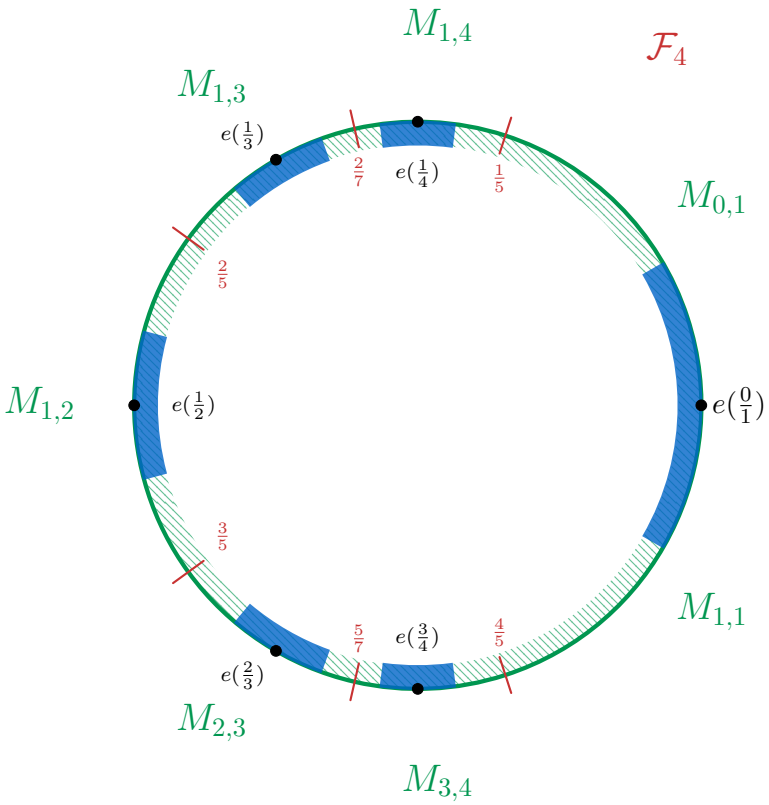

Figura 2.2.1: *Representación geométrica de la disección de Farey de orden* $N = 4$, $\mathcal{F}_4 = \{\frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}\}$ *sobre el círculo unitario. Los sectores verdes representan la disección de Farey* $M_{a,q}$*, los cuales cubren la totalidad de la circunferencia, cada arco de la disección esta separado por las lineas rojas. Superpuestos en azul oscuro se muestran los Arcos Mayores* $\mathfrak{M}_{a,q}$*, centrados en las raíces de la unidad* $e(a/q)$ *y definidos por la condición* $\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{qN}$*. Las regiones verdes no cubiertas por los arcos azules ilustran los arcos menores. La figura pone de manifiesto la contención natural* $\mathfrak{M}_{a,q} \subset M_{a,q}$*. El tamaño de los arcos mayores se ha escalado gráficamente para fines ilustrativos.*

Gracias a esta separación Hardy y Littlewood analizaron la integral en cada arco.

Se toma la disección de Farey de orden N suficientemente grande (Hardy y Littlewood usaron $N \asymp n$), por lo que

$$\begin{aligned} r_{s,A_k}(n) &= \rho^{-n} \int_0^1 f_{A_k}(\rho e(\alpha))^s e(-n\alpha) d\alpha \\ &= \rho^{-n} \int_{\mathfrak{M}} f_{A_k}(\rho e(\alpha))^s e(-n\alpha) d\alpha + \rho^{-n} \int_{\mathfrak{m}} f_{A_k}(\rho e(\alpha))^s e(-n\alpha) d\alpha \end{aligned}$$

Antes de proceder, es pertinente hacer una aclaración notacional. Si bien Hardy y Littlewood no introdujeron explícitamente en sus primeros trabajos la nomenclatura compacta que utilizaremos, su análisis conduce de manera natural a esta descomposición. Es por esto que en lo siguiente, adoptaremos la notación moderna estándar por razones de claridad, manteniendo intacto el argumento original.

Para los arcos mayores, la integral explícitamente se desarrolla como

$$\rho^{-n} \int_{\mathfrak{M}} f_{A_k}(\rho e(\alpha))^s e(-n\alpha) d\alpha = \rho^{-n} \sum_{\substack{1 \le q \le N \\ (a,q)=1}} \int_{\mathfrak{M}_{a,q}} f_{A_k}(\rho e(\alpha))^s e(-n\alpha) d\alpha$$

Como ya discutimos los arcos mayores nos determinaran segmentos donde la contribución de la función generadora es mayor, es por ello que se aprovecha la estructura de estos arcos para poder dar aproximaciones buenas para el integrando. Notemos que para cada $\alpha \in \mathfrak{M}_{a,q}$ existirá $|\beta| \le \frac{1}{qN}$ tal que

$$\alpha = \frac{a}{q} + \beta$$

con ello la suma exponencial se reescribe como

$$f_{A_k}(\rho e(\alpha)) = \sum_{m=0}^{\infty} \rho^{m^k} e\left(\alpha m^k\right) = \sum_{m=0}^{\infty} \rho^{m^k} e\left(\frac{a}{q} m^k\right) e\left(\beta m^k\right)$$

ademas, dado que $\rho \to 1^-$ (con una elección estratégica del radio $\rho = e^{-1/n}$) podemos aproximar dicha suma exponencial por una suma finita, dependiente de un valor X (donde $X = n^{\frac{1}{k}}$), esta aproximación es válida porque la contribución de los términos con $m > X$ es despreciable (o absorbida por el error) debido al decaimiento exponencial ρ^{m^k}:

$$f_{A_k}(\rho e(\alpha)) = \sum_{0 \le m \le X} e\left(\frac{a}{q} m^k\right) e\left(\beta m^k\right) + error$$

El punto clave es que la dependencia en $\frac{a}{q}$ puede separarse de la dependencia en β. Agrupando los términos modulo q, Hardy y Littlewood muestran que

$$f_{A_k}(\rho e(\alpha)) = \frac{1}{q} S(a,q) I(\beta) + O(q)$$

donde $S(q,a)$ es una suma de Gauss generalizada sobre el modulo q definida por:

$$S(a,q) = \sum_{r=1}^{q} e\left(\frac{a r^k}{q}\right)$$

e $I(\beta)$ es una integral oscilatoria que refleja la contribución del parámetro β.

$$I(\beta) = \int_0^X e(\beta x^k)dx$$

El termino de error es pequeño de forma uniforme en cada arco mayor, gracias a los resultados sobre sumas exponenciales (ver Apéndice A).

Al elevar a la potencia s, obtenemos

$$f_{A_k}(\rho e(\alpha))^s = \frac{1}{q^s}S(a,q)^s I(\beta)^s + error$$

sustituyendo en la integral sobre los arcos mayores e integrar respecto a β, se obtiene una contribución principal de la forma

$$\rho^{-n} \sum_{\substack{1\leq q\leq N \\ (a,q)=1}} \frac{S(a,q)^s}{q^s} e\left(-\frac{an}{q}\right) \int_{-\frac{1}{qN}}^{\frac{1}{qN}} I(\beta)^s e(-n\beta)d\beta$$

Al tomar el límite $\rho \to 1^-$, la contribución principal proviene de la singularidad de la función generadora en el punto $z = 1$. Hardy y Littlewood demostraron que el comportamiento asintótico en los arcos mayores está gobernado por el producto de un factor aritmético y un factor analítico que depende de la función Gamma.

$$\rho^{-n} \int_{\mathfrak{M}} f_{A_k}(\rho e(\alpha))^s e(-n\alpha)d\alpha \sim \mathfrak{G}_{k,s}(n)\mathfrak{J}_{k,s}(n)$$

donde:

- Se tiene un **factor aritmético**, o denominada **serie singular**. La convergencia y positividad de esta serie son cruciales para garantizar la existencia de soluciones, dependiendo del tamaño de s;

$$\mathfrak{G}_{k,s}(n) = \sum_{q=1}^{\infty} \sum_{\substack{1\leq a\leq q \\ (a,q)=1}} \frac{S(a,q)^s}{q^s} e\left(-\frac{an}{q}\right)$$

- El **factor analítico**. Refleja la densidad de soluciones y surge de la evaluación asintótica de la singularidad de la función generadora. Hardy y Littlewood calcularon este valor explícitamente en términos de la función Gamma:

$$\mathfrak{J}_{k,s}(n) = \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)} n^{\frac{s}{k}-1}$$

En conclusión, el análisis sobre los arcos mayores establece la fórmula asintótica principal de Hardy-Littlewood, válida siempre que el número de variables s sea suficientemente grande para controlar el término de error proveniente de los arcos menores. Es por esto que lo siguiente hecho por Hardy y Littlewood fue demostrar que la contribución proveniente de los arcos menores es de orden estrictamente inferior al término principal.

$$\rho^{-n} \int_{\mathfrak{m}} f_{A_k}(\rho e(\alpha))^s e(-n\alpha)d\alpha$$

Este paso es esencial para justificar que la fórmula asintótica que obtuvieron a partir de los arcos mayores describe correctamente el comportamiento de la función de representaciones.

Recordemos que los arcos menores se definen como el complemento de los arcos mayores,

$$\mathfrak{m} = [0,1] \setminus \mathfrak{M}$$

y corresponden a aquellos valores de α que no admiten una aproximación racional suficientemente buena con denominador pequeño.

Con ello sea $\alpha \in \mathfrak{m}$, por la aproximación de Dirichlet (**Lema A.0.3**), existen enteros a, q con $(a,q) = 1$ tales que

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}$$

sin embargo, como α esta en los arcos menores, necesariamente se tiene que $q > Q$, pues de lo contrario α estaría contenido en algún intervalo $\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{qQ}$ asociado a un arco mayor. Esta observación me dice que en los arcos menores, toda aproximación racional relevante involucra denominadores grandes y, como habíamos mencionado, las sumas exponenciales involucradas presentaran grandes cancelaciones. El control inicial de las sumas exponenciales en los arcos menores descansa en el Lema de Weyl (**Lema A.0.2**), que vincula el tamaño de la suma con la calidad de la aproximación racional de α, proporcionando la cota (usando la estimación finita)

$$|f_{A_k}(\rho e(\alpha))| \ll \left|\sum_{1 \leq m \leq X} e\left(\alpha m^k\right)\right| \ll X^{1-\sigma}, \quad \sigma = \frac{1}{2^{k-1}} \tag{2.2.1}$$

uniformemente para $\alpha \in \mathfrak{m}$. Esta es la estimación utilizada en el trabajo original de Hardy y Littlewood; versiones mas modernas refinan el valor de σ, pero no son necesarias en el resultado clásico.

Con lo anterior Hardy y Littlewood estimaron la contribución total de los arcos menores, siendo que

$$\left|\rho^{-n} \int_{\mathfrak{m}} f_{A_k}(\rho e(\alpha))^s e(-n\alpha) d\alpha\right| \ll \int_{\mathfrak{m}} |f_{A_k}(\rho e(\alpha))|^s \, d\alpha$$

aplicando la desigualdad de Hölder para separar la integral en dos factores, utilizando el exponente 2^k y aprovechar la estimación de 2.2.1

$$\begin{aligned}\int_{\mathfrak{m}} |f_{A_k}(\rho e(\alpha))|^s \, d\alpha &\leq \left(\sup_{\alpha \in \mathfrak{m}} |f_{A_k}(\rho e(\alpha))|\right)^{s-2^k} \int_0^1 |f_{A_k}(\rho e(\alpha))|^{2^k} \, d\alpha \\ &\ll X^{(s-2^k)(1-\sigma)} \left(\int_0^1 |f_{A_k}(e(\alpha))|^{2^k} \, d\alpha\right)\end{aligned}$$

y usando el Lema de Hua (**Lema A.0.6**) para estimar el valor de la segunda integral faltante, se obtiene

$$\int_{\mathfrak{m}} |f_{A_k}(\rho e(\alpha))|^s \, d\alpha \ll X^{(s-2^k)(1-\sigma)} X^{2^k - k + \varepsilon} = X^{s-k-\nabla}$$

donde, $\nabla = \sigma(s - 2^k) + \varepsilon$. Para que la contribución de los arcos menores sea despreciable frente al termino principal obtenido en los arcos mayores, cuyo orden es X^{s-k}, es necesario y suficiente que $\nabla > 0$. Esto conduce a la condición moderna sobre el numero de variables:

$$s > 2^k$$

Es de importancia tener que realizar una aclaración histórica y técnica respecto a la condición $s > 2^k$. En la literatura clásica introductoria, es frecuente encontrar la condición más débil (y más exigente en número de variables) $s > 2k(k+1)$ o similares de orden cuadrático $O(k^2)$. Esta diferencia surge de la elección del método de aproximación sobre los arcos menores.

La cota **clásica** (dada por Hardy y Littlewood) $s > 2k(k+1)$ se obtiene si, en lugar del Lema de Hua para la potencia 2^k, se utilizan estimaciones más elementales a un exponente menor (como la potencia $2k$), cargando así todo el peso de la demostración en la desigualdad de Weyl. Al depender exclusivamente de la cota del supremo, se desperdicia la información sobre la cancelación promedio, requiriendo un número innecesariamente alto de variables para compensarlo. La cota moderna $s > 2^k$, presentada aquí, es significativamente más eficiente para valores pequeños de k (los de mayor interés histórico como $k = 3, 4$). Al emplear el exponente 2^k, el Lema de Hua captura la estructura global de la integral, permitiendo relajar la cantidad de variables. Sin embargo, en tiempos actuales, las técnicas desarrolladas por Iván Vinográdov superan a ambas aproximaciones, reduciendo la exigencia a $s \sim k \log k$. Aun así, en el contexto de lo realizado por Hardy y Littlewood, la condición derivada mediante el Lema de Hua representa "lo que es suficiente".

Con la hipótesis impuesta de $s > 2^k$ (o $s > 2k(k+1)$ originalmente), la integral sobre los arcos menores satisface (cuando $n \to \infty$)

$$\rho^{-n} \int_{\mathfrak{m}} f_{A_k}(\rho e(\alpha))^s e(-n\alpha) d\alpha = o(X^{s-k})$$

con ello, se concluye que para s suficientemente grande la contribución principal a

$$r_{s,A_k}(n) = \rho^{-n} \int_0^1 f_{A_k}(\rho e(\alpha))^s e(-n\alpha) d\alpha$$

proviene exclusivamente de los arcos mayores. En consecuencia, se obtiene la formula asintótica de Hardy-Littlewood

$$\boxed{r_{s,A_k}(n) \sim \mathfrak{G}_{k,s}(n)\mathfrak{J}_{k,s}(n)}$$

Remplazando el valor $\mathfrak{J}_{k,s}(n)$, se da así con la formula asintótica mas reconocida

$$r_{s,A_k}(n) \sim \frac{\Gamma(1+\frac{1}{k})^s}{\Gamma(\frac{s}{k})} n^{\frac{s}{k}-1} \mathfrak{G}_{k,s}(n) \tag{2.2.2}$$

La formula asintótica 2.2.2, como mencionamos en un inicio, permite extraer consecuencias inmediatas al problema de Waring. Hardy y Littlewood probaron existe una constante $C > 0$ tal que la serie singular $S_{k,s}(n) > C$ para todo n, siempre que se satisfagan condiciones de congruencia (lo cual queda garantizado si $s > 4k$). Dado que el factor $n^{\frac{s}{k}-1}$ tiende a infinito para $s > k$, se deduce que

$$r_{s,A_k}(n) \to \infty \quad \text{cuando } n \to \infty$$

En particular esto nos dice que existe un $N > 0$ tal que $r_{s,A_k}(n) > 0$ para todo $n > N$. Por definición de $G(k)$, esto implica la cota inferior

$$G(k) \leq s$$

Para poder notar el poder de este resultado examinemos lo que nos dice sobre la distribución de representaciones para los casos clásicos antes del desarrollo de Hardy y Littlewood.

Como se discutió en la introducción histórica del problema de Waring, se conocía que $g(3) = 9$ (Wieferich, 1909) y que $G(3) \leq 8$ (Landau, 1909). Veamos lo que predice la formula asintótica bajo la condición moderna de suficiencia $s > 2^k$.

Para $k = 3$, la condición $s > 2^3 = 8$ sugiere tomar $s = 9$. Sustituyendo estos valores en la formula asintótica, obtenemos que el numero de formas de escribir un entero grande como suma de 9 cubos crece como:

$$r_{9,A_3}(n) \sim \frac{\Gamma(\frac{4}{3})^9}{\Gamma(3)} n^{\frac{9}{3}-1} \mathfrak{G}_{3,9}(n) = Cn^2 \mathfrak{G}_{3,9}(n)$$

por lo que el numero de representaciones crece de forma cuadrática. Y dado que $\mathfrak{G}_{3,9}(n)$ es una función acotada inferiormente por una constante positiva, tenemos la certeza de que $r_{9,A_3}(n) \to \infty$, por lo que se concluye que $G(3) \leq 9$. Sin embargo, refinamientos posteriores al método del circulo (usando sumas de Vinográdov) permiten reducir el numero de variable necesarias para el problema asintótico hasta $s = 7$ ($G(3) \leq 7$), lo cual es consistente con el resultado de Landau de que 8 cubos son suficientes para todo n grande.

Para el caso de potencias cuartas el constraste es aun mayor. Sabemos por el trabajo de Lioville que $g(4) \leq 53$, una cota que fue mejorada paulatinamente hasta probarse que $g(4) = 19$ en 1986. Nuestra condición suficiente $s > 2^4 = 16$ nos intuye a considerar $s = 17$. La formula asintótica predice que

$$r_{17,A_4}(n) \sim \frac{\Gamma(\frac{5}{4})^{17}}{\Gamma(\frac{17}{4})} n^{\frac{17}{4}-1} \mathfrak{G}_{4,17}(n) = Cn^{3.25} \mathfrak{G}_{4,17}(n)$$

garantizando que, asintoticamente, 17 cuartas potencias son mas que suficiente para representar cualquier entero grande, es decir, $G(4) \leq 17$. Esto demuestra la eficiencia del Método del Circulo frente a los métodos algebraicos clásicos. Mientras que Liouville requirió identidades complejas para llegar a 53 variables, el análisis de Hardy y Littlewood muestra directamente que con aproximadamente 17 variables, el numero de soluciones no solo existe, sino que tiende a infinito rápidamente.

En resumen, la fórmula asintótica de Hardy y Littlewood no solo confirma la existencia de soluciones (resolviendo el Problema de Waring), sino que cuantifica la "abundancia" de estas representaciones problema crucial en la combinatoria como bien habíamos mencionado. Nos revela que, una vez superado el umbral de variables impuesto por la geometría de los arcos menores, el número de soluciones explota polinomialmente, validando las intuiciones de Euler y Lagrange desde una perspectiva puramente analítica.

Para concluir el análisis del método de Hardy y Littlewood clásico, es importante realizar una pausa reflexiva sobre las herramientas combinatorias elegidas. En la Sección 2.1 estudiamos las particiones $p(n)$ con la formulación original de Hardy y Ramanujan, donde el objeto central fue la **función generadora de particiones** (con $A = \mathbb{Z}^+$)

$$P_A(z) = \sum_{n=0}^{\infty} p_A(n) z^n = \prod_{a \in A} (1 - z^a)^{-1}$$

Sin embargo, en esta sección, siguiendo a Hardy y Littlewood, hemos trabajado exclusivamente con la **función generadora de representaciones** (con $A = A_k$)

$$R_{k,A}(z) = \sum_{n=0}^{\infty} r_{k,A}(n) z^n = f_A^k(z), \quad f_A(z) = \sum_{a \in A} z^a$$

¿Porque se hizo esto? El paso "natural", de acuerdo a lo hecho por Hardy y Ramanujan en el caso de particiones de enteros, seria considerar también la función generadora de particiones de potencias para el problema de Waring, sin embargo esto no fue hecho así por Hardy y Littlewood. Este cambio no es meramente notacional ni histórico, sino estructural. El objetivo final de esta sección es explicar con precisión por qué el Método del Círculo moderno se formula casi exclusivamente en términos de funciones generadoras de representaciones, y por qué el caso de las particiones constituye una excepción profunda pero aislada.

Dado lo hecho al inicio de esta sección, sabemos que las funciones generadoras para el numero de representaciones vienen dadas por

$$R_{k,A}(z) = \sum_{n=0}^{\infty} r_{k,A}(n) z^n = f_A^k(z) \quad \text{y} \quad R_A(z) = \sum_{n=0}^{\infty} r_A(n) z^n = \frac{f_A(z)}{1 - f_A(z)}$$

de donde

$$r_{k,A}(n) = \frac{1}{2\pi i} \int_\gamma \frac{f_A^k(z)}{z^{n+1}} dz, \quad r_A(n) = \frac{1}{2\pi i} \int_\gamma \frac{f_A(z)}{z^{n+1}(1 - f_A(z))} dz$$

lo que reduce el problema analítico al estudio de una potencia finita de la función de representación

$$f_A(z) = \sum_{a \in A} z^a$$

Este objeto posee una estructura analítica relativamente simple: es analitica en el disco unitario y, cuando A es suficientemente denso, presenta un comportamiento controlado cerca de $z = 1$. Ademas también presentara puntos de mayor cancelación en las raíces de la unidad, el análisis local de $f_A^k(z)$ cerca de raíces de la unidad puede realizarse mediante aproximaciones racionales y sumas exponenciales del tipo

$$S_A(h, q) = \sum_{a \in A} e\left(\frac{ha}{q}\right)$$

lo que encaja de manera natural con la distinción de arcos mayores y arcos menores. El método del círculo moderno se apoya crucialmente en la posibilidad de demostrar que la contribución de los arcos menores es asintóticamente despreciable respecto a los arcos mayores. Para funciones del tipo $f_A^k(z)$, esto se logra mediante estimaciones de Weyl, Vinogradov o versiones refinadas de estos, que proporcionan cancelación efectiva en las sumas exponenciales asociadas. Para la función de particiones, este mecanismo falla de manera fundamental.

La función generadora de particiones dada por

$$P_A(z) = \prod_{a \in A} (1 - z^a)^{-1}$$

es un **producto infinito**, cuya estructura analítica es mucho más rígida y difícil de controlar. Incluso en el caso clásico con $A = \mathbb{Z}^+$, la función $P(z)$ presenta:

- Singularidades acumuladas en todas las raíces de la unidad.
- Una frontera natural en el disco unitario.

y lo mas importante, puede llegar a presentar un **crecimiento explosivo** cerca de las raíces de la unidad. Retomando el ejemplo $A = \mathbb{Z}^+$, tomando $z = e^{-t}$,

$$\log P(e^{-t}) = \sum_{n=1}^{\infty} -\log\left(1 - e^{-nt}\right) \sim \int_0^{\infty} -\log\left(1 - e^{-tx}\right) dx$$

haciendo el cambio de variable $u = tx$, de donde $dx = \frac{du}{t}$, se llega a

$$\begin{aligned}\log P(e^{-t}) &\sim \frac{1}{t}\int_0^{\infty} -\log\left(1 - e^{-u}\right) du = \frac{1}{t}\int_0^{\infty} \sum_{k=1}^{\infty} \frac{e^{-ku}}{k} du \\ &= \frac{1}{t}\sum_{k=1}^{\infty} \frac{1}{k}\int_0^{\infty} e^{-ku} du = \frac{1}{t}\sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{1}{t}\zeta(2)\end{aligned}$$

por lo que

$$P(e^{-t}) \asymp \exp\left(\frac{\pi^2}{6t}\right),\ t \to 0^+$$

este crecimiento impide obtener cancelación suficiente fuera de los arcos mayores, lo que hace inviable una descomposición eficaz del círculo unitario.

Este comportamiento vendrá totalmente determinado por el conjunto A, pues en general para

$$P_A(z) = \prod_{a \in A} (1 - z^a)^{-1}$$

tomando $z = e^{-t}$, llegamos a

$$\log P_A(e^{-t}) = \sum_{a \in A} -\log\left(1 - e^{-at}\right)$$

podemos reescribir esta suma rigurosamente usando una integral de Riemann-Stieltjes:

$$\log P_A(e^{-t}) = \int_0^{\infty} -\log\left(1 - e^{-tx}\right) d\pi_A(x)$$

donde $\pi_A(x)$ es la función contadora de A definida en el capitulo 1

$$\pi_A(x) = \sum_{\substack{n \leq x \\ n \in A}} 1$$

Usando integración por partes llegamos a

$$\log P_A(e^{-t}) = \left[-\pi_A(x)\log\left(1 - e^{-tx}\right)\right]_0^{\infty} + \int_0^{\infty} \pi_A(x) \frac{te^{-tx}}{1 - e^{-tx}} dx$$

aquí, como $A \subseteq \mathbb{Z}^+$ infinito, $\pi_A(x) \leq \pi_{\mathbb{Z}^+}(x) = \lfloor x \rfloor$ y $\pi_A(x) \to 0$ cuando $x \to 0^+$, se tiene

$$\log P_A(e^{-t}) = t\int_0^\infty \frac{\pi_A(x)}{e^{tx}-1}dx$$

por lo que una aproximación asintótica dependerá de que la función contadora $\pi_A(x)$ se comporte asintóticamente como una función suave y bien comportada. En el caso del problema Waring (que en este contexto serian las particiones totales de enteros como suma de k-esimas potencias), al considerar $A_k = \left\{m^k : m \in \mathbb{Z}_{\geq 0}\right\}$, tendremos

$$\pi_{A_k}(x) = \sum_{0\leq n^k \leq x} 1 = \sum_{0\leq n\leq \sqrt[k]{x}} 1 = \left\lceil \sqrt[k]{x} \right\rceil \sim x^{\frac{1}{k}}$$

de forma que

$$\log P_{A_k}(e^{-t}) = t\int_0^\infty \frac{\pi_{A_k}(x)}{e^{tx}-1}dx \sim t\int_0^\infty \frac{x^{\frac{1}{k}}}{e^{tx}-1}dx$$

tomando $u = xt$

$$\log P_{A_k}(e^{-t}) \sim t^{-\frac{1}{k}}\int_0^\infty \frac{u^{\frac{1}{k}}}{e^{u}-1}du$$

y recordando el resultado clásico, para $\mathrm{Re}(s) > 1$

$$\Gamma(s)\zeta(s) = \int_0^\infty \frac{u^{s-1}}{e^{u}-1}du$$

identificando los exponentes llegamos a que

$$\log P_{A_k}(e^{-t}) \sim t^{-\frac{1}{k}}\Gamma\left(1+\frac{1}{k}\right)\zeta\left(1+\frac{1}{k}\right)$$

teniendo un crecimiento exponencial de la forma

$$P_{A_k}(e^{-t}) \asymp \exp\left(t^{-\frac{1}{k}}\Gamma\left(1+\frac{1}{k}\right)\zeta\left(1+\frac{1}{k}\right)\right)$$

De forma mas general si $\pi_A(x) \sim Cx^\alpha$ cuando $x \to \infty$ (con $\alpha > 0$), entonces siguiendo el mismo procedimiento (con su debida justificación) llegamos a que

$$\log P_A(e^{-t}) \sim \frac{C}{t^\alpha}\Gamma(\alpha+1)\zeta(\alpha+1)$$

Sin embargo no todos los conjuntos A tienen este comportamiento, un ejemplo bien conocido el resultante del **Teorema de los Números Primos** el cual afirma que

$$\pi_{\mathbb{P}}(x) \sim \frac{x}{\log x}$$

esto nos hace cuestionarnos ¿Cuando una aproximación de $\pi_A(x)$ no sera suficiente? Si A es un conjunto arbitrario, pueden ocurrir dos cosas que rompen la aproximación:

1. **Crecimiento muy rápido**: Si $A = \{2^n : n \in \mathbb{Z}^+\}$, entonces $\pi_A(x) \sim \log_2(x)$. La densidad decae exponencialmente. La singularidad en $t = 0$ de la integral es mucho más suave (a veces ni siquiera es una singularidad del mismo tipo), por lo que la integral "estándar" sobreestimaria el valor final..

2. **Distribución irregular:** Si A tiene grandes "huecos" seguidos de agrupamientos densos de numeros, el límite asintótico de $\pi_A(x)/x^\alpha$ podría no existir (podría oscilar). En ese caso, la suma no se comporta como la integral de una función suave.

El problema de poder dar una buena estimación al crecimiento de la función generadora de particiones $P_A(z)$ fue estudiado y trabajado por **Günter Meinardus** en su articulo de 1954 titulado "*Asymptotische Aussagen über Partitionen*" [24] que con la notación de este documento se centra en el estudio de dar estimaciones para $P_A(z)$ mediante el uso de series de Dirichlet, para controlar su crecimiento

Definición 2.2.3

Sea $A \subseteq \mathbb{Z}^+$ infinito. Entonces se define a la **serie de Dirichlet asociada al conjunto** A como;

$$D_A(s) = \sum_{a\in A} \frac{1}{a^s} = \sum_{n=1}^{\infty} \frac{\delta_A(n)}{n^s} \quad \text{con } s \in \mathbb{C}$$

Meinardus estableció las condiciones exactas para obtener la asintótica de $P_A(e^{-t})$ a partir de exigir condiciones técnicas rigurosas de $D_A(s)$ sobre analiticidad y crecimiento:

1. **Analiticidad y Polos**: La serie $D_A(s)$ converge para $\mathrm{Re}(s) > \alpha > 0$ y puede extenderse analíticamente a una región $\mathrm{Re}(s) \geq -C_0$ (con $0 < C_0 < 1$). En esta región, $D_A(s)$ debe ser analitica excepto por un polo simple en $s = \alpha$ con residuo K.

2. **Acotación Vertical**: Escribiendo $s = \sigma + it$, existe una constante $C_1 > 0$ tal que para σ fijo y $|t|$ suficientemente grande en la región extendida:

   $$|D_A(s)| \leq C_1|t|^{C_2}$$

   Esto asegura que la función no crezca demasiado rápido en la dirección imaginaria, permitiendo el control de integrales de contorno.

3. **Condición Aritmética:** Esta condición es sutil y asegura que la singularidad en $z = \alpha$ sea dominante y no existan otras singularidades de igual peso en el círculo unitario (evitando el fenómeno de los "arcos menores" destructivos en el Método del Círculo).

Bajo estas condiciones, Meinardus probó que el crecimiento asintótico es:

$$\log P_A(e^{-t}) \sim K\Gamma(\alpha)\zeta(\alpha+1)t^{-\alpha}$$

Mas aun, utilizando el **Método del Punto de Silla**, sobre la transformada de Mellin inversa de la función generadora logro obtener una formula asintotica para el numero de particiones $p_A(n)$

Teorema 2.2.2 (Meinardus-1937)

El número de particiones $p_A(n)$ tiene la formula asintotica:

$$p_A(n) \sim C \cdot n^{\kappa} \cdot \exp\left(L \cdot n^{\frac{\alpha}{\alpha+1}}\right)$$

donde

- *El exponente principal:*

$$L = \left(1 + \frac{1}{\alpha}\right) [K\Gamma(\alpha+1)\zeta(\alpha+1)]^{\frac{1}{\alpha+1}}$$

- *El exponente polinomial:*

$$\kappa = \frac{D_A(0) - 1 - \frac{\alpha}{2}}{\alpha+1}$$

- *La constante multiplicativa:*

$$C = e^{D'_A(0)} \cdot [2\pi(\alpha+1)]^{-\frac{1}{2}} \cdot [K\Gamma(\alpha+1)\zeta(\alpha+1)]^{\frac{1-2D_A(0)}{2(\alpha+1)}}$$

Es importante notar que el cálculo de las constantes C y κ requiere evaluar $D_A(0)$ y $D'_A(0)$. En muchos casos de interés (como caracteres de Dirichlet o formas modulares), estos valores son calculables, lo que hace al teorema extremadamente práctico para obtener asintóticas explícitas sin recurrir a desigualdades elementales menos precisas. El teorema de Meinardus sigue siendo la herramienta estándar para asintóticas de particiones, aunque versiones más modernas (desarrolladas por Andrew Granville y R. C. Vaughan) han relajado algunas condiciones sobre las hipótesis de la serie de Dirichlet asociada.

El gran logro de Meinardus fue convertir al Método del Circulo en un teorema abstracto reutilizable sin embargo es preciso aclarar que funciona si y solo si la serie de Dirichlet asociada $D_A(s)$ tiene buenas propiedades analíticas (continuación analítica, polos controlados y crecimiento acotado en franjas verticales), por lo que no es un teorema general sobre cualquier conjunto A, pero si cubre varios conjuntos con densidad regular, como los enteros $\mathbb{Z}^+$, progresiones aritméticas, potencias k-ésimas (n^k) o números primos. Y se mantiene al margen de conjuntos mas "irregulares" como el ejemplo ya dado donde $A = \{2^n : n \in \mathbb{Z}^+\}$, pues en tal caso la serie de Dirichlet es $\sum 2^{-ks}$, que es muy distinta a una función zeta clásica. La asintótica aquí es de tipo $\log p_A(n) \sim C(\log n)^2$, lo cual no encaja en la forma e^{n^α} de Meinardus. Para estos casos se requieren métodos mas especializados.

Otra restricción técnica más fuerte se aplica a la frontera del disco unitario, pues el teorema de Meinardus exige que la función generadora no tenga singularidades "fuertes" en el círculo unitario fuera de $z = 1$ (o $t = 0$). Si el conjunto A tiene una estructura aritmética tal que existen otras raíces de la unidad donde la función generadora explota con fuerza comparable a la principal, el método del punto de silla estándar falla o requiere modificaciones masivas.

En resumen, el crecimiento explosivo de $P_A(z)$ dependiente de cada conjunto A necesita un análisis especifico en cada caso, por lo que no es aplicable el mismo análisis hecho para particiones de enteros.

Otro motivo por el cual Hardy y Ramanujan lograron aplicar el método del círculo a las particiones de enteros es la existencia de una estructura modular extraordinaria. Como vimos en la sección 2.1,

$$F(e^{2\pi i\tau}) = \frac{e^{\pi i\tau/12}}{\eta(\tau)}$$

donde $\eta(\tau)$ es la función eta de Dedekind, que satisface profundas ecuaciones funcionales modulares. Estas simetrías permiten trasladar el análisis desde el borde del disco unidad hacia regiones donde la función es controlable. Sin embargo, esta estructura modular es exclusiva del caso $A = \mathbb{Z}^+$. Para conjuntos generales A, no existe un análogo de la función eta ni transformaciones modulares que compensen el crecimiento del producto infinito. Por esta razón, el trabajo de Hardy y Ramanujan debe entenderse como un caso excepcional, no como un modelo generalizable.

Si nos reducimos al caso de partes fijas, podríamos creer que sí podría aplicarse indirectamente el método del circulo. Para particiones en un número fijo de partes, la función generadora puede expresarse en términos finitos de $f_A(z)$. Como vimos:

$$P_{2,A}(z) = \frac{1}{2}\left(f_A^2(z) + f_A(z^2)\right)$$

$$P_{3,A}(z) = \frac{1}{6}\left(f_A^3(z) + 3f_A(z)f_A(z^2) + 2f_A(z^3)\right)$$

donde aplicando la formula integral de Cauchy obtendremos que

$$p_{2,A}(n) = \frac{1}{2\pi i}\int_\gamma \frac{\frac{1}{2}\left(f_A^2(z) + f_A(z^2)\right)}{z^{n+1}}dz$$

$$p_{3,A}(n) = \frac{1}{2\pi i}\int_\gamma \frac{\frac{1}{6}\left(f_A^3(z) + 3f_A(z)f_A(z^2) + 2f_A(z^3)\right)}{z^{n+1}}dz$$

si bien en un inicio podría parecer factible, ya que aparecen términos de la forma $f_A^k(z)f_A(z^m)$, justamente esto es lo que hará que el manejo de las singularidades (o puntos de mayor crecimiento) sea en extremo cuidadoso, pues por cada raíz de la unidad, cada raíz m-esima de si misma también se vuelve una singularidad o punto importante de crecimiento debido al factor $f_A(z^m)$, por lo que el análisis correcto de las zonas de mayor crecimiento se vuelve inmanejable para casos grandes. En consecuencia, salvo para k muy pequeño ($k = 2$), el problema vuelve a presentar las mismas dificultades estructurales que el caso general de particiones.

De todo lo anterior se desprende que el método del círculo moderno se formula de manera natural sobre funciones generadoras de representaciones

$$R_{k,A}(z) = f_A^k(z)$$

ya que estas presentan:

- Una estructura analítica controlable.
- Posibilidad de análisis local mediante estimaciones tipo Weyl y Vinogradov

- Cancelación efectiva en los arcos menores.
- Singularidades simples y aisladas.

En contraste, las funciones generadoras de particiones introducen productos infinitos, singularidades acumuladas y crecimiento exponencial incompatible con la descomposición del círculo, salvo en el caso excepcional de particiones de enteros hecha por Hardy y Ramanujan.

Una vez descartado el uso de las funciones generadoras de particiones aun queda una duda pendiente. **¿Que pasa con el numero de representaciones totales $r_A(n)$?** Recordemos que la función generadora de las representaciones totales viene dada por

$$R_A(z) = \sum_{n=0}^{\infty} r_A(n) z^n = \frac{f_A(z)}{1 - f_A(z)}$$

A diferencia de la función $R_{k,A}(z) = f_A^k(z)$ la cual es analítica en $\mathbb{D}$, tenemos que la función generadora $R_A(z)$ es analítica únicamente en el subconjunto de $\mathbb{D}$ donde $f_A(z) \neq 1$. En particular, si existe $r \in (0,1)$ tal que $f_A(r) = 1$, entonces $R_A(z)$ presenta una singularidad en $z = r$, que sera dominante en el comportamiento de la función. Al extraer coeficientes mediante la fórmula de Cauchy,

$$r_A(n) = \frac{1}{2\pi i} \int_\gamma \frac{f_A(z)}{z^{n+1}(1 - f_A(z))} dz$$

el comportamiento asintótico estará gobernado principalmente por la singularidad más cercana al origen, no por oscilaciones locales en el argumento de z cerca de la frontera. En consecuencia:

- La descomposición en arcos mayores y menores pierde sentido.
- La contribución dominante ya no proviene racionales con denominador pequeño.
- El problema deja de ser esencialmente oscilatorio y pasa a ser uno de análisis de singularidades.

por lo que aplicar el método del circulo clásico no aporta información relevante al problema. Y es necesario hacer un análisis distinto.

Otra forma de verlo, seria tratar de considerar que

$$r_A(n) = \sum_{k=1}^{n} r_{k,A}(n)$$

aunque esta identidad es formalmente correcta, resulta asintóticamente inútil en general, porque

- El valor de k que contribuye de forma dominante puede crecer con n.
- Las asintóticas disponibles para $r_{k,A}(n)$ suelen ser válidas solo para k fijo y no de manera uniforme en k.
- No existe una única escala dominante: contribuyen representaciones con un numero de partes distintas.

En resumen, en la teoría aditiva aparecen dos marcos conceptualmente distintos, determinados por la manera en que se fija (o no) el número de partes en las representaciones de un entero.

Por un lado, se encuentran las representaciones con un número fijo de partes, que constituyen el dominio natural del método del círculo, desarrollado por Hardy y Littlewood. En este marco, el análisis se basa en el estudio de sumas exponenciales asociadas a potencias finitas de la función de representación, y el fenómeno fundamental es estudiar las oscilaciones en las aportaciones cerca de la frontera del disco unitario. La descomposición del círculo unitario en arcos mayores y arcos menores permite aislar el término principal, proveniente de aproximaciones racionales con denominadores pequeños, y controlar los términos de error mediante estimaciones uniformes. Este enfoque resulta especialmente eficaz en problemas como el de Waring o las conjeturas de Goldbach, donde el número de sumandos forma parte esencial del planteamiento.

Por otro lado, cuando se consideran las representaciones totales, es decir, aquellas en las que el número de partes no está fijado (como ocurre en el caso de las particiones), el comportamiento analítico cambia de manera fundamental. En este segundo marco, el objeto central ya no es un fenómeno oscilatorio, sino el análisis de las singularidades de la función de representación. El crecimiento de los coeficientes está gobernado por la aparición de polos dominantes y presenta un carácter exponencial. Este es el contexto en el que se inscriben los métodos desarrollados por Hardy y Ramanujan, y posteriormente sistematizados y generalizados por Wright y Meinardus.

Intentar tratar este segundo marco utilizando las herramientas propias del primero no solo son una simplificación conceptual, sino un error de enfoque. El hecho de que el método del círculo se aplique casi exclusivamente a representaciones con un número fijo de partes no es una limitación creada, sino una condición estructural fundamental. Las representaciones totales mezclan distintos tamaños de partes, introducen singularidades dominantes y eliminan la estructura oscilatoria que hace posible el análisis mediante arcos mayores y menores. Por esta razón, el estudio asintótico de funciones como $r_A(n)$ pertenece naturalmente a otras teorías, desarrolladas en paralelo, pero basadas en herramientas esencialmente distintas.

Desde esta perspectiva, el aporte de Hardy y Littlewood va más allá de la mera extensión del método del círculo al problema de Waring. Su trabajo estableció las bases conceptuales del método clásico, en particular la **distinción entre arcos mayores y menores** y el uso de **funciones generadoras asociadas a representaciones**. Estas ideas constituyen el punto de partida de todas las versiones posteriores del método, incluidas las modificaciones fundamentales introducidas por **Iván Matvéievich Vinográdov**, que se estudiarán en la siguiente sección.

2.3. Vinográdov

El desarrollo del método del círculo no se detuvo con las contribuciones fundamentales de Hardy y Littlewood. Sus ideas iniciales abrieron una línea de investigación que, durante las décadas siguientes, sería profundamente transformada y ampliada. En este proceso, una figura resulta central: **Iván Matvéievich Vinográdov.** Su trabajo no solo consolidó el método del círculo como una herramienta robusta de la teoría analítica de números, sino que redefinió su alcance y eficacia, particularmente en problemas aditivos de naturaleza aritmética profunda mediante modificaciones fundamentales al método.

Vinográdov nació en 1891 en Rusia y desarrolló la mayor parte de su carrera en un

contexto matemático muy distinto al de Cambridge. Mientras que Hardy y Littlewood trabajaban dentro de una tradición analítica influida por el análisis complejo, Vinográdov se formó en la escuela rusa de teoría de números, caracterizada por una orientación más técnica. Esta diferencia de formación condicionó de manera decisiva su aproximación al método del círculo. Las modificaciones introducidas por Vinogradov al método del círculo pueden encontrarse, en su forma original en [6], con una explicación detallada dada por Karatsuba en [25], mientras que exposiciones modernas y sistemáticas se presentan en [1, 7].

Vinográdov es considerado por algunos, un maestro en las sumas exponenciales, ya en 1918 tuvo sus primeros acercamientos a estos objetos donde de forma independiente junto con George Pólya (*Über den Wert der Partialsummen der Dirichletschen Reihen bei* $s = 1$) demostró una cota uniforme dado un carácter de Dirichlet no principal modulo q[4]:

$$\max_{1\leq N\leq q}\left|\sum_{n=1}^{N}\chi(n)\right| \leq C\sqrt{q}\log q$$

donde $C > 0$ es una constante absoluta. O de manera equivalente, para cualesquiera enteros $0 \leq M < N \leq q$,

$$\left|\sum_{n=M+1}^{N}\chi(n)\right| \ll \sqrt{q}\log q$$

Esta desigualdad proporciona una cota no trivial para las sumas parciales de caracteres, y siendo uno de los primeros resultados generales de este tipo, previo a refinamientos posteriores. Para una mejor comprensión de los carácteres de Dirichlet guiamos al lector al **Apendice A**.

Trabajos posteriores ya daban a notar la inclinación del joven Vinogradov a trabajar sobre distintas estimaciones aplicadas a funciones de carácter exponencial. Entre 1920 y 1923, Vinográdov desarrolló nuevas técnicas para el estudio de problemas de puntos reticulares, como el problema del círculo de Gauss y el de la hipérbola de Dirichlet. En estos trabajos introdujo de manera sistemática métodos analíticos basados en la descomposición en series trigonométricas de funciones discontinuas asociadas al conteo de puntos enteros tales como la función parte fraccionaria $\{x\}$. Este enfoque permitió reducir el problema geométrico a la estimación de sumas exponenciales del tipo

$$\sum_{n=1}^{N} e(f(n)) \tag{2.3.1}$$

Por esos mismos años, en 1924, Vinográdov abordó el problema de la distribución de partes fraccionarias de funciones de dos variables. En estos trabajos, publicados en los *Comptes Rendus de l'Académie des Sciences*, refinó métodos introducidos previamente por Weyl para la estimación de sumas exponenciales polinómicas de la forma 2.3.1. En particular, sistematizó el procedimiento de diferenciación sucesiva, controlando de manera más precisa las constantes que aparecen al iterar el proceso, y extendió estas técnicas al caso de varias variables. Estos avances sentaron las bases de los métodos que Vinográdov desarrollaría plenamente en la década siguiente. Estos desarrollos lo formaron cada vez

[4]En la literatura moderna, se le denomina "Desigualdad de Pólya–Vinográdov". El nombre se utiliza para la formulación unificada de los resultados de ambos, aunque los argumentos y contextos originales de Pólya y Vinográdov no eran idénticos. La versión estándar con el factor $q\log q$ es una normalización posterior ampliamente aceptada.

mas en la técnica y habilidad para controlar el crecimiento de sumas exponenciales, tales como las que aparecen al aplicar el método del circulo.

Ya en 1926 el método del circulo implementado por Hardy y Littlewood había tenido tiempo suficiente para ser entendido y estudiado por otros matemáticos, uno de ellos fue Vinográdov el cual observo como estimaciones tipo Weyl eran fundamentales para poder controlar el crecimiento de los arcos menores, sin embargo se dio cuenta del problema fundamental de hacer aproximaciones del tipo

$$f_A(\rho e(\alpha)) = \sum_{a\in A} \rho^a e(\alpha a) \sim \sum_{\substack{a\in A \\ a\leq X}} e(\alpha a)$$

realizadas en el problema de Waring, por Hardy y Littlewood. Ademas de esto, noto la fuerte dependencia y sensibilidad del método al crecimiento de la función generadora

$$R_{k,A}(z) = f_A^k(z)$$

cerca de la frontera del disco unitario, mas específicamente, cerca de las raíces de la unidad.

Estas simplificaciones y dependencia vienen del hecho fundamental que la función de representación $f_A(z)$ es una serie infinita con radio de convergencia 1. Este enfoque es natural desde el punto de vista formal pues, a través del análisis complejo, permite expresar el número de representaciones mediante una identidad exacta;

$$r_{k,A}(n) = \rho^{-n} \int_0^1 f_A(\rho e(\alpha))^k e(-n\alpha) d\alpha$$

y trabajar sobre ella, pero como mencionamos, causa problemas delicados a tratar cada uno. Fue Vinográdov quien introdujo una modificación conceptual decisiva: en lugar de trabajar con la función de representación infinita, propuso **considerar su versión truncada**, ya que esta era suficiente para contar el numero de representaciones de un entero. ¿Como exactamente?

Demos un recordatorio del análisis hecho en el Capitulo 1. Dado $A \subseteq \mathbb{Z}^+$ infinito, el numero de representaciones de un entero positivo n como suma de k elementos de A, vienen empaquetados en los coeficientes de la serie:

$$r_{k,A}(n) = [z^n] f_A^k(z) = [z^n] \left(\sum_{a\in A} z^a \right)^k \tag{2.3.2}$$

donde la función de representación de A es una serie infinita. La ecuación 2.3.2 nos cuenta el numero de soluciones de la ecuación aditiva,

$$x_1 + x_2 + \cdots + x_k = n,\ x_i \in A$$

pero podemos notar un detalle importante. Dado un n fijo, podemos exigir condiciones mas especificas a las soluciones, pues cada variable x_i no podrá exceder el valor de n, de tal forma que es suficiente con contar el numero de soluciones de

$$x_1 + x_2 + \cdots + x_k = n,\ x_i \in A \text{ y } x_i \leq n$$

Mediante la formula producto de Cauchy y considerando la serie truncada podemos obtener que,

$$\left(\sum_{\substack{a\in A\\ a\leq n}} z^a\right)^k = \left(\sum_{m=0}^{n} \delta_A(m) z^m\right)^k = \sum_{m=0}^{nk} \left(\sum_{\substack{x_1+x_2+\cdots+x_k=m\\ 0\leq x_i\leq n}} \delta_A(x_1)\delta_A(x_2)\cdots\delta_A(x_k)\right) z^m \tag{2.3.3}$$

notando que el sumando interior no es cero unicamente si tenemos una solución de la ecuación $x_1 + x_2 + \cdots + x_k = m$ donde $x_i \in A$ y $0 \leq x_i \leq n$, tendremos que el coeficiente n-esimo sera:

$$r_{k,A}(n) = [z^n]\left(\sum_{\substack{a\in A\\ a\leq n}} z^a\right)^k \tag{2.3.4}$$

mas aun, con la ecuación 2.3.3, para cada $m \leq n$,

$$r_{k,A}(m) = [z^m]\left(\sum_{\substack{a\in A\\ a\leq n}} z^a\right)^k$$

Con esto podemos obtener el numero de representaciones de n, $r_{k,A}(n)$, a través de una suma finita (dependiente de n), de tal forma que le daremos su debida definición a la función involucrada.

Definición 2.3.1

Sea $A \subseteq \mathbb{Z}^+$ infinito y $n \in \mathbb{Z}^+$ fijo. Definimos la **función de representación de A truncada en n** como

$$f_A(z,n) := \sum_{\substack{a\in A\\ a\leq n}} z^a$$

La ecuación 2.3.4 afirma que.

$$r_{k,A}(n) = [z^n] f_A^k(z,n)$$

recuperando así el numero de representaciones a partir de, ya no una serie infinita, sino de una suma finita (polinomio). La diferencia crucial entre ambos enfoques es que la función de representación $f_A^k(n)$ contenía toda la información del numero de representaciones para cada entero positivo mientras que con la función $f_A^k(z,n)$ no es necesaria toda la información del numero de representaciones para todo entero positivo, sino la suficiente para una n en especifico. Esta distinción la podemos ver al analizar nuestro caso de representaciones de enteros.

Ejemplo. Recordemos que la función de representación de los enteros es:

$$f_{\mathbb{Z}^+}(z) = \sum_{a\in\mathbb{Z}^+} z^a = \sum_{m=1}^{\infty} z^m = \frac{z}{1-z}$$

de tal forma que

$$r_k(n) = [z^n] f^k_{\mathbb{Z}^+}(z) = [z^n] \frac{z^k}{(1-z)^k} = \binom{n-1}{k-1}$$

Pero al considerar la función de representación de los enteros truncada en n,

$$f_{\mathbb{Z}^+}(z,n) = \sum_{\substack{a \in \mathbb{Z}^+ \\ a \leq n}} z^a = \sum_{m=1}^{n} z^m = \frac{z(1-z^n)}{1-z}$$

obtenemos que para cada $m \in \mathbb{Z}^+$,

$$r_k(m) = [z^m] f^k_{\mathbb{Z}^+}(z,n) = [z^m] \frac{z^k(1-z^n)^k}{(1-z)^k}$$

usando el teorema del binomio generalizado

$$\frac{z^k}{(1-z)^k} = z^k \sum_{t=0}^{\infty} \binom{-k}{t} (-1)^t z^t = z^k \sum_{t=0}^{\infty} \binom{t+k-1}{t} z^t$$

ademas

$$(1-z^n)^k = \sum_{j=0}^{k} \binom{k}{j} (-1)^j z^{jn}$$

multiplicando,

$$f^k_{\mathbb{Z}^+}(z,n) = z^k \sum_{j=0}^{k} \binom{k}{j} (-1)^j z^{jn} \sum_{t=0}^{\infty} \binom{t+k-1}{t} z^t$$

por lo tanto,

$$f^k_{\mathbb{Z}^+}(z,n) = \sum_{j=0}^{k} \binom{k}{j} (-1)^j \sum_{t=0}^{\infty} \binom{t+k-1}{t} z^{t+k+jn}$$

Para obtener el coeficiente $[z^m]$ queremos que

$$t + k + jn = m \quad \Rightarrow \quad t = m - k - jn$$

esto exige que $m - k - jn \geq 0$, luego

$$[z^m] f^k_{\mathbb{Z}^+}(z,n) = \sum_{\substack{j \geq 0 \\ m-k-jn \geq 0}} (-1)^j \binom{k}{j} \binom{m-jn-1}{k-1}$$

pero dado que $j \in \mathbb{Z}$ podemos considerar el rango de la suma como

$$\sum_{j=0}^{\lfloor \frac{m-k}{n} \rfloor} (-1)^j \binom{k}{j} \binom{m-jn-1}{k-1}$$

De forma sencilla podemos verificar que para $m \leq n$ (y la suposición implícita de $m, n > k$) tendremos que $\frac{m-k}{n} < 1$, entonces la suma es no cero solo para $j = 0$, por lo que

$$r_k(m) = [z^m] f^k_{\mathbb{Z}^+}(z,n) = (-1)^0 \binom{k}{0} \binom{m-(0)n-1}{k-1} = \binom{m-1}{k-1}$$

como ya sabíamos. Para valores de $m > n$ dicha formula ya no nos dará el numero de representaciones, como se puede ver en la figura 2.3.1

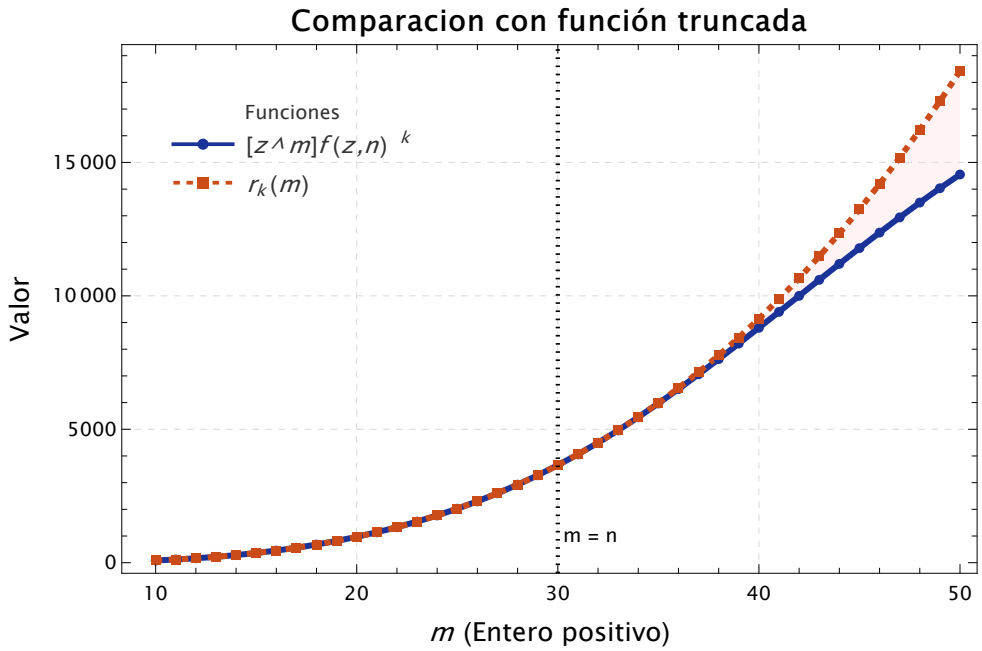

Figura 2.3.1: *Grafica de los valores de $r_k(m)$ y el valor obtenido con la serie truncada para cada $1 \leq m \leq 50$ con $k = 4$. Note como a partir de $m = n$ ambas graficas dejan de ser iguales.*

Dado que la función de representación truncada $f_A(z, n)$ es un polinomio, sera una función entera, por tanto, es posible utilizar la formula integral de Cauchy sin necesidad de ningún análisis de convergencia, obteniendo que

$$r_{k,A}(n) = \frac{1}{2\pi i} \int_\gamma \frac{f_A^k(z,n)}{z^{n+1}} dz$$

para cualquier contorno circular γ centrado en el origen. Esta condición nos da la posibilidad de tomar el **disco unitario** como contorno de integración a diferencia del contorno utilizado para las particiones y el problema de Waring, obteniendo la representación:

$$r_{k,A}(n) = \int_0^1 f_A(e(\alpha), n)^k e(-n\alpha) d\alpha$$

Esta modificación introduce un cambio profundo en la naturaleza analítica del método del círculo. Al reemplazar la función de representación infinita por una suma truncada dependiente de n el problema deja de estar ligado a cuestiones de convergencia y comportamiento singular cerca de la frontera, y se transforma en el estudio de sumas exponenciales finitas bien definidas, como las estudiadas en el Apéndice A..

$$f_A(e(\alpha), n) = \sum_{\substack{a \in A \\ a \leq n}} e(\alpha a)$$

Desde un punto de vista técnico, esta transición resulta exacta. En el método clásico, el análisis de los arcos menores dependía de aproximaciones formales entre la función y sumas finitas, lo que introducía dependencias del radio del contorno circular de integración

ρ y de la proximidad a las raíces de la unidad $e(\frac{h}{k})$:

$$f_A(\rho e(\alpha)) \sim \sum_{\substack{a\in A\\ a\leq X}} e\left(\frac{h}{k}a\right)$$

En cambio, al trabajar directamente con la función truncada $f_A(z,n)$, las sumas exponenciales que aparecen en los arcos menores son finitas desde el inicio, lo que permite aplicar de manera directa las estimaciones de Weyl y Hua.

Otro cambio de estructura fundamental al método del circulo es que podemos prescindir de la formula integral de Cauchy, centrándonos mas en un análisis real. Sea $n \in \mathbb{Z}$ entonces,

$$\int_0^1 e(nx)dx = \begin{cases} 1 & \text{si } n = 0 \\ 0 & \text{en otro caso} \end{cases} \tag{2.3.5}$$

Esta identidad fundamental nos da el siguiente resultado inmediato

Proposición 2.3.1

Sea $A \subseteq \mathbb{Z}^+$ infinito y $n \in \mathbb{Z}^+$. Tendremos que

$$\begin{aligned} r_{k,A}(n) &= \sum_{\substack{x_i\in A\\ x_i\leq n}} \int_0^1 e((x_1+\cdots+x_k)\alpha)e(-n\alpha)d\alpha \\ &= \int_0^1 f_A(e(\alpha),n)^k e(-n\alpha)d\alpha \end{aligned}$$

Demostración. Por la ecuación 2.3.5, la integral

$$\int_0^1 e((x_1+\cdots+x_k)\alpha)e(-n\alpha)d\alpha = \int_0^1 e((x_1+\cdots+x_k-n)\alpha)d\alpha = \begin{cases} 1 & \text{si } n = x_1+\cdots+x_k \\ 0 & \text{en otro caso} \end{cases}$$

de donde sumando para todas las posibles variables $x_i \in A$ con $x_i \leq n$, por cada solución de la ecuación aditiva $n = x_1 + \cdots + x_k$ con $x_i \in A$ y $x_i \leq n$ sumaremos un 1. De tal forma que recuperamos el numero total de representaciones $r_{k,A}(n)$. Más aun, con esta expresión podemos recuperar la obtenida a partir de la formula integral de Cauchy. En

efecto,

$$r_{k,A}(n) = \sum_{\substack{x_i \in A \\ x_i \leq n}} \int_0^1 e((x_1 + \cdots + x_k)\alpha) e(-n\alpha) d\alpha = \int_0^1 \sum_{x_i \in A} e((x_1 + \cdots + x_k)\alpha) e(-n\alpha) d\alpha$$

$$= \int_0^1 \left[\sum_{\substack{x_1 \in A \\ x_1 \leq n}} \cdots \sum_{\substack{x_k \in A \\ x_k \leq n}} e(x_1\alpha) \cdots e(x_k\alpha) \right] e(-n\alpha) d\alpha$$

$$= \int_0^1 \left(\sum_{\substack{x_1 \in A \\ x_1 \leq n}} e(x_1\alpha) \right) \cdots \left(\sum_{\substack{x_k \in A \\ x_k \leq n}} e(x_k\alpha) \right) e(-n\alpha) d\alpha$$

$$= \int_0^1 \left(\sum_{\substack{a \in A \\ a \leq n}} e(\alpha a) \right)^k e(-n\alpha) d\alpha = \int_0^1 f_A(e(\alpha), n)^k e(-n\alpha) d\alpha$$

□

Una duda que podría surgir es si no era posible trabajar con el conjunto infinito A directamente, evitando el truncamiento. Sin embargo, esto presenta un obstáculo fundamental en el análisis. Dada la suma infinita

$$\sum_{x_i \in A} \int_0^1 e((x_1 + \cdots + x_k)\alpha) e(-n\alpha) d\alpha$$

dicha expresión es convergente, ya que solo hay un numero finito de soluciones a la ecuación aditiva. El problema fundamental seria en el paso de intercambiar la suma con la integral

$$\int_0^1 \sum_{x_i \in A} e((x_1 + \cdots + x_k)\alpha) e(-n\alpha) d = \int_0^1 \left(\sum_{a \in A} e(\alpha a) \right)^k e(-n\alpha) d\alpha$$

Para que este paso sea válido (o incluso para que la expresión tenga sentido), la serie infinita

$$\sum_{a \in A} e(\alpha a)$$

debe converger a una función integrable en $[0, 1]$, sin embargo,

$$|e(\alpha a)| = 1$$

por lo que la serie diverge para casi para toda α (excepto quizás para conjuntos de medida cero donde podría haber cancelaciones excepcionales), de tal forma que la serie no esta bien definida y no existe. Entonces no es posible hacer dicho análisis.

Con estas nuevas modificaciones y su perspicacia en el estudio de las sumas exponenciales fue que, en 1927, Vinográdov obtuvo resultados asintóticos para el problema de Waring, publicados en *Izvestiya Akademii Nauk SSSR*[5]. Su cota para $G(k)$ era del mismo

[5]No existe un único artículo en el que Vinográdov presente de manera directa sus resultados sobre el problema de Waring. Estos se encuentran dispersos en varios trabajos publicados entre 1926 y 1928, principalmente en ruso, en revistas como Izvestiya Akademii Nauk SSSR. La exposición moderna del método y de los resultados se debe en gran parte a reconstrucciones posteriores en la literatura, en particular en los textos de Hardy, Davenport y Vaughan, donde el enfoque de Vinográdov se presenta como una reformulación aritmética del método del círculo.

orden que la de Hardy y Littlewood, es decir, del orden de $k2^k$ pero el método constituía una simplificación notable, ya que prescindía del uso del análisis complejo (formula integral de Cauchy) y de ciertas estimaciones delicadas en los arcos menores. Detallaremos aquí estas mejoras sustanciales.

En el enfoque de Hardy y Littlewood, el punto de partida fue el estudio de la función

$$f_{A_k}(\rho e(\alpha)) = \sum_{m=0}^{\infty} \rho^{m^k} e\left(\alpha m^k\right), \quad 0 < \rho < 1$$

la cual permite expresar el número de representaciones mediante,

$$r_{s,A_k}(n) = \rho^{-n} \int_0^1 f_{A_k}(\rho e(\alpha))^s e(-n\alpha) d\alpha$$

siendo necesario justificar posteriormente el paso al límite $\rho \to 1^-$.

Con las modificaciones, Vinográdov introdujo la representación,

$$f_{A_k}(z,n) := \sum_{\substack{a \in A_k \\ a \leq n}} z^a = \sum_{0 \leq m^k \leq n} z^{m^k} = \sum_{0 \leq m \leq X} z^{m^k}, \quad X = n^{\frac{1}{k}}$$

considerando la suma exponencial

$$F(\alpha) := f_{A_k}(e(\alpha), n) = \sum_{0 \leq m \leq X} e(\alpha m^k)$$

Mediante el uso de la **Proposición 2.3.1** tenemos

$$r_{s,A_k}(n) = \int_0^1 F(\alpha)^s e(-n\alpha) d\alpha$$

sin necesidad de introducir parámetros extra ni justificar intercambios de límites haciendo que el objeto de estudio quede completamente determinado por una suma finita de naturaleza aritmética.

La disección del intervalo $[0,1]$ en arcos mayores y arcos menores se mantiene idéntica en a la utilizada por Hardy y Littlewood. Para $\alpha \in \mathfrak{M}_{a,q}$, se escribe

$$\alpha = \frac{a}{q} + \beta, \quad |\beta| \leq \frac{1}{qN}$$

y se aprovecha esta aproximación racional para separar la parte aritmética de la parte analítica en la suma exponencial. Agrupando los términos módulo q, Vinográdov obtiene, al igual que Hardy y Littlewood, una aproximación del tipo

$$F(\alpha) = F(\frac{a}{q} + \beta) = \frac{1}{q} S(a,q) I(\beta) + O(q)$$

donde

$$S(a,q) = \sum_{r=1}^{q} e\left(\frac{ar^k}{q}\right)$$

es la suma de Gauss generalizada, e $I(\beta)$ es la integral oscilatoria

$$I(\beta) = \int_0^X e(\beta x^k)dx$$

En consecuencia, la contribución principal de los arcos mayores sigue descomponiéndose en un factor aritmético (serie singular) y un factor analítico, exactamente como en el método clásico. La diferencia crucial esta en la justificación de esta aproximación. En el enfoque de Hardy y Littlewood, la parte analítica surge de la singularidad de la serie de potencias cuando $\rho \to 1^-$, este paso introduce un término de error cuyo comportamiento debe controlarse cuidadosamente.

En el método de Vinográdov, la suma exponencial está truncada desde el inicio para $m \leq X$. No existe un margen de error que deba despreciarse, y la integral $I(\beta)$ aparece de manera directa como un objeto asociado a la suma finita. Luego, al construir la integral singular, Vinográdov extiende el dominio de integración de la variable β a todo la recta real$\mathbb{R}$ (que originalmente está restringida al tamaño del arco mayor), aprovechando que la integral oscilatoria $I(\beta)$ decae rápidamente fuera de los arcos mayores, mostrando que el error generado por esta extención de la integral es controlable.

Sustituyendo la aproximación anterior en la integral sobre los arcos mayores y elevando a la potencia s, se obtiene una contribución principal de la forma

$$\sum_{q=1}^{\infty} \sum_{\substack{1\leq a\leq q \\ (a,q)=1}} \frac{S(a,q)^s}{q^s} e\left(-\frac{an}{q}\right) \int_{-\infty}^{\infty} I(\beta)^s e(-n\beta)d\beta$$

De este modo, reaparecen la serie singular

$$\mathfrak{G}_{k,s}(n) = \sum_{q=1}^{\infty} \sum_{\substack{1\leq a\leq q \\ (a,q)=1}} S(a,q)^s e\left(-\frac{an}{q}\right)$$

y la aparición de una **integral singular**

$$\mathfrak{J}_{k,s}(n) = \int_{-\infty}^{\infty} I(\beta)^s e(-n\beta)d\beta$$

cuya evaluación conduce al mismo factor gamma obtenido por Hardy y Littlewood. En particular, el término principal final permanece sin cambios:

$$r_{s,A_k}(n) \sim \frac{\Gamma(1+\frac{1}{k})^s}{\Gamma(\frac{s}{k})} n^{\frac{s}{k}-1} \mathfrak{G}_{k,s}(n)$$

Es en el tratamiento de los arcos menores donde la modificación de Vinográdov muestra su mayor ventaja. En el enfoque de Hardy y Littlewood, la estimación

$$|f_{A_k}(\rho e(\alpha))| \ll X^{1-\sigma}$$

requiere justificar la aplicación de la desigualdad de Weyl a una serie infinita, recurriendo implícitamente a sumación parcial y a cotas uniformes respecto al parámetro ρ. Al trabajar con la suma finita $F(\alpha)$, Vinográdov puede aplicar directamente el Lema de Weyl para $\alpha \in \mathfrak{m}$,

$$|F(\alpha)| = \left| \sum_{0\leq m\leq X} e(\alpha m^k) \right| \ll X^{1-\sigma}$$

La estructura general de la estimación se mantiene formalmente igual (uso de la desigualdad de Hölder y del Lema de Hua para controlar potencias), pero la ausencia de promediar simplifica sustancialmente los argumentos técnicos.

Como consecuencia de esta reformulación, Vinográdov obtuvo cotas para $G(k)$ del mismo orden de magnitud que las de Hardy y Littlewood, sin embargo, la eliminación del uso del análisis complejo, el uso fundamental de sumas exponenciales finitas y el manejo promedio de los arcos menores constituyen una mejora sustancial en la prueba. Estas ideas permitirían desarrollos posteriores que reducirían de manera sustancial el número de variables necesarias, culminando en cotas del orden $k \log k$ y estableciendo el uso de sumas truncadas como una base del método del circulo.

2.4. Consolidación

Antes de entrar en el desarrollo de esta sección, es conveniente realizar una aclaración conceptual sobre el punto exacto en el que se encuentra el método del círculo tras los avances discutidos en las secciones anteriores.

En la Sección 2.2 se analizó el surgimiento del método del círculo clásico a partir de los trabajos de Hardy y Littlewood, haciendo énfasis en dos ideas fundamentales: por un lado, el paso del estudio de funciones generadoras de particiones al análisis del número de representaciones en un número fijo de partes; y por otro, la introducción geométrica de la distinción entre arcos mayores y arcos menores como herramienta central para separar la estructura aritmética principal de los fenómenos de cancelación analítica.

Posteriormente, en la Sección 2.3 se estudió la modificación introducida por Vinogradov al método del círculo, consistiendo en el reemplazado de la función de representación infinita por la versión truncada. Esta truncación transforma el problema en uno finito y permite aplicar de manera directa estimaciones sobre sumas exponenciales, particularmente en el análisis de los arcos menores.

Con todo esto presentaremos una estructura unificada aplicable a conjuntos arbitrarios de enteros positivos con todo lo visto en las secciones anteriores.

Primeramente, como hemos visto hasta este momento, el estudio del numero de representaciones de n en k partes de elementos de A, estará íntimamente ligada a la función de representación truncada. Pero en esta nueva visión del método la consideraremos como una suma exponencial desde un inicio.

Definición 2.4.1

Sea $A \subseteq \mathbb{Z}^+$ infinito. Definimos la **suma exponencial asociada a** A (truncada en x) como la función $F : \mathbb{R} \times \mathbb{R}^+ \to \mathbb{C}$ definida por:

$$F_A(\alpha, x) := f_A(e(\alpha), x) = \sum_{\substack{a \in A \\ a \leq x}} e(\alpha a) = \sum_{m \leq x} \delta_A(m) e(\alpha m)$$

La función $F_A(\alpha, x)$ está bien definida para todo $x > 0$, pues se trata de una suma finita. Para x fijo, es una función continua y periódica en α, mientras que para α fijo es una función escalonada en x. Con ello por la **Proposición 2.3.1** el numero de representaciones

de n como suma de k elementos de A, vendrá dado por[6]

$$r_{k,A}(n) = \int_0^1 F_A^k(\alpha, n)e(-n\alpha)d\alpha$$

Con ello es claro como el crecimiento de $r_{k,A}(n)$ sera dependiente de saber describir el comportamiento de $F_A(\alpha, n)$ de forma eficaz en el intervalo $[0, 1]$. Es por eso que nos detendremos a estudiar esta función, mas específicamente, su crecimiento y promedio.

Un caso particular de especial importancia que es inmediato es $\alpha = 0$ (y todo α entero), para el cual se recupera la función contadora del conjunto A,

$$F_A(0, x) = \sum_{\substack{a\in A\\ a\leq x}} e(0) = \pi_A(x)$$

Siendo, de hecho, una representación del valor máximo en modulo que podrá tomar, teniendo la siguiente cota trivial.

Lema 2.4.1

Sea $A \subseteq \mathbb{Z}^+$ infinito. Entonces para todo $\alpha \in [0, 1]$

$$|F_A(\alpha, x)| \leq \pi_A(x)$$

Demostración. En efecto,

$$|F_A(\alpha, x)| = \left|\sum_{\substack{a\in A\\ a\leq x}} e(\alpha a)\right| \leq \sum_{\substack{a\in A\\ a\leq x}} |e(\alpha a)| = \sum_{\substack{a\in A\\ a\leq x}} 1 = \pi_A(x)$$

alcanzando la igualdad cuando $\alpha \in \mathbb{Z}$ (salvo otros puntos excepcionales). □

En el método del círculo, esto justifica por qué el "Arco Mayor" centrado en 0 (o en 1) es el que aporta el término principal asintótico: es donde la función es "más grande".

Ejemplo. Notemos el cambio en la magnitud de $|F_A(\alpha, x)|$ con los ejemplos que ya hemos manejado, considerando los conjuntos $\mathscr{A}$ y A_k, tenemos

$$\pi_{\mathscr{A}}(x) = \sum_{1\leq 2n+1\leq x} 1 = \sum_{0\leq n\leq \frac{x-1}{2}} 1 = \left\lceil \frac{x-1}{2} \right\rceil$$

$$\pi_{A_k}(x) = \sum_{0\leq n^k\leq x} 1 = \sum_{0\leq n\leq \sqrt[k]{x}} 1 = \lceil \sqrt[k]{x} \rceil$$

de tal forma que

$$|F_{\mathscr{A}}(\alpha, x)| \leq \left\lceil \frac{x-1}{2} \right\rceil$$

$$|F_{A_k}(\alpha, x)| \leq \lceil \sqrt[k]{x} \rceil$$

como podemos observar en la Figura 2.4.1

[6] Técnicamente es valido considerar $\int_0^1 F_A^k(\alpha, x)e(-n\alpha)d\alpha$ para cada $x > n$, sin embargo, esto no presenta ninguna ventaja analítica, ya que los términos correspondientes a sumandos $a > n$ se anulan tras la integración. Es por ello que en la practica se considera específicamente $x = n$.

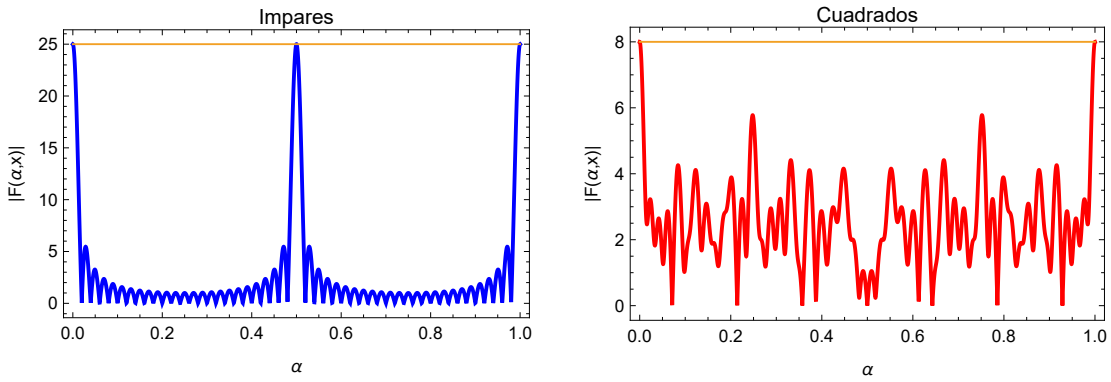

Figura 2.4.1: *Para $x = 50$, se observa el comportamiento oscilatorio de $|F_A(\alpha, 50|)$ para el caso de impares $\mathscr{A}$ y cuadrados A_2, con $\alpha \in [0,1]$. Observando el crecimiento acotado por $\lceil \frac{50-1}{2} \rceil = 25$ y $\lfloor \sqrt[2]{50} \rfloor = 7$.*

Si bien ya sabemos el valor máximo que podrá tomar $|F_A(\alpha, x)|$, este no refleja el valor promedio de dicha función, ya que en la mayor parte del intervalo $[0,1]$ no alcanza su valor máximo. Una herramienta que refleja mejor el crecimiento promedio de una función es tomar su media cuadrática:

Lema 2.4.2

Sea $A \subseteq \mathbb{Z}^+$ infinito. Entonces

$$\int_0^1 |F_A(\alpha, x)|^2 \, d\alpha = \pi_A(x)$$

Demostración. En efecto,

$$\begin{aligned}\int_0^1 |F_A(\alpha, x)|^2 \, d\alpha &= \int_0^1 F_A(\alpha, x)\overline{F_A(\alpha, x)}d\alpha = \int_0^1 F_A(\alpha, x)F_A(-\alpha, x)d\alpha \\ &= \int_0^1 \left(\sum_{\substack{a \in A \\ a \leq x}} e(\alpha a) \right) \left(\sum_{\substack{m \in A \\ m \leq x}} e(-\alpha m) \right) d\alpha \\ &= \sum_{\substack{a \in A \\ a \leq x}} \sum_{\substack{m \in A \\ m \leq x}} \int_0^1 e(\alpha(a-m))d\alpha\end{aligned}$$

y por la ecuación 2.3.5, el único sumando que sobrevive es aquel tal que $a - m = 0$, por lo que

$$\int_0^1 |F_A(\alpha, x)|^2 \, d\alpha = \sum_{\substack{a \in A \\ a \leq x}} 1 = \pi_A(x)$$

□

Por tanto, la media cuadrática de $F_A(\alpha, x)$ en $[0,1]$ sera:

$$\sqrt{\int_0^1 |F_A(\alpha, x)|^2 \, d\alpha} = \sqrt{\pi_A(x)}$$

Esto indica que, si bien la función tiene picos de altura $\pi_A(x)$ (como en $\alpha = 0, 1$), "en promedio" es mucho más pequeña (de orden $\sqrt{\pi_A(x)}$). Aplicado a nuestros ejemplos, esto establece que el crecimiento promedio es

$$|F_{\mathscr{A}}(\alpha, x)| \approx \sqrt{\frac{x-1}{2}} \quad \text{y} \quad |F_{A_k}(\alpha, x)| \approx x^{\frac{1}{2k}}$$

En un primer momento podríamos pensar que esto seria una aproximación al numero de representaciones sin embargo no sera el caso, por ejemplo, para suma de 4 cuadrados,

$$r_{4,A_2}(20) = 18$$

mientras que

$$20^{\frac{1}{2(2)}} \approx 2.1$$

Esto es debido a la naturaleza oscilatoria que proporciona el termino $e(-n\alpha)$ en la integral. Provocando que un estudio promedio del crecimiento no sea suficiente, dando a notar como el conocer los puntos donde las oscilaciones son mayores dicten el orden del crecimiento. Para ver esto retomemos la Figura 2.4.1, podemos notar como hay un mayor crecimiento en $\alpha = 0, 1$ (puntos donde alcanza el máximo) entonces podríamos decir que la mayor contribución viene de cuando $\alpha \approx 0, 1$. Así que la altura del integrando cerca de estos puntos es $(\pi_A(n))^k$ y el ancho promedio de ese "valle" sera del orden de $\frac{1}{n}$, debido a que para generar cancelaciones oscilatorias se necesita completar al menos una vuelta completa, por tanto tendremos la estimación

$$r_{k,A}(n) \approx \frac{1}{n}\pi_A^k(n)$$

Veamos esta estimación, aplicada a nuestros ejemplos. Sabiendo (de acuerdo al Capitulo 1) que $r_{k,\mathscr{A}}(n)$ sera no cero cuando $n \equiv k \pmod 2$,

$$r_{k,\mathscr{A}}(n) \approx \frac{1}{n}\pi_{\mathscr{A}}^k(n) = \frac{1}{n}\left\lceil \frac{n-1}{2} \right\rceil^k$$

para el caso $k = 3$, con n impar, podemos notar que se convierte en una buena aproximación. Sabemos que en este caso,

$$r_{3,\mathscr{A}}(n) = T_{(n-1)/2} = \frac{(n-1)(n-3)}{8}$$

y en nuestra aproximación

$$r_{3,\mathscr{A}}(n) \approx \frac{1}{n}\left\lceil \frac{n-1}{2} \right\rceil^3$$

resultando que, efectivamente,

$$r_{3,\mathscr{A}}(n) \sim \frac{1}{n}\left\lceil \frac{n-1}{2} \right\rceil^3$$

sin embargo, al tomar $k = 4$ o mayor, esta aproximación se vuelve menos exacta como podemos notar en la Figura 2.4.2

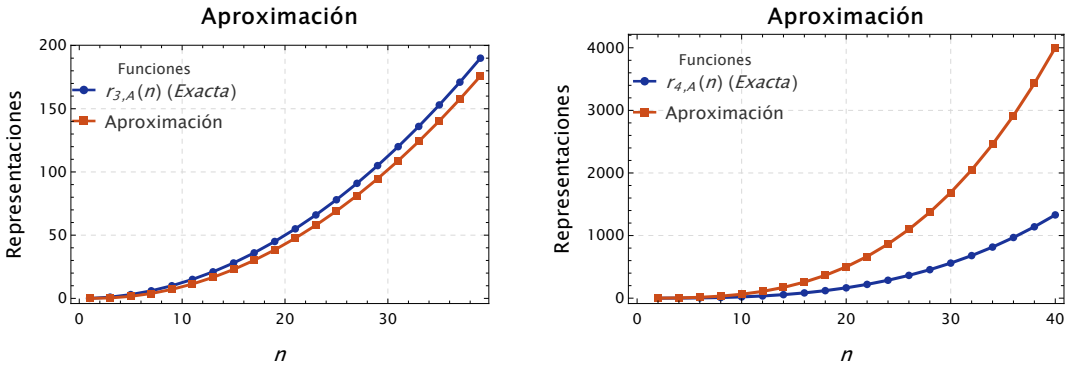

Figura 2.4.2: *Comparación de $r_{3,\mathscr{A}}(n)$ (para impares) y $r_{4,\mathscr{A}}(n)$ (para pares) con sus aproximaciones $\frac{1}{n}\left\lceil\frac{n-1}{2}\right\rceil^k$.*

De la misma manera esta estimación nos diría que para el caso de suma de cuatro cuadrados

$$r_{4,A_2}(20) \approx \frac{1}{n}\pi^4_{A_2}(n) = \frac{1}{n}\left\lceil\sqrt[4]{n}\right\rceil^4 \approx 1$$

resulta evidente que proporciona una aproximación muy deficiente.

Estos dos ejemplos nos dicen dos cosas. La primera; tomar un intervalo cercano a $\alpha = 0$ si puede darnos una aproximación eficiente, pero dependerá del nivel de oscilaciones presentes, es por ello que en el caso de impares al subir la cantidad de sumandos, nuestra aproximación (unicamente considerando la oscilación de $\alpha = 0$) es insuficiente, al igual que en el caso de suma de cuadrados por lo que es necesario identificar todas las oscilaciones constructivas que ocurren. Como segunda; el nivel de oscilaciones depende de los valores del numero a representar n y de la cantidad de sumandos k mostrando la delicadeza aritmética de ambos. Sera claro para el lector que la necesidad de seccionar el intervalo $[0,1]$ en partes de mayor aportación es el paso lógico a seguir, donde entrara en juego de forma **"natural"**, sin necesidad de hacer análisis de singularidades, el aplicar la lógica de los **arcos mayores**. Esto se consolida como una ventaja teórica ya que todo deja de depender de singularidades de funciones analíticas, a depender unicamente del estudio de sub-intervalos de $[0,1]$ donde una función oscilatoria tiene mayores picos. En este sentido, el método del círculo adquiere una formulación plenamente aritmética y geométrica, donde la descomposición del intervalo unitario refleja directamente la estructura de las sumas exponenciales involucradas.

Para poder reflejar esto podemos retomar el resultado de la **Proposición 2.2.1**, el cual no depende del conjunto que estemos tomando.

Proposición 2.4.1

Sea $\alpha \in \mathbb{Q}$ tal que $\alpha = {}^a/_q$ con $a \in \mathbb{Z}, q \in \mathbb{Z}^+$ y $(a,q) = 1$. Para cualquier conjunto $A \subseteq \mathbb{Z}^+$ infinito, el conjunto de valores $\{e(\alpha a) : a \in A\}$ es un subconjunto finito de las raíces q-ésimas de la unidad.

La proposición anterior establece que, cuando $\alpha = {}^a/_q$ es un número racional, el conjunto de valores que toma $e(\alpha a)$ para $a \in A$ es finito. Geométricamente, esto significa que los vectores unitarios sumados en $F_A(\alpha, x)$ no pueden apuntar en cualquier dirección del

círculo, sino que están restringidos a un conjunto discreto de q direcciones posibles (las raíces q-ésimas de la unidad).

Sin embargo, es importante notar que el hecho de que α sea racional **permite la alineación** de los vectores, pero **no la garantiza**. Que la suma crezca hasta formar un "pico" o se cancele depende enteramente de la aritmética específica del conjunto A, es decir, de cómo se distribuyen los elementos de A en las clases de residuos módulo q. Para ilustrar esto, consideremos conjuntos específicos:

- Caso $A = \mathbb{Z}^+$, con $\alpha = \frac{1}{2}$. Los elementos son 1, 2, 3, 4,.... Sus residuos modulo 2 se distribuyen de forma alternante, siendo, 1, 0, 1, 0,.... Por tanto, la suma $F_{\mathbb{Z}^+}(\frac{1}{2}, x)$ se convierte en

$$F_{\mathbb{Z}^+}(\frac{1}{2}, x) = \sum_{\substack{a\in\mathbb{Z}^+\\ a\leq x}} e\left(\frac{a}{2}\right) = e\left(\frac{1}{2}\right)+e\left(\frac{2}{2}\right)+e\left(\frac{3}{2}\right)+\cdots+e\left(\frac{\lfloor x\rfloor}{2}\right) = -1+1-1+\cdots+(-1)^{\lfloor x\rfloor}$$

  A pesar de que α es racional, la distribución alternante de los residuos provoca una cancelación casi perfecta. La suma está acotada y no genera un pico.

- Caso $A = \mathscr{A}$ impares, con $\alpha = \frac{1}{2}$. Los elementos son 1, 3, 5, 7,.... Sus residuos modulo 2 se distribuyen de forma uniforme, siendo, 1, 1, 1, 1,.... Por tanto, la suma $F_{\mathscr{A}}(\frac{1}{2}, x)$ se convierte en

$$F_{\mathscr{A}}(\frac{1}{2}, x) = \sum_{\substack{a\in\mathscr{A}\\ a\leq x}} e\left(\frac{a}{2}\right) = e\left(\frac{1}{2}\right) + e\left(\frac{3}{2}\right) + e\left(\frac{5}{2}\right) + \cdots = -1-1-1-\cdots$$

  Aquí, el conjunto $\mathscr{A}$ tiene una distribución concentrada en una sola clase de residuo. Esto genera una alineación total de los vectores en la dirección -1. El módulo de la suma crece linealmente con x, generando un pico máximo, como se puede observar en la Figura 2.4.1. Cosa que no pasa en el caso de suma de cuadrados.

- Caso $A = A_2$, con $\alpha = \frac{1}{2}$. Los elementos son 1, 4, 9, 16,.... Sus residuos modulo 2 se son, 1, 0, 1, 0,.... Al igual que en el caso de los enteros, vemos una alternancia entre residuos 1 y 0, lo que genera términos -1 y 1.

$$F_{A_2}(\frac{1}{2}, x) = \sum_{\substack{a\in A_2\\ a\leq x}} e\left(\frac{a}{2}\right) = \sum_{n^2\leq x} e\left(\frac{n^2}{2}\right) = -1+1-1+1-\cdots$$

  Por lo que no habrá un pico, tal y como se tiene en la Figura 2.4.1. Sin embargo, si cambiamos a $\alpha = \frac{1}{3}$, los residuos de $1, 4, 9, 16, 25, 36,...$ modulo 3 son $1, 1, 0, 1, 1, 0, ...$, por lo que nunca aparece el residuo 2, este hueco en la distribución modulo 3 genera que en la suma haya pocas cancelaciones,

$$\begin{aligned} F_{A_2}(\frac{1}{3}, x) &= \sum_{n^2\leq x} e\left(\frac{n^2}{3}\right) = e\left(\frac{1}{3}\right)+e\left(\frac{4}{3}\right)+e\left(\frac{9}{3}\right)+e\left(\frac{16}{3}\right)+e\left(\frac{25}{3}\right))+e\left(\frac{36}{3}\right)+\cdots \\ &= e\left(\frac{1}{3}\right)+e\left(\frac{1}{3}\right)+e\left(\frac{0}{3}\right)+e\left(\frac{1}{3}\right)+e\left(\frac{1}{3}\right)+e\left(\frac{0}{3}\right)+\cdots \\ &= 2e\left(\frac{1}{3}\right)+1+2e\left(\frac{1}{3}\right)+1+\cdots \end{aligned}$$

  siendo entonces un pico, como se observa también en la Figura 2.4.1.

La racionalidad de α es una condición necesaria para la formación de picos (que serán los intervalos a considerar arcos mayores) porque discretiza las direcciones, pero la magnitud del pico está determinada por el sesgo de la distribución de A en las clases de residuos módulo q. Si A se distribuye equitativamente entre todas las clases (como $\mathbb{Z}$), habrá cancelación. Si A evita ciertas clases o se concentra en pocas (como los impares o los cuadrados en ciertos módulos), habrá interferencia constructiva.

Motivados por el análisis anterior, donde identificamos que la interferencia constructiva solo es posible en entornos de racionales con denominador pequeño, adoptamos la siguiente definición clásica para los arcos mayores, que formaliza estas regiones en el caso general:

Definición 2.4.2 (Arcos Mayores y Menores)

Sea $A \subseteq \mathbb{Z}^+$ infinito y sea

$$F_A(\alpha, x) = \sum_{\substack{a \in A \\ a \leq x}} e(\alpha a)$$

su suma exponencial asociada. Sean $Q = Q(x) \to \infty$ y $\delta = \delta(x) \to 0$ funciones positivas. Definimos los **arcos mayores** como

$$\mathfrak{M} = \bigcup_{\substack{1 \leq q \leq Q \\ (a,q)=1}} \mathfrak{M}_{a,q}, \quad \mathfrak{M}_{a,q} := \left\{ \alpha \in [0,1] : \left| \alpha - \frac{a}{q} \right| \leq \delta(x,q) \right\}$$

donde $\delta(x,q)$ es una función que satisface

$$\delta(x,q) \ll \frac{1}{q}(\text{escala natural del problema})$$

El complemento

$$\mathfrak{m} := [0,1] \setminus \mathfrak{M}$$

se denominan **arcos menores.**

La noción de arcos mayores no es intrínseca al conjunto A, sino a la escala de oscilación de la suma exponencial $F_A(\alpha, x)$, es decir, también sera dependiente del numero $x = n$ a representar. La elección concreta del parámetro Q y del tamaño de los arcos depende del problema aritmético considerado, recuperándose como casos particulares la definicion clásica en el problema de Waring, donde $A = A_k$ nos da

$$F_{A_k}(\alpha, n) = \sum_{m \leq X} e(\alpha m^k), \quad X \sim n^{\frac{1}{k}}$$

La contribución principal de esta suma se concentra en los valores de α cercanos a racionales con denominador pequeño, pues si $\alpha = \frac{a}{q} + \beta$, con $(a,q) = 1$, la fase se descompone como $\alpha m^k = \frac{a}{q} m^k + \beta m^k$, permitiendo agrupar la suma en clases módulo q. Para que el término βm^k varíe lentamente y la suma pueda aproximarse mediante una combinación de sumas de Gauss e integrales suaves, es necesario que la fase adicional introducida por β permanezca pequeña en la escala natural de las progresiones módulo q. Al escribir $m = r + ql$, la suma se descompone en clases modulo q y la variación relevante de la fase esta gobernada por $\beta q^k l^k$. Para que esto sea estable cuando $l \leq X/q$, se necesita

que

$$|\beta|\, qX^{k-1} \ll 1$$

lo cual conduce a la condición natural $|\beta| \ll \frac{1}{qX^k}$. En consecuencia, los arcos mayores asociados a Waring son intervalos centrados en fracciones reducidas $\frac{a}{q}$, con $q \leq N$, de tamaño $\asymp \frac{1}{qX^k}$. Dado que $X^k \sim n$ esta elección corresponde a trabajar con una disección de Farey de orden $N \asymp n$, coincidiendo con la definición clásica de Hardy y Littlewood y mostrando que el caso de Waring se recupera como una especialización natural de la definición general de arcos mayores.

Asi el numero de representaciones de n como suma de k elementos de A lo podremos separar de la forma,

$$r_{k,A}(n) = \int_{\mathfrak{M}} F_A^k(\alpha, n) e(-n\alpha) d\alpha + \int_{\mathfrak{m}} F_A^k(\alpha, n) e(-n\alpha) d\alpha$$

donde buscaremos conseguir un termino principal a través de los arcos mayores y un termino de error con magnitud menor en los arcos menores.

Observación. Es importante señalar que la definición del conjunto de arcos mayores $\mathfrak{M}$ identifica únicamente aquellos intervalos del $[0, 1]$ en los que es es posible la alineación de vectores, motivada por la cercanía de α a racionales con denominador pequeño. Sin embargo, el hecho de que un intervalo pertenezca a los arcos mayores no garantiza, por sí mismo, que la suma exponencial $F_A(\alpha, x)$ alcance valores de gran magnitud en dicho intervalo (por ejemplo el caso $\alpha = \frac{1}{2}$ en los cuadrados). El crecimiento efectivo de la suma exponencial depende de manera esencial de la distribución aritmética del conjunto A en las clases de residuos módulo q. En caso de tener una distribución que reduzca las cancelaciones, la restricción a vecindades $\alpha \approx \frac{a}{q}$, permite que la integral sobre $\mathfrak{M}$ proporcione el término principal en la estimación de $r_{k,A}(n)$ y un termino de error sobre $\mathfrak{m}$. Demostrar que esta última es de orden inferior constituye, habitualmente, el desafío analítico central en el método del circulo. Esto también refleja como unicamente aquellos conjuntos que presentan una distribución aritmética significativa en las clases de residuos módulo q pueden explotar dichas regiones para generar una contribución dominante. Este hecho explica por qué el método del círculo resulta especialmente eficaz en problemas aditivos no lineales, como los de Waring y Goldbach, mientras que para conjuntos con comportamiento esencialmente uniforme la disección en arcos mayores y menores no conduce a información sustancial.

En resumen, la formulación moderna del método del círculo presentada en esta sección unifica el tratamiento de los problemas aditivos bajo una sola identidad integral exacta basada en sumas exponenciales finitas:

$$r_{k,A}(n) = \int_{\mathfrak{M}} F_A^k(\alpha, n) e(-n\alpha) d\alpha + \int_{\mathfrak{m}} F_A^k(\alpha, n) e(-n\alpha) d\alpha$$

Observando la transición, desde las series generadoras infinitas hacia las sumas exponenciales truncadas $F_A(\alpha, n)$, notando como fue cambiando la dificultad del problema: de las singularidades en el plano complejo, al estudio de la distribución aritmética de los elementos de A en las clases de residuos módulo q.

Hemos establecido que la eficiencia del método depende críticamente de la dicotomía entre arcos mayores y menores siempre que el conjunto A posea una distribución predecible

en progresiones aritméticas y que la suma exponencial $F_A(\alpha, n)$ exhiba una cancelación suficiente en arcos menores, lo cual ocurre cuando el comportamiento de A es lo bastante "aleatorio".

Apéndice A

Sumas Exponenciales

En este apéndice estudiaremos sumas de la forma

$$\sum_{1\leq m\leq N} e(m\alpha), \quad \text{donde} \quad e(x)=\exp(2\pi i x)$$

y daremos estimaciones para sumas que involucran números irracionales a partir de números racionales suficientemente cercanos.

Consideremos la suma exponencial

$$\sum_{1\leq m\leq N} e(m\alpha)$$

donde $\alpha=\frac{a}{q}$ con $(a,q)=1$. Si $m\equiv r\,(\mathrm{mod}\,q)$ entonces $e(m\alpha)=e(r\alpha)$, pues si escribimos $m=tq+r$ se tiene

$$e(m\alpha)=e\left((tq+r)\frac{a}{q}\right)=e\left(ta+r\frac{a}{q}\right)=e(ta)e\left(r\frac{a}{q}\right)=e(r\alpha)$$

De aquí obtenemos nuestra primera cota elemental. En efecto,

$$\begin{aligned}\sum_{1\leq m\leq N} e(m\alpha) &= \sum_{1\leq m\leq N} e\left(m\frac{a}{q}\right)=\sum_{1\leq r\leq q} e\left(r\frac{a}{q}\right)\cdot \#\left\{1\leq m\leq N : m\equiv r\,(\mathrm{mod}\,q)\right\}\\ &= \sum_{1\leq r\leq q} e\left(r\frac{a}{q}\right)\sum_{\substack{1\leq m\leq N\\ m\equiv r\,(\mathrm{mod}\,q)}} 1\end{aligned}$$

por el algoritmo de la división, escribimos $N=tq+s$ para alguna $t\in\mathbb{Z}^+$ y $1\leq s<q$. Entonces, para un residuo r, los enteros m tales que $1\leq m\leq N$ y $m\equiv r\,(\mathrm{mod}\,q)$ son de la forma $m=r+t'q$, y cumplen que

$$t'q\leq r+t'q\leq N$$

por lo que cualquier entero $t'\leq\frac{N}{q}$ genera un entero $r+t'q$ congruente con r modulo q, y entonces

$$\sum_{\substack{1\leq m\leq N\\ m\equiv r\,(\mathrm{mod}\,q)}} 1=\left\lfloor\frac{N}{q}\right\rfloor+O(1)=\frac{N}{q}+O(1)$$

entonces

$$\sum_{1\leq m\leq N} e(m\alpha) = \sum_{1\leq r\leq q} e\left(r\frac{a}{q}\right)\left[\frac{N}{q}+O(1)\right] = \frac{N}{q}\sum_{1\leq r\leq q} e\left(r\frac{a}{q}\right)+O(q) = O(q)$$

La última igualdad se debe a que la suma de las raíces q-ésimas de la unidad es cero, y por tanto

$$\sum_{1\leq m\leq N} e(m\alpha) = O(q)$$

Esto nos da la intuición que la magnitud de la suma involucrada dependerá unicamente de la representación racional de α y no del tamaño de N, mas en concreto dependerá de su denominador. El problema se vuelve mas interesante si consideramos α un numero irracional, pues veremos que la magnitud de la suma dependerá de la cercanía de α con el entero mas cercano. Es por ello que introduciremos la siguiente notación.

Definición A.0.1

Para cada $\alpha \in \mathbb{R}$ definimos

$$\|\alpha\| := \min\{|n-\alpha| : n \in \mathbb{Z}\}$$

Claramente $0 \leq \|\alpha\| \leq \frac{1}{2}$. Para continuar primero probaremos el siguiente lema de calculo elemental.

Lema A.0.1

Si $0 < \alpha < \frac{1}{2}$, *entonces* $2\alpha < \sin(\pi\alpha) < \pi\alpha$

Demostración. El lado derecho es inmediato pues $\sin(x) < x$ para todo $x \in \mathbb{R}^+$, para el lado izquierdo recordemos que $\sin(\pi x)$ es cóncava en $(0,1)$ por lo que la recta que pasa por el origen y el punto $(\frac{1}{2}, \sin(\frac{\pi}{2})) = (\frac{1}{2}, 1)$ dada por $y = 2x$ queda por debajo de la función en el intervalo $(0, \frac{1}{2})$, es decir, $2x < \sin(\pi x) \underset{\alpha\in(0,1/2)}{\Rightarrow} 2\alpha < \sin(\pi\alpha)$. □

Haremos uso de este lema para obtener una desigualdad clásica para sumas exponenciales sobre un rango finito. Esta desigualdad, debido a Weyl, muestra la dependencia de esta suma con el valor de $\|\alpha\|$.

Lema A.0.2 (Weyl)

Para $\alpha \in \mathbb{R}$,*y enteros* N_1 *y* N_2 *con* $N_1 < N_2$, *tenemos que*

$$\left|\sum_{m=N_1+1}^{N_2} e(\alpha m)\right| \ll \min\left(N_2 - N_1, \frac{1}{\|\alpha\|}\right)$$

donde la constante implícita es absoluta.

Demostración. Tenemos que probar que

$$\left|\sum_{m=N_1+1}^{N_2} e(\alpha m)\right| \ll N_2 - N_1 \quad \text{y} \quad \left|\sum_{m=N_1+1}^{N_2} e(\alpha m)\right| \ll \frac{1}{\|\alpha\|}$$

La primer cota es clara, pues

$$\left|\sum_{m=N_1+1}^{N_2} e(\alpha m)\right| \leq \sum_{m=N_1+1}^{N_2} 1 \leq N_2 - N_1$$

Por otro lado, si $\alpha \in \mathbb{Z}$ tendremos que $\|\alpha\| = 0$, entonces

$$\left|\sum_{m=N_1+1}^{N_2} e(\alpha m)\right| = \left|\sum_{m=N_1+1}^{N_2} 1\right| = N_2 - N_1$$

Ahora supongamos que $0 < \|\alpha\| < 1/2$, en este caso podemos ver a nuestra suma como una geométrica,

$$\begin{aligned}\left|\sum_{m=N_1+1}^{N_2} e(\alpha m)\right| &= \left|\sum_{m=N_1+1}^{N_2} e(\alpha)^m\right| = \left|\frac{e(\alpha)^{N_2+1} - e(\alpha)^{N_1+1}}{e(\alpha)-1}\right| = \left|e(\alpha)^{N_1+1}\frac{e(\alpha)^{N_2-N_1}-1}{e(\alpha)-1}\right| \\ &= \frac{\left|e(\alpha)^{N_2-N_1}-1\right|}{|e(\alpha)-1|} \leq \frac{2}{|e(\alpha)-1|} = \frac{1}{\left|\frac{\exp(2\pi i\alpha)-1}{2}\right|} \\ &= \frac{1}{\left|\exp(-\pi i\alpha)\frac{\exp(2\pi i\alpha)-1}{2}\right|} = \frac{1}{\left|\frac{\exp(\pi i\alpha)-\exp(-\pi i\alpha)}{2i}\right|} = \frac{1}{|\sin(\pi\alpha)|}\end{aligned}$$

Sin embargo, dado que existe $n \in \mathbb{Z}$tal que $\|\alpha\| = |n-\alpha|$tendremos,

$$|\sin(\pi\,\|\alpha\|)| = |\sin(\pm\pi(n-\alpha))| = |\sin(\pi n - \pi\alpha)| = |\pm\sin(\pi\alpha)| = |\sin(\pi\alpha)|$$

lo que implica, usando el Lema A.0.1,

$$\left|\sum_{m=N_1+1}^{N_2} e(\alpha m)\right| = \frac{1}{|\sin(\pi\,\|\alpha\|)|} < \frac{1}{2\,\|\alpha\|} < \frac{1}{\|\alpha\|}$$

□

Este resultado nos da la relación entre las sumas exponenciales con la distancia al entero más cercano, más aún, veremos que dar una buena aproximación de estas sumas dependerá de que tan buena aproximación por racionales demos de α. Para establecer esto veamos un primer resultado aplicando el método de casillas.

Lema A.0.3 (aproximación racional de Dirichlet)

Sean $\alpha, Q \in \mathbb{R}$ con $Q \geq 1$. Entonces existen enteros a, q con $(a,q) = 1$ y $1 \leq q \leq Q$ tales que

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{qQ}$$

Demostración. Consideremos $N = \lfloor Q \rfloor$. Primero probaremos la existencia de enteros a, q con $1 \leq q \leq Q$ que satisfacen la desigualdad, sin imponer la condición $(a,q) = 1$. Notaremos que, al reducir posteriormente la fracción $\frac{a}{q}$ a su forma irreducible, el nuevo denominador no aumenta y por tanto seguirá siendo $\leq Q$.

Consideremos los números

$$\beta_q := \{\alpha q\} = \alpha q - \lfloor \alpha q \rfloor \, , \; q = 1, 2, ..., N$$

por ser la parte fraccionaria, cada uno de estos números vive en $[0, 1)$. Ahora partamos el intervalo en $N + 1$ subintervalos, siendo estos

$$B_r = \left[\frac{r-1}{N+1}, \frac{r}{N+1} \right) \, , \; r = 1, 2, ..., N + 1$$

Si alguno de los números β_q vive en B_1, entonces terminaremos pues esto implicaría que

$$|\alpha q - \lfloor \alpha q \rfloor| \leq \frac{1}{N+1} < \frac{1}{Q}$$

y el resultado se sigue dividiendo ambos lados por q.

Lo mismo pasa si algún β_q vive en B_{N+1}, pues en este caso,

$$|1 - \beta_q| = |1 - (\alpha q - \lfloor \alpha q \rfloor)| = |\alpha q + (\lfloor \alpha q \rfloor - 1)| \leq \frac{1}{N+1} < \frac{1}{Q}$$

y de nuevo se sigue el resultado dividiendo por q. Entonces, supongamos pues que todos los β_q viven en los $N - 1$ intervalos B_r con $r = 2, 3, ..., N$. Pero por el principio de las casillas tenemos que necesariamente debe existir un par β_u y β_v con $1 \leq v \leq u \leq N$ tal que ambos pertenecen al mismo intervalo B_r. Siendo este el caso consideremos $q = u - v$, por lo que

$$|\alpha q - (\lfloor \alpha u \rfloor - \lfloor \alpha v \rfloor)| = |(\alpha u - \lfloor \alpha u \rfloor) - (\alpha v - \lfloor \alpha v \rfloor)| = |B_u - B_v| \leq \frac{1}{N+1} < \frac{1}{Q}$$

y dividiendo por $q = u - v$ obtenemos el resultado. □

En particular el lema anterior implica que, dado números reales α y Q con $Q \geq 1$, uno puede encontrar enteros a y q con $1 \leq q \leq Q$ y $(a, q) = 1$ tales que

$$\left| \alpha - \frac{a}{q} \right| < \frac{1}{q^2}$$

Esto tiene algunas consecuencias interesantes que veremos en los siguientes.

Lema A.0.4

Sean $\alpha \in \mathbb{R}$, y a, q enteros con $q \geq 1$, $(a, q) = 1$. Si

$$\left| \alpha - \frac{a}{q} \right| < \frac{1}{q^2}$$

entonces

$$\sum_{r=1}^{q/2} \frac{1}{\|\alpha r\|} \ll q \log q$$

Demostración. Por hipótesis sabemos que existe $\theta \in [-1,1]$ tal que

$$\alpha - \frac{a}{q} = \frac{\theta}{q^2}$$

entonces para $1 \leq r \leq \frac{q}{2}$

$$\alpha r = \frac{ar}{q} + \frac{\theta r}{q^2}$$

por lo tanto

$$\left|\alpha r - \frac{ar}{q}\right| = \frac{|\theta|\, r}{q^2} \leq \frac{r}{q^2} \leq \frac{1}{2q}$$

Sea N un entero cualquiera. Utilizando la desigualdad triangular inversa para el valor absoluto, podemos escribir:

$$|\alpha r - N| = \left|\left(\frac{ar}{q} - N\right) + \left(\alpha r - \frac{ar}{q}\right)\right| \geq \left|\frac{ar}{q} - N\right| - \left|\alpha r - \frac{ar}{q}\right|$$

por definición, se tiene que $|ar/q - N| \geq \|ar/q\|$ para cualquier $N \in \mathbb{Z}$. Si además consideramos la acotación del término de error $|\alpha r - ar/q| \leq 1/2q$, obtenemos la cota:

$$|\alpha r - N| \geq \left\|\frac{ar}{q}\right\| - \frac{1}{2q}$$

Dado que esta desigualdad es válida para todo $N \in \mathbb{Z}$, debe cumplirse también para aquel entero N_0 que minimiza la distancia $|\alpha r - N_0|$. Por lo tanto, concluimos que:

$$\|\alpha r\| = \min_{N \in \mathbb{Z}} |\alpha r - N| \geq \left\|\frac{ar}{q}\right\| - \frac{1}{2q}$$

con ello obtenemos

$$\sum_{r=1}^{q/2} \frac{1}{\|\alpha r\|} \leq \sum_{r=1}^{q/2} \frac{1}{\left\|\frac{ar}{q}\right\| - \frac{1}{2q}}$$

Ahora, es claro que para cada $1 \leq r \leq \frac{q}{2}$ existe $n_r \in \mathbb{Z}$ tal que

$$\left\|\frac{ar}{q}\right\| = \left|\frac{ar}{q} - n_r\right| = \left|\frac{ar - qn_r}{q}\right| = \frac{|ar - qn_r|}{q} = \frac{s_r}{q}$$

donde $s_r := ar - qn_r$. Como $0 \leq \left\|\frac{ar}{q}\right\| \leq \frac{1}{2} \Rightarrow 0 \leq s_r \leq \frac{q}{2}$.

Notemos que $s_r = 0$ si, y solo si, $r \equiv 0 \,(\mathrm{mod}\, q)$, pero como $1 \leq r \leq \frac{q}{2}$ tendremos pues $s_r \neq 0$. Más aun, para cada $1 \leq r \leq \frac{q}{2}$ tendremos que s_r son todos distintos esto es pues si suponemos que

$$\left\|\frac{\alpha r_1}{q}\right\| = \left\|\frac{\alpha r_2}{q}\right\|$$

entonces existen enteros n_1, n_2 tales que

$$\left|\frac{\alpha r_1}{q} - n_1\right| = \left|\frac{\alpha r_2}{q} - n_2\right| \Rightarrow ar_1 - qn_1 = \pm\,(ar_2 - qn_2)$$

con lo cual $ar_1 \equiv ar_2 \,(\mathrm{mod}\, q)$, pero como $(a,q) = 1$ y $1 \leq r_1, r_2 \leq \frac{q}{2}$ tendremos que

$$r_1 \equiv r_2 \,(\mathrm{mod}\, q) \Rightarrow r_1 = r_2$$

De esta forma

$$\left\{\left\|\frac{ar}{q}\right\| : 1 \leq r \leq \frac{q}{2}\right\} = \left\{\frac{s}{q} : 1 \leq s \leq \frac{q}{2}\right\}$$

por lo tanto,

$$\sum_{r=1}^{q/2} \frac{1}{\|\alpha r\|} \leq \sum_{r=1}^{q/2} \frac{1}{\left\|\frac{\alpha r}{q}\right\| - \frac{1}{2q}} = \sum_{s=1}^{q/2} \frac{1}{\frac{s}{q} - \frac{1}{2q}} = 2q \sum_{s=1}^{q/2} \frac{1}{2s-1} \leq 2q \sum_{s=1}^{q/2} \frac{1}{s} \ll q \log q$$

□

Lema A.0.5

Sean $\alpha \in \mathbb{R}$, y a, q enteros con $q \geq 1$, $(a, q) = 1$. Si

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{q^2}$$

entonces para cualquier número real no negativo v y entero $h \geq 0$, tenemos

$$\sum_{r=1}^{q} \text{mín}\left(v, \frac{1}{\|\alpha(hq+r)\|}\right) \ll v + q \log q$$

Demostración. Comenzaremos estableciendo una cota para la cantidad de términos que caen en intervalos pequeños. Por hipótesis, existe $\theta \in [-1, 1]$ tal que

$$\alpha = \frac{a}{q} + \frac{\theta}{q^2}$$

Para $1 \leq r \leq q$, desarrollamos la expresión:

$$\alpha(hq+r) = \alpha hq + \alpha r = h\left(a + \frac{\theta}{q}\right) + r\left(\frac{a}{q} + \frac{\theta}{q^2}\right) = ah + \frac{ar}{q} + \frac{\theta h}{q} + \frac{\theta r}{q^2}$$

Consideremos la parte fraccionaria $\{x\} = x - \lfloor x \rfloor$. Analizaremos la distribución de los valores $\{\alpha(hq+r)\}$. Notemos que

$$\{\alpha(hq+r)\} = \left\{\frac{ar}{q} + \frac{\theta h}{q} + \frac{\theta r}{q^2}\right\}$$

definimos el término de error $\delta(r)$ y el entero $K = \lfloor \theta h \rfloor$ como sigue:

$$\frac{\theta h}{q} + \frac{\theta r}{q^2} = \frac{\theta h + \theta r/q}{q} = \frac{\lfloor \theta h \rfloor + \{\theta h\} + \theta r/q}{q} = \frac{K + \delta(r)}{q}$$

donde $\delta(r) = \{\theta h\} + \frac{\theta r}{q}$. Dado que $0 \leq \{\theta h\} < 1$, $|\theta| \leq 1$ y $1 \leq r \leq q$, tenemos que

$$-1 \leq \delta(r) < 2$$

Así, para cada r existe un entero k_r tal que

$$\{\alpha(hq+r)\} = \frac{ar + K + \delta(r)}{q} - k_r = \frac{ar - qk_r + K + \delta(r)}{q}$$

Ahora, consideremos un subintervalo $I \subset [0,1)$ de longitud $1/q$, por ejemplo $I = [t, t+1/q]$.

Si$\{\alpha(hq+r)\} \in I$, entonces

$$qt \leq ar - qk_r + K + \delta(r) \leq qt + 1$$

Despejando el término entero $ar - qk_r$, obtenemos

$$qt - K - \delta(r) \leq ar - qk_r \leq qt - K - \delta(r) + 1$$

Debido a que $-1 \leq \delta(r) < 2$, el termino $ar - qk_r$ esta contenido a un intervalo de longitud a lo mas $1 - (-1) + 2 = 4$. Es decir, los valores enteros de la forma $ar - qk_r$ deben pertenecer a un intervalo abierto de longitud 4. Por otro lado notemos que si tenemos dos indices distintos $1 \leq r_1 < r_2 \leq q$ tales que

$$ar_1 - qk_{r_1} = ar_2 - qk_{r_2}$$

entonces $ar_1 \equiv ar_2 \pmod{q}$. Como $(a,q) = 1$, esto implica que $r_1 \equiv r_2 \pmod{q}$, y por tanto $r_1 = r_2$. Por lo tanto, todos los enteros de la forma $ar - qk_r$ son distintos para cada r.

Dado que un intervalo de longitud 4 contiene a lo más 4 enteros distintos, concluimos que para cualquier t, existen a lo más 4 valores de $r \in [1,q]$ tales que $\{\alpha(hq+r)\} \in [t, t+1/q]$.

Finalmente, regresando a la distancia al entero más cercano, notemos que $||\alpha(hq+r)|| \in [0, 1/2]$. La condición

$$||\alpha(hq+r)|| \in J(s) := \left[\frac{s}{q}, \frac{s+1}{q}\right)$$

implica que la parte fraccionaria satisface

$$\{\alpha(hq+r)\} \in \left[\frac{s}{q}, \frac{s+1}{q}\right) \quad \text{o} \quad \{\alpha(hq+r)\} \in \left(1 - \frac{s+1}{q}, 1 - \frac{s}{q}\right].$$

Como cada una de estas condiciones corresponde a un intervalo de longitud $1/q$, por lo demostrado anteriormente, hay a lo más 4 soluciones para cada posible caso. Por lo tanto, existen a lo más 8 valores de $r \in [1,q]$ tales que $||\alpha(hq+r)|| \in J(s)$.

Apliquemos este hecho para estimar la suma

$$\sum_{r=1}^{q} \text{mín}\left(v, \frac{1}{\|\alpha(hq+r)\|}\right)$$

Si $\|\alpha(hq+r)\| \in J(0) = [0, \frac{1}{q}]$,entonces usamos la desigualdad

$$\text{mín}\left(v, \frac{1}{\|\alpha(hq+r)\|}\right) \leq v$$

Si $\|\alpha(hq+r)\| \in J(s)$ para algún $s \geq 1$, entonces usamos la desigualdad

$$\text{mín}\left(v, \frac{1}{\|\alpha(hq+r)\|}\right) \leq \frac{1}{\|\alpha(hq+r)\|} \leq \frac{q}{s}$$

Dado que $\|\alpha(hq+r)\| \in J(s)$ para algún $s < \frac{q}{2}$, se sigue que

$$\sum_{r=1}^{q} \text{mín}\left(v, \frac{1}{\|\alpha(hq+r)\|}\right) \leq 8v + 8\sum_{r=1}^{q} \frac{q}{s} \ll v + q\log q$$

□

EL siguiente lema es de suma importancia en el teorema de Vinogradov.

Proposición A.0.1

Sea $\alpha \in \mathbb{R}$ tal que

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{q^2}$$

para algún racional $\frac{a}{q}$ donde $q \geq 1$ y $(a,q) = 1$. Entonces, para cualquier numero real $X \geq 1$, se tiene

$$\sum_{0\leq m\leq X} \text{mín}\left(\frac{n}{m}, \frac{1}{\|m\alpha\|}\right) \ll \left(\frac{n}{q} + X + q\right)\log(2qX)$$

Demostración. Sabemos que para cada $0 \leq m \leq X$ existe un único $1 \leq r \leq q$ tal que $m \equiv r \pmod q$, es decir, $m = hq + r$ con $0 \leq h \leq {}^{X}/_{q}$y $1 \leq r \leq q$, por lo que

$$\sum_{0\leq m\leq X} \text{mín}\left(\frac{n}{m}, \frac{1}{\|m\alpha\|}\right) \leq \sum_{0\leq h\leq {}^{X}/_{q}} \sum_{1\leq r\leq q} \text{mín}\left(\frac{n}{hq+r}, \frac{1}{\|\alpha(hq+r)\|}\right)$$

ahora, para $h = 0$ la suma interior es

$$\sum_{1\leq r\leq q} \text{mín}\left(\frac{n}{r}, \frac{1}{\|\alpha r\|}\right) = \sum_{1\leq r\leq q/2} \text{mín}\left(\frac{n}{r}, \frac{1}{\|\alpha r\|}\right) + \sum_{q/2<r\leq q} \text{mín}\left(\frac{n}{r}, \frac{1}{\|\alpha r\|}\right)$$

para el primer sumando, por el **Lema A.0.4**

$$\sum_{1\leq r\leq q/2} \text{mín}\left(\frac{n}{r}, \frac{1}{\|\alpha r\|}\right) \leq \sum_{1\leq r\leq q/2} \frac{1}{\|\alpha r\|} \ll q\log q$$

para el segundo sumando, tenemos

$$hq + r = r > \frac{q}{2} = \frac{(h+1)q}{2}$$

por lo que

$$\sum_{q/2<r\leq q} \text{mín}\left(\frac{n}{r}, \frac{1}{\|\alpha r\|}\right) = \sum_{q/2<r\leq q} \text{mín}\left(\frac{n}{hq+r}, \frac{1}{\|\alpha(hq+r)\|}\right) \ll \sum_{q/2<r\leq q} \text{mín}\left(\frac{n}{(h+1)q}, \frac{1}{\|\alpha(hq+r)\|}\right)$$

Por otro lado, si $h \geq 1$ entonces

$$hq + r > hq \geq \frac{(h+1)q}{2}$$

así, por todo lo anterior

$$\sum_{0\leq m\leq X} \text{mín}\left(\frac{n}{m}, \frac{1}{\|m\alpha\|}\right) \ll q\log q + \sum_{0\leq h\leq {}^{X}/_{q}} \sum_{1\leq r\leq q} \text{mín}\left(\frac{n}{(h+1)q}, \frac{1}{\|\alpha(hq+r)\|}\right)$$

y usando el **Lema A.0.5** con $v = {}^{n}/_{(h+1)q}$ en la suma interior obtenemos

$$\begin{aligned}\sum_{0\le m\le X} \text{mín}\left(\frac{n}{m}, \frac{1}{\|m\alpha\|}\right) &\ll q\log q + \sum_{0\le h\le {}^{X}/_{q}} \left(\frac{n}{(h+1)q} + q\log q\right)\\ &\ll q\log q + \left(\sum_{0\le h\le {}^{X}/_{q}} \frac{n}{(h+1)q}\right) + \sum_{0\le h\le {}^{X}/_{q}} q\log q\\ &\ll q\log q + \frac{n}{q}\left(\sum_{0\le h\le {}^{X}/_{q}} \frac{1}{h+1}\right) + \left(\frac{X}{q}+1\right) q\log q\\ &\ll 2q\log q + \frac{n}{q}\log\left(\frac{X}{q}+1\right) + X\log q\end{aligned}$$

y finalmente, notamos que

$$\begin{aligned}2\log q &\ll \log(2qX)\\ \frac{X}{q} + 1 &\le X + q \le 2qX\end{aligned}$$

lo cual es válido para todo $q \ge 1$. En consecuencia:

$$\sum_{0\le m\le X} \text{mín}\left(\frac{n}{m}, \frac{1}{\|m\alpha\|}\right) \ll q\log(2qX) + \frac{n}{q}\log(2qX) + X\log(2qX) = \left(\frac{n}{q} + X + q\right)\log(2qX)$$

□

Otra desigualdad importante en las sumas exponenciales es la desigualdad de Hua, la cual proporciona un control efectivo de momentos altos de la suma exponencial asociada a las potencias k-ésimas. En el método del círculo, este resultado es esencial para estimar la contribución de los arcos menores, permitiendo obtener decaimiento suficiente siempre que el número de sumandos s sea suficientemente grande. En combinación con el Lema de Weyl, constituye la herramienta analítica central para el tratamiento del Problema de Waring. Para los intereses de esta tesis unicamente colocaremos su enunciado.

Lema A.0.6 Desigualdad de Hua

Sea $k \ge 2$ un entero fijo y sea

$$g(\alpha) = \sum_{1\le m\le X} e\left(\alpha m^k\right)$$

Entonces, para todo $\varepsilon > 0$, se tiene

$$\int_0^1 |g(\alpha)|^{2^k} d\alpha \ll X^{2^k - k + \varepsilon}.$$

La constante implícita depende únicamente de k y de ε.

Apéndice B

Sumas de Ramanujan

En este apéndice veremos propiedades básicas sobre las llamadas "Sumas de Ramanujan" las cuales serán un paso crucial en la prueba del teorema de Vinográdov.

Definición B.0.1

Para cualesquiera $n, q \in \mathbb{N}$ se define la suma de Ramanujan en n y q como

$$c_q(n) := \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e\left(\frac{an}{q}\right) \quad \text{donde} \quad e(x) = \exp(2\pi i x)$$

Veremos que esta función es multiplicativa y con ello daremos una expresión en términos de la función de Möbius y la función φ de Euler. Para esto recordemos los hechos básicos de la **convolución de Dirichlet**. Para un análisis completamente detallado revisar [20].

Definición B.0.2

Sean $F, G : \mathbb{Z}^+ \to \mathbb{C}$ funciones aritméticas. Se define la **convolución de Dirichlet** de F y G como la función aritmética

$$(F * G)(n) := \sum_{d|n} F(d) G\left(\frac{n}{d}\right)$$

Observación. El conjunto de todas las funciones aritméticas $F : \mathbb{Z}^+ \to \mathbb{C}$, provisto de la suma de funciones y de la convolución de Dirichlet, forma un anillo conmutativo. En particular, la convolución de Dirichlet es conmutativa, es decir,$F * G = G * F$. El elemento identidad para la convolución es la función ε, definida por $\varepsilon(1) = 1$ y $\varepsilon(n) = 0$ para $n > 1$.

El resultado mas celebre respecto a la convolución es la respectiva formula de inversión.

Teorema B.0.1 (Formula de inversión de Möbius)

Sean $F, G : \mathbb{Z}^+ \to \mathbb{C}$ funciones aritméticas. Entonces

$$F = 1 * G \iff G = F * \mu$$

donde $1(n) = 1$ para todo n. En particular la función de Möbius es el inverso de 1 respecto a la convolución de Dirichlet:

$$1 * \mu = \varepsilon$$

Con esto podemos probar el siguiente lema que nos ayudara en las propiedades elementales de las sumas de Ramanujan.

Lema B.0.1

Sea $f : \mathbb{Q} \to \mathbb{C}$ y sean, $F, G : \mathbb{Z}^+ \to \mathbb{C}$ definidas por:

$$F(n) := \sum_{k=1}^{n} f\left(\frac{k}{n}\right) \quad y \quad G(n) := \sum_{\substack{k=1 \\ (k,n)=1}}^{n} f\left(\frac{k}{n}\right)$$

entonces

$$F = 1 * G$$

donde $1(n) = 1$ para todo n. En particular

$$G = F * \mu$$

Demostración. Reescribiendo la función F,

$$F(n) = \sum_{k=1}^{n} f\left(\frac{k}{n}\right) = \sum_{d|n} \sum_{\substack{k=1 \\ (k,n)=d}}^{n} f\left(\frac{k}{n}\right)$$

Agrupamos los términos según el máximo común divisor $d = (k, n)$. Para cada divisor $d \mid n$, consideramos aquellos k con $1 \leq k \leq n$ tales que $(k, n) = d$, de modo que

$$F(n) = \sum_{d|n} \sum_{\substack{k=1 \\ (k,n)=d}}^{n} f\left(\frac{k}{n}\right)$$

Si $(k, n) = d$, podemos escribir $k = md$ con $1 \leq m \leq \frac{n}{d}$ y $(m, \frac{n}{d}) = 1$. Con este cambio de variable se obtiene

$$F(n) = \sum_{d|n} \sum_{\substack{m=1 \\ (m,n/d)=1}}^{n/d} f\left(\frac{m}{(n/d)}\right) = \sum_{d|n} G\left(\frac{n}{d}\right) = (1 * G)(n)$$

por lo tanto, aplicando la fórmula de inversión de Möbius a esta identidad, se concluye que $G = F * \mu$. □

Corolario B.0.1

La suma de Ramanujan $c_q(n)$ es multiplicativa en la variable q y, ademas

$$c_q(n) = \sum_{d|(n,q)} \mu(\frac{q}{d})d$$

en particular, si $(q,n) = 1$ entonces $c_q(n) = \mu(q)$,

Demostración. La primer parte es inmediata, pues por el **Lema B.0.1**

$$c_q(n) = (F * \mu)(n)$$

donde

$$F(q) = \sum_{a=1}^{q} e(\frac{an}{q}) = \begin{cases} q & \text{si } q \mid n \\ 0 & \text{si } q \nmid n \end{cases}$$

la cual es una función multiplicativa en q y, dado que la funciona de Möbius también lo es, tendremos pues que $c_q(n)$ es multiplicativa. Por otro lado

$$c_q(n) = (F * \mu)(n) = \sum_{d|q} \mu(\frac{q}{d})F(d) = \sum_{d|q \text{ y } d|n} \mu(\frac{q}{d})d = \sum_{d|(n,q)} \mu(\frac{q}{d})d$$

□

Proposición B.0.1

La suma de Ramanujan puede expresarse en la siguiente forma:

$$c_q(n) = \frac{\mu(q\,')\varphi(q)}{\varphi(q\,')} \quad con\, q\,' = \frac{q}{(n,q)}$$

Demostración. Por el **Corolario B.0.1** tenemos

$$c_q(n) = \sum_{d|(n,q)} \mu(\frac{q}{d})d$$

Sea $g = (n,q)$ y escribamos $q = q'g$, donde $q' = \frac{q}{g}$, entonces $\frac{q}{d} = q'\frac{g}{d}$, por lo que en la suma podemos hacer el cambio de variable $d = \frac{g}{c}$ con $c \mid g$, obteniendo

$$c_q(n) = \sum_{c|g} \mu(q'c)\frac{g}{c}$$

Note que si $(q',c) > 1$, existirá un primo p tal que $p \mid q'$ y $p \mid c$, entonces $p^2 \mid q'c$, lo implica que $\mu(q'c) = 0$, por lo tanto, la suma sera unicamente para aquellos $(q',c) = 1$, lo que permite separar la función multiplicativa: $\mu(q'c) = \mu(q')\mu(c)$. Siendo,

$$c_q(n) = \sum_{c|g} \mu(q'c)\frac{g}{c} = \sum_{\substack{c|g \\ (q\,',c)=1}} \mu(q\,')\mu(c)\frac{g}{c} = \mu(q\,')g \sum_{\substack{c|g \\ (q\,',c)=1}} \frac{\mu(c)}{c}$$

la suma es multiplicativa, y puede escribirse como un producto sobre primos,

$$\sum_{\substack{c|(n,q)\\(q',c)=1}} \frac{\mu(c)}{c} = \prod_{\substack{p|g\\(q',p)=1}} \left(1-\frac{1}{p}\right) = \prod_{\substack{p|g\\p\nmid q'}} \left(1-\frac{1}{p}\right)$$

este ultimo paso se da pues, $p \mid q \,\mathrm{y}\, p\nmid q' \;\Leftrightarrow\; p \mid (n,q) \,\mathrm{y}\, p\nmid q'$. Ademas notemos que los primos que dividen a g y no dividen a q' son exactamente los primos que dividen a q y no dividen a q', por lo tanto

$$\sum_{\substack{c|(n,q)\\(q',c)=1}} \frac{\mu(c)}{c} = \prod_{\substack{p|q\\p\nmid q'}} \left(1-\frac{1}{p}\right) = \frac{\prod\limits_{p|q}\left(1-\frac{1}{p}\right)}{\prod\limits_{p|q'}\left(1-\frac{1}{p}\right)}$$

usando la identidad conocida

$$\varphi(m) = m\prod_{p|m}\left(1-\frac{1}{p}\right)$$

obtenemos finalmente que

$$c_q(n) = \mu(q')g\frac{\prod\limits_{p|q}\left(1-\frac{1}{p}\right)}{\prod\limits_{p|q'}\left(1-\frac{1}{p}\right)} = \mu(q')\frac{q\prod\limits_{p|q}\left(1-\frac{1}{p}\right)}{q'\prod\limits_{p|q'}\left(1-\frac{1}{p}\right)} = \frac{\mu(q')\varphi(q)}{\varphi(q')}$$

□

Bibliografía

[1] Murty, M. R., & Sinha, K. (2023). *An introduction to the circle method*. American Mathematical Society.

[2] Hardy, G. H., & Ramanujan, S. (1918). Asymptotic formulae in combinatory analysis. *Proceedings of the London Mathematical Society*, s2-17(1), 75–115.

[3] Hardy, G. H., & Littlewood, J. E. (1922). Some problems of Partitio Numerorum. IV. The singular series in Waring's problem and the value of the number G(k). *Mathematische Zeitschrift*, 12(1), 161–188.

[4] Chamizo, F., Cristóbal, E., & Ubis, A. (2006). El método del círculo. *La Gaceta de la RSME*, 9(2), 465–481.

[5] Zaccagnini, A. (2005). *Introduction to the circle method of Hardy, Ramanujan and Littlewood*. Harish-Chandra Research Institute.

[6] Vinogradov, I. M. (2004). *Method of trigonometrical sums in the theory of numbers*. Dover Publications.

[7] Vaughan, R. C. (1997). *The Hardy-Littlewood Method* (2ed). Cambridge University Press.

[8] Jorge, J. U. (2023). *El método del círculo y el teorema de Vinográdov*. Seminario impartido, Facultad de Ciencias.

[9] Nathanson, M. B. (1996). *Additive number theory: The classical bases*. Springer.

[10] Andrews, G. E. (1976). *The theory of partitions. Addison-Wesley.*

[11] MacMahon, P. A. (1915). *Combinatory analysis* (Vols. I–II). Cambridge University Press.

[12] Kanigel, R. (1991). *The man who knew infinity: A life of the genius Ramanujan*. Scribner

[13] Berndt, B. C., & Rankin, R. A. (1995). *Ramanujan: Letters and commentary*. American Mathematical Society & London Mathematical Society.

[14] Hardy, G. H. (2017). *A mathematician's apology*. Cambridge University Press.

[15] Andrews, G. E. (1976). *The Theory of Partitions*. Addison-Wesley.

[16] Petrow, I. N. (2008). *Vinogradov's Three Primes Theorem*. (Doctoral dissertation, University of Cambridge).

[17] DeSalvo, S. (2021). Will the real Hardy-Ramanujan formula please stand up? *INTEGERS: Electronic Journal of Combinatorial Number Theory*, 21(A88)

[18] Murty, M. Ram. (2013). The Partition Function Revisited. En *The Legacy of Srinivasa Ramanujan* (RMS-Lecture Notes Series, No. 20, pp. 261–279). Roma: RMS

[19] Ahlfors, L. V. (1979). *Complex analysis: An introduction to the theory of analytic functions of one complex variable* (3rd ed.). McGraw-Hill.

[20] Apostol, T. M. (1976). *Introduction to Analytic Number Theory*. Springer-Verlag.

[21] Rademacher, H. (1937). On the Partition Function $p(n)$. *Proceedings of the London Mathematical Society.*

[22] Hardy, G. H., & Littlewood, J. E. (1922). Some problems of *Partitio Numerorum: IV. The singular series in Waring's problem and the value of the number* $G(k)$. Mathematische Zeitschrift, 12(1), 161–188.

[23] Conway, J. B. (1978). *Functions of One Complex Variable I* (2nd ed.). Springer.

[24] Meinardus, G. (1954). Asymptotische Aussagen über Partitionen. *Mathematische Zeitschrift*, 59, 388–398

[25] Karatsuba, A. A. (1985). Ivan Matveevich Vinogradov (on the ninety-fifth anniversary of his birth). *Russian Mathematical Surveys.*