Capítulo 4

El método del círculo

4.1. Arcos mayores y menores

En 1918 Hardy y Ramanujan [Ha-Ra] introdujeron una técnica analítica muy poderosa, denominada actualmente *método del círculo*, para tratar problemas aditivos. Su propósito inicial fue el estudio de las particiones pero Hardy y Littlewood desarrollaron la técnica en una serie artículos aplicándola a diversos problemas, por ello el método del círculo también es conocido como *método de Hardy y Littlewood*.

Para fijar ideas nos centraremos en el problema consistente en dar una aproximación asintótica del número de representaciones, $r_k(N)$, de un número grande N como suma de k elementos de un conjunto $\mathcal{B}$ de enteros no negativos. Es decir, se busca una fórmula asintótica para

$$r_k(N) = \#\{(b_1, b_2, \ldots, b_k) \in \mathcal{B}^k \ : \ N = b_1 + b_2 + \cdots + b_k\}.$$

Se comienza construyendo la función generatriz de $r_k(n)$

$$F(z) = \sum_{b \in \mathcal{B}} z^b \qquad \Rightarrow \qquad F^k(z) = \sum_{n=0}^{\infty} r_k(n) z^n.$$

El radio de convergencia de F es 1, por tanto la aplicación de la fórmula integral de Cauchy

$$r_k(N) = \frac{1}{2\pi i} \int_{C_r} F^k(z) \frac{dz}{z^{N+1}} \tag{4.1}$$

es correcta si C_r es la circunferencia $\{|z| = r\}$ con $0 < r < 1$.

A partir de (4.1), como es habitual en teoría analítica de números, se intenta obtener información a partir de las singularidades el problema es que la única singularidad encerrada por C_r es el polo $z = 0$ que no podemos aprovechar porque hallar su residuo es tanto como calcular $r_k(N)$ y volvemos al problema inicial. Por otra parte, típicamente no tiene sentido extender C_r más allá en busca de nuevas singularidades porque fuera del círculo $|z| < 1$ no hay función, en el lenguaje de la variable compleja se dice que la circunferencia unidad es la frontera natural [Ru].

A efectos de tener no sólo un círculo sino también un método, se elige r muy cercano a 1 buscando sentir la influencia de las "principales singularidades" de F en la circunferencia unidad. Por otra parte r debe estar suficientemente separado de 1 como para que no haya "interferencias" entre las influencias de diferentes singularidades. El tamaño de r está en realidad relacionado con el de N, siendo la elección natural (si $r_k(N)$ no crece desmesuradamente rápido) tomar $1-r$ comparable a $1/N$. En este caso r^n es muy pequeño justamente cuando n es mucho mayor que N, de modo que en la definición de $F(z)$ los términos con b mucho mayor que N son despreciables, lo que concuerda con el hecho de que $N = b_1 + b_2 + \cdots + b_k \Rightarrow b_i \leq N$. Es decir, como los $b \in \mathcal{B}$ grandes en comparación con N no afectan a la definición de $r_k(N)$, tampoco deben ser relevantes en el comportamiento asintótico de F.

Para cuantificar la influencia de las singularidades se divide la circunferencia C_r en los llamados *arcos mayores* y *arcos menores*. Los primeros serán aquellos arcos en los que se pueden dar buenas aproximaciones de F, gracias a la cercanía de grandes singularidades, mientras que en los segundos nos tendremos que contentar con una cota superior. Para que el método funcione, la contribución de los arcos mayores debe ser de orden superior que la de los arcos menores, con ello se conseguirá una fórmula asintótica para $r_k(N)$. Esto no implica que la medida de los arcos mayores sea más grande que la de sus hermanos menores, antes bien, en la mayoría de las aplicaciones la medida de los arcos mayores tiende a cero cuando $N \to \infty$ pero en ese conjunto esquelético está la mayor contribución.

Las potencias $\{z^n\}_{n=1}^{\infty}$ "resuenan" cuando $z = r\ e(a/b)$ siendo la resonancia más notoria cuanto menor sea b, por ello los arcos mayores están naturalmente centrados en puntos cuyo argumento es un múltiplo racional de 2π con denominador pequeño. El análisis de F cerca de puntos de este tipo lleva al estudio de la distribución de los elementos de $\mathcal{B}$ en progresiones aritméticas. Por ejemplo, si $\#\mathcal{B} \cap [0, N] \sim CN$ y todos los elementos de $\mathcal{B}$ son impares, sumando por partes se puede obtener $F(r) \sim -F(-r) \sim C(1-r)^{-1}$ cuando $r \to 1^-$, y si todos son de la forma $3n+1$, $F(re(1/3)) \sim Ce(1/3)(1-r)^{-1}$. Sin embargo si hubiera tantos pares como impares, por ejemplo si $2n \in \mathcal{B} \Rightarrow 2n+1 \in \mathcal{B}$, entonces $F(-r) = O(1)$ y en las cercanías de -1 no tendríamos un arco mayor. De esta forma, el método del círculo llega a funcionar en ocasiones como una forma analítica cuantitativa de un principio local-global que transforma resultados módulo q (locales) en resultados en $\mathbb{Z}$ (globales). La misma filosofía apareció al estudiar los métodos de criba, si se conocía la distribución de los elementos de un conjunto en progresiones aritméticas se podía decir algo de su distribución en $\mathbb{Z}$. El método del círculo aspira a resultados más poderosos: fórmulas asintóticas más que acotaciones, y por ello hay que disponer de una información de mayor entidad.

En algunas de las primeras aplicaciones del método del círculo, F tenía propiedades muy específicas que no heredaban sus sumas parciales (propiedades de autoemejanza dadas por relaciones modulares). Sin embargo, en general, trabajar con series infinitas puede conllevar algunas incomodidades técnicas que se evitan con una formulación ligeramente distinta del método del círculo, cronológicamente posterior. Está basada en la sencilla observación, antes comentada, de que $N = b_1 + b_2 + \cdots + b_k \Rightarrow b_i \leq N$. Por

tanto en (4.1), se puede reemplazar F por F_N, la suma parcial de la serie que define F correspondiente a los $b \leq N$. Como F_N es un polinomio, no hay problemas para escoger $r = 1$, lo que con el cambio $z = e(x)$ transforma (4.1) en la sencilla igualdad:

$$r_k(N) = \int_I S^k(x)\, e(-Nx)\, dx \qquad \text{con} \quad S(x) = \sum_{b \in \mathcal{B}_N} e(bx) \tag{4.2}$$

donde I es cualquier intervalo de longitud uno, digamos por ejemplo $I = [-1/2, 1/2]$, y $\mathcal{B}_N = \mathcal{B} \cap [0, N]$. Los arcos mayores serán ahora subintervalos de $[-1/2, 1/2]$ en los que tengamos una buena aproximación para $S(x)$ que se traduzca en otra para la integral correspondiente sobre ellos; mientras que en el resto, los arcos menores, confiamos en que acotaciones de la suma trigonométrica $S(x)$ sean suficientes para acumular su contribución en un témino de error. Por el análisis anterior, los arcos mayores serán intervalos alrededor de ciertos racionales con denominador pequeño.

Sólo para ilustrar un poco la estructura del método, supongamos que nos empeñamos en aproximar con el método del círculo

$$r_k(N) = \#\{(n_1, n_2, \ldots, n_k) \in \mathbb{N}^k \ : \ N = n_1 + n_2 + \cdots + n_k\}$$

para $k \geq 2$. Esto es un objetivo ridículo porque es fácil probar directamente la fórmula

$$r_k(N) = \left(\begin{array}{c} N-1 \\ k-1 \end{array} \right)$$

Si no nos arredramos, en las formulaciones (4.1) y (4.2) se ha de escoger respectivamente

$$F(z) = z + z^2 + z^3 + \cdots = \frac{z}{1-z} \qquad \text{y} \qquad S(x) = \sum_{n=1}^{N} e(nx) = \frac{e(Nx) - 1}{1 - e(-x)}.$$

En el arco del círculo de radio $r = 1 - 1/N$ y argumento $|\arg(z)| \ll 1/N$, la función F es como N y se hace pequeña cuando nos alejamos de este arco. De la misma forma, la suma $S(x)$ es como N si $|x| \ll 1/N$ y es pequeña cuando estamos lejos de este intervalo (siempre dentro de $[-1/2, 1/2]$). En ambos casos hay un "arco mayor" asociado a $0/1$ (a través del argumento en el primer caso y a través del propio valor de la variable en el segundo) de donde proviene la parte del león de $r_k(N)$, y tanto (4.1) como (4.2) hacen sospechar $r_k(N) \sim CN^{k-1}$. Concretando matemáticamente las imprecisiones semánticas disfrazadas en "es como" y "lejos" se puede llegar a la fórmula asintótica (cf. [Cr] §2)

$$r_k(N) \sim \frac{N^{k-1}}{(k-1)!}$$

que está de acuerdo con la expresión exacta.

4.2. Las conjeturas de Goldbach

Nuestro objetivo, por supuesto no son las tonterías recién comentadas, sino enfrentarnos a los grandes problemas aditivos. Uno de los más conocidos es la llamada *Conjetura*

de Goldbach que debe su nombre a que esencialmente fue planteada por C. Goldbach en una carta a Euler:

Conjetura de Goldbach: *Todo número par mayor que* 2 *se puede escribir como suma de dos primos.*

Aunque ésta sea la conjetura de Goldbach por antonomasia, al mismo autor se debe otra conjetura más débil pero de enunciado igualmente simple[1].

Conjetura de Goldbach ternaria: *Todo número impar mayor que* 5 *se puede escribir como suma de tres primos.*

Los apelativos de "conjetura" ya nos hace sospechar que por mucho que el lector escudriñe en la literatura no encontrará el gran teorema que las pruebe. Lo cierto es que el método del círculo tiene algo que decir y produce algunos resultados parciales de interés, en particular la forma ternaria de la conjetura de Goldbach está resuelta salvo un número finitio de casos (inalcanzables por cualquier ordenador imaginable).

Para empezar veamos rápidamente cómo el método del círculo nos puede dar con poco esfuerzo una gran intuición incluso cuando no funciona.

Al aplicarlo a la conjetura de Goldbach, con la formulación de (4.2), se tiene

$$r_2(N) = \int_0^1 (S(x))^2 e(-Nx)\, dx \qquad \text{con} \qquad S(x) = \sum_{p \le N} e(px).$$

La "densidad" de los primos hasta N es $\pi(N)/N \sim 1/\log N$, con lo cual muy cerca de $x = 0$ se debería cumplir algo así como (??)

$$S(x) \sim \frac{D(x)}{\log N} \qquad \text{con} \qquad D(x) = \sum_{n \le N} e(nx).$$

Por otro lado, muy cerca por ejemplo de $x = 1/2$, la aproximación debe ser

$$S(x) \sim -\frac{D(x - 1/2)}{\log N}$$

simplemente porque todos los primos, excepto $p = 2$, son impares y por tanto $e(px) = -e(p(x-1/2))$. Si $x = 1/3$, debemos considerar el hecho de que $e(p/3)$ es $e(1/3)$ ó $e(2/3)$ dependiendo de si $p \equiv 1\ (3)$ o $p \equiv 2\ (3)$. Como la "mitad" de los primos es de cada uno de estos dos tipos,

$$S(x) \sim \left(\frac{e(1/3)}{2 \log N} + \frac{e(2/3)}{2 \log N} \right) D(x - 1/3) = -\frac{D(x - 1/3)}{2 \log N}.$$

[1]En realidad en ambos casos las conjeturas están ligeramente reformuladas con respecto al original porque en tiempos de Goldbach y Euler se consideraba que 1 era primo.

En general, el teorema de los números primos en progresiones aritméticas asegura que los primos están equidistribuidos en cada una de las $\phi(q)$ progresiones aritméticas módulo q que contienen infinitos primos y según el Lema 4.2.5 que probaremos más adelante, $\sum_{(n,q)=1} e(n/q) = \mu(q)$; por todo esto se espera (y de hecho se prueba) que muy cerca de la fracción irreducible $x = a/q$ se cumple

$$S(x) = \frac{\mu(q)}{q \log N} D(x - a/q) + \text{ términos de error.}$$

Como veremos, la prueba de verdad consiste nada más en sumar por partes empleando el teorema de los números primos en progresiones aritméticas (véase la Proposición 4.2.4). Los pocos conocimientos que se tienen en la dirección de la hipótesis de Riemann generalizada se reflejan en que realmente el término de error no se *come* al principal sólo cuando q es muy pequeño (como un logaritmo de N) y x está realmente muy cerca de a/q.

La función $D(x)$ es pequeña si x no está próxima a un entero, lo que sugiere que no se pierde mucho aproximando $\int_{|x|<\epsilon} (D(x))^2 e(-Nx)\ dx$ por $\int_0^1 (D(x))^2 e(-Nx)\ dx$. Teniendo esto en cuenta, la parte principal de la contribución de los arcos mayores es

$$\sum_{(a,q)=1} \frac{\mu(q)}{q^2 (\log N)^2} e(-Na/q) \int_0^1 (D(x))^2 e(-Nx)\ dx \sim \sum_q \frac{\mu(q)}{q^2 (\log N)^2} c_q(-N) N$$

donde $c_q(-N)$ es como se indica en el Lema 4.2.5 y usando la evaluación allí indicada, no es difícil escribir esta suma de funciones multiplicativas como el producto

$$\frac{N}{(\log N)^2} \prod_{p \not| N} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p|N} \left(1 + \frac{1}{p-1}\right).$$

Si podemos justificar todos los argumentos anteriores y que la contribución de los arcos mayores es dominante haciendo honor a su nombre, entonces habremos probado la conjetura de Goldbach, porque para N par el producto anterior no se anula. Demasiado bueno para ser cierto...

El fallo no está en los pasos anteriores, que son incondicionalmente ciertos, sino en la imposibilidad de probar que la contribución de los arcos menores es pequeña. Además esta imposibilidad es teórica, es más una limitación del método que un reflejo de nuestra ignorancia sobre el conjunto de primos. Una explicación poco precisa de esta afirmación pasa por notar que si $x \notin \mathbb{Q}$, las oscilaciones $e(px)$ no tienen ninguna razón por la deban resonar, es lógico pensar que no difieren mucho de variables aleatorias independientes aunque realmente no lo son). Por el teorema central del límite entonces la parte real e imaginaria de $S(x)/\pi(x)$ cuando N crece se deberían comportan como una distribución normal lo que hace sospechar que no se puede mejorar la acotación $S(x) \ll N^{1/2+\epsilon}$ y como los arcos menores tienen casi toda la medida (hay "pocos" números cerca de los racionales) la integral de $|S(x)|^2$ sobre los arcos menores ya supera al término principal. ¿No significa eso que es imposible que la contribución heurística de los arcos mayores que hemos hallado antes sea correcta? De ningún modo, porque al estimar la contribución de

los arcos menores mediante una cota superior estamos perdiendo el signo, es plausible que al integrar $S^2(x)e(-Nx)$ y sumar en los arcos menores haya mucha cancelación.

Este razonamiento también se aplica en general al aproximar $r_2(N)$ cuando, hablando sin rigor, $\mathcal{B}$ tiene densidad positiva en $\mathbb{N}$ o si la densidad decae menos que $N^{-\epsilon}$ para cualquier $\epsilon > 0$. Esta idea se puede resumir en la frase: *El método del círculo no se aplica a problemas binarios*. Lo cual deja fuera del alcance del método del círculo la Conjetura de Goldbach y otros problemas como el número de representaciones $N = x_1^{2k} + \cdots + x_{4k}^{2k}$ con $x_j \in \mathbb{Z}$, $k < 2$, ya que $\mathcal{B} = \{x_1^{2k} + \cdots + x_{2k}^{2k}\}$ tiene en cierto sentido densidad positiva en $\mathbb{N}$ porque, si nos olvidamos de las multiplicidades, cualquier elección de $|x_j| \leq N^{1/2k}/2k$, $1 \leq j \leq 2k$, da lugar a un elemento de de $\#\mathcal{B}_N$ y hay $c_k N$ posibles elecciones .

Reparar esta limitación del método del círculo requiere no estimar arcos menores individualmente, sino estudiar la cancelación que puede haber entre varios de ello. En un importante trabajo [Kl] H.D. Kloosterman consiguió este objetivo para formas cuadráticas diagonales cuaternarias (de cuatro variables).

Después de esta disgresión y este desengaño vamos a demostrar que para más de dos sumandos no hay problema bajo una condición de paridad obvia: si por ejemplo escribimos N como suma de tres primos, típicamente N es impar porque si N es par uno de los sumandos es necesariamente el 2 y en realidad estamos representando $N-2$ como suma de dos primos. En general, si $N-k$ es impar, $r_k(N)$ se relaciona con $r_{k-1}(N-2)$ y por tanto las representaciones "genuinas" de N como suma de k primos requieren que N y k tengan la misma paridad.

Teorema 4.2.1 *Dado un entero $k > 2$, para $N \equiv k \pmod 2$ se verifica la fórmula asintótica*

$$r_k(N) \sim \frac{\mathfrak{G}_k(N) N^{k-1}}{(k-1)!(\log N)^k} \qquad con \quad \mathfrak{G}_k(N) = \prod_{p \nmid N} \left(1 + \frac{(-1)^{k+1}}{(p-1)^k}\right) \prod_{p \mid N} \left(1 + \frac{(-1)^k}{(p-1)^{k-1}}\right).$$

Corolario 4.2.2 (Teorema de Vinogradov) *Cualquier número impar suficientemente grande se puede expresar como suma de tres primos.*

Según las consideraciones anteriores la conjetura de Goldbach es inalcanzable con el método del círculo porque nos falta al menos un sumando. Podemos crearlo artificialmente promediando, y si un promedio da lo que tiene que dar y la dispersión es poca, entonces es que casi todos los términos son los que tienen que ser. Sin divagar, de un resultado en media deduciremos:

Teorema 4.2.3 *Casi todo número par es suma de dos primos, esto es,*

$$\#\{2n \leq N \ : \ r_2(2n) = 0\} = o(N).$$

Observación: Se conocen resultados más precisos que aseguran que incluso en intervalos "cortos" casi todo número par es suma de dos primos [Mo-Va] (véase también [Pe]).

Para la prueba de estos resultados utilizaremos consideraremos en lugar de $r_k(N)$ y $S(x)$ las cantidades

$$r_k^*(N) = \sum_{p_1+p_2+\cdots+p_k=N} (\log p_1)(\log p_2)\cdots(\log p_k) \qquad \text{y} \qquad S^*(x) = \sum_{p\le N} e(px)\log p.$$

La razón es la misma por la que nos decidimos por $\psi(x)$ en lugar de $\pi(x)$: las fórmulas son más sencillas y se puede pasar de una cantidad a la otra sumando por partes. Con estas definiciones (4.2) tiene su análogo en

$$r_k^*(N) = \int_{-1/2}^{1/2} \big(S^*(x)\big)^k e(-Nx)\,dx. \tag{4.3}$$

Pretendemos aproximar en los arcos mayores $S^*(x)$ por $S^*(a/q+\delta)$ con δ pequeño y dividir la sumación en sucesiones módulo q para aproximar mediante el Teorema de Siegel-Walfisz después de extraer el factor $e(n\delta)$ sumando por partes. Recuérdese que los primos en progresiones aritméticas sólo quedan controlados asintóticamente con el Teorema de Siegel-Walfisz cuando q es a lo más una potencia de logaritmo ya que el término de error sólo gana a la estimación trivial una cantidad de este orden. Esto nos sugiere exigir $q < (\log N)^B$ y $N|\delta| < (\log N)^B$. En definitiva, los arcos mayores serán

$$\mathfrak{M}_{a/q} = \{x \,:\, \|x - a/q\| < (\log N)^B/N\} \cap [-1/2, 1/2]$$

con $\|\cdot\|$ la distancia al entero más cercano y $q < (\log N)^B$, $(a,q) = 1$, $1 \le a \le q$.

Denotaremos por $\mathfrak{M}$ la unión de todos ellos. Nótese que la medida de $\mathfrak{M}$ tiende a cero, aun así esperamos que la mayor contribución a la integral de (4.3) esté allí.

Nuestro proyectos en los arcos mayores se materializa en el siguiente resultado:

Proposición 4.2.4 *Si $x \in \mathfrak{M}_{a/q}$, entonces*

$$S^*(x) = \frac{\mu(q)}{\phi(q)} \sum_{n\le N} e((x-a/q)n) + O\bigg(\frac{N}{(\log N)^{2B}}\bigg).$$

Antes de dar la prueba nos detendremos en el resultadillo al que nos habíamos referido en la exposición informal.

Lema 4.2.5 *Sea la* suma de Ramanujan

$$c_q(N) = \sum_{\substack{n=1\\(n,q)=1}}^{q} e\big(N\frac{n}{q}\big).$$

Si $N/q = N'/q'$ con N' y q' coprimos entonces $c_q(N) = \mu(q')\phi(q)/\phi(q')$.

Demostración: Es fácil ver, usando el teorema chino del resto, que $c_{q_1q_2}(N) = c_{q_1}(N) \cdot c_{q_2}(N)$, esto es, que $c_q(N)$ es multiplicativa en q, por ello basta considerar el caso $q = p^r$ con p primo.

Si $r = 1$ y $p \not| N$ entonces $c_q(N)$ es la suma de las raíces q-ésimas de la unidad excepto la raíz 1, por tanto $c_q(N) = 0 - 1 = \mu(q)$. Si $r > 1$ y $p \not| N$

$$c_q(N) = \sum_{n=1}^{q} e(Nn/q) - \sum_{m=1}^{q/p} e(pNm/q)$$

y ambas sumas son nulas por ser sumas de todas las raíces de la unidad.

Si $p|N$ y $N/q = N'/q'$ con $p \not| N'$,

$$c_q(N) = \sum_{\substack{n=1 \\ (n,q)=1}}^{q} e(Nn/q) = \sum_{\substack{n=1 \\ (n,q)=1}}^{q} e(N'n/q') = \frac{\phi(q)}{\phi(q')} \sum_{\substack{n=1 \\ (n,q')=1}}^{q'} e(N'n/q').$$

La última igualdad se sigue porque $f(n) = e(N'n/q')$ tiene periodo q' y por tanto podemos agrupar los $\phi(q)$ sumandos del sumatorio anterior de $\phi(q')$ en $\phi(q')$ términos. □

Demostración de la Proposición 4.2.4: No es difícil probar (ejercicio) que la contribución a $S^*(x)$ de los sumandos con $(n, q) \neq 1$ es pequeña y que tampoco perdemos mucho más que una raíz cuadrada al añadir a mano las potencias de los primos:

$$S^*(x) = \sum_{\substack{n \leq N \\ (n,q)=1}} \Lambda(n) e(nx) + O(N^{1/2}).$$

Escribamos, para abreviar, $\delta = x - a/q$. Factorizando $e(nx) = e(an/q)e(n\delta)$ y empleando la ortogonalidad de los caracteres, se sigue

$$S^*(x) = \frac{1}{\phi(q)} \sum_{r=1}^{q} \sum_{\chi} \overline{\chi}(r) \sum_{n \leq N} \chi(n)\Lambda(n) e(ar/q) e(n\delta) + O(N^{1/2}),$$

y agrupando términos

$$S^*(x) = \frac{1}{\phi(q)} \sum_{\chi} \tau(\overline{\chi}, a) \psi_\delta(N, \chi) + O(N^{1/2}) \tag{4.4}$$

donde

$$\tau(\overline{\chi}, a) = \sum_{r=1}^{q} \overline{\chi}(r) e(ar/q) \qquad \text{y} \qquad \psi_\delta(N, \chi) = \sum_{n \leq N} \chi(n)\Lambda(n) e(n\delta).$$

Sumando por partes y por el Teorema de Siegel-Walfisz (empléese mejor para $\psi(x, \chi)$, en vez de para $\pi(x; q, a)$, con $A = 4B$), si $\chi \neq \chi_0$

$$\psi_\delta(N, \chi) = e(N\delta)\psi(N, \chi) - 2\pi i\delta \int_1^N e(\delta t)\psi(t, \chi)\, dt \ll (1 + |\delta|N) \frac{N}{(\log N)^{4B}}.$$

Además aplicando las propiedades de ortogonalidad, se tiene que

$$\sum_{\chi} |\tau(\overline{\chi}, a)|^2 = \sum_{r,s=1}^{q} \sum_{\chi} \overline{\chi}(r)\chi(s)e(a(r-s)/q) \leq q\phi(q).$$

Así pues, por la desigualdad de Cauchy-Schwarz, la contribución a (4.4) de $\chi \neq \chi_0$ es $O\big((1+|\delta|N)q^{1/2}N(\log N)^{-4B}\big)$. Mientras que si $\chi = \chi_0$,

$$\psi_\delta(N, \chi_0) = \sum_{n\leq N} e(n\delta) + \sum_{n\leq N} (\Lambda(n) - 1)e(n\delta),$$

y procediendo como antes, el segundo sumatorio es $O(N(\log N)^{-4B})$. Como $\tau(\overline{\chi_0}, a)$ coincide con la suma de Ramanujan $c_q(a) = \mu(q)$ (según el Lema 4.2.5), se deduce finalmente de (4.4)

$$S^*(x) = \frac{\mu(q)}{\phi(q)} \sum_{n\leq N} e(n\delta) + O\bigg((1+|\delta|N)q^{1/2}\frac{N}{(\log N)^{4B}}\bigg).$$

Sustituyendo $\delta = x - a/q$ y recordando los rangos de δ y q (de la definición de los arcos mayores), se llega al resultado deseado. □

Los arcos menores son los que conforman el complementario de la unión de los mayores, es decir, la unión de los arcos menores es:

$$\mathfrak{m} = [-1/2, 1/2] - \mathfrak{M}.$$

La contribución cuando integramos sobre $\mathfrak{m}$ en (4.3) queremos que sea despreciable pero eso no significa en absoluto que sea sencillo acotar $S^*(x)$ en $\mathfrak{m}$ y sobre su dificultad reposa toda la enjundia del teorema. I.M. Vinogradov utilizó originalmente unos argumentos basados en la idea de que una suma sobre primos se puede escribir como una suma de sumas sobre enteros (mediante un proceso de criba), y de que hay razones analíticas para que todas sean grandes (cf. [El]). Cuarenta años después, R.C. Vaughan encontró una curiosa identidad que simplificaba mucho los argumentos y su atajo es el que emplearemos aquí.

Proposición 4.2.6 *Se cumple la acotación*

$$\max_{x\in\mathfrak{m}} |S^*(x)| \ll \frac{N}{(\log N)^{B/2-4}}.$$

Demostración: La *identidad de Vaughan* afirma que dados $N_1, N_2 \in \mathbb{N}$ con $N_1N_2 \leq N$, para cualquier función g

$$\sum_{n\leq N} \Lambda(n)g(n) = S_1 + S_2 + S_3 + S_4$$

donde

$$S_1 = \sum_{n\le N_1} \Lambda(n)g(n), \qquad S_2 = -\sum_{n\le N_1N_2} \Big(\sum_{\substack{l\le N_1,\ m\le N_2\\ lm=n}} \mu(m)\Lambda(l)\Big) \sum_{k\le N/n} g(nk),$$

$$S_3 = \sum_{n\le N_2} \mu(n) \sum_{k\le N/n} g(nk)\log k, \quad S_4 = \sum_{N_1<n<N/N_2} \Lambda(n) \sum_{N_2<j\le N/n} \Big(\sum_{l|j,\ l\le N_2} \mu(l)\Big) g(nj).$$

La prueba consiste simplemente en partir de la siguiente trivialidad

$$-\frac{\zeta'(s)}{\zeta(s)} = F(s) - \zeta(s)F(s)G(s) - \zeta'(s)G(s) + \big(-\frac{\zeta'(s)}{\zeta(s)} - F(s)\big)(1-\zeta(s)G(s))$$

con $F(s) = \sum_{n\le N_1} \Lambda(n)n^{-s}$ y $G(s) = \sum_{n\le N_2} \mu(n)n^{-s}$. Comparando los coeficientes de n^{-s} en cada miembro y multiplicándolos por $g(n)$ y sumando, se obtiene la identidad deseada.

En el caso $g(n) = e(f(n))$ si $1 \le n \le N$ y cero en otro caso, vamos a deducir

$$\begin{aligned}(4.5)\qquad \sum_{n\le N} \Lambda(n)e(f(n)) \ll N_1 + \log N \sum_{n\le N_1N_2} \Big| \sum_{k\le N/n} g(nk)\Big| \\ + N^{1/2}(\log N)^3 \max_{N_1<I\le N/N_2} \max_{N_2\le j\le N/I} \sum_{N_2<k\le N/I} \Big| \sum_{I<n\le 2I} g(nj)\,\overline{g}(nk)\Big|.\end{aligned}$$

Para ello, estimando trivialmente S_1 se obtiene el primer término del segundo miembro, N_1. Usando que $|\mu(m)| \le 1$ y que $\sum_{l|n} \Lambda(l) = \log n$, de S_2 se obtiene el segundo término, y S_3 se acota de la misma forma. Antes de tratar S_4, se divide en intervalos diádicos el rango de n, esto es, se considera $I < n \le 2I$ con I una potencia de dos, $N_1 < I < N/N_2$. Entonces

$$|S_4| \le \max_{N_1<I\le N/N_2} \Big| \sum_{I<n\le 2I} \sum_{N_2<j\le N/n} \Lambda(n)a_j g(nj)\Big|$$

con $|a_j| \le d(j)$ el número de divisores de j. Tras las acotaciones elementales (!?) $\sum_{i\le x} \Lambda^2(i) \ll x\log x$ y $\sum_{j\le x} d^2(j) \ll x(\log x)^3$, se concluye la prueba de (4.5).

Eligiendo $N_1 = N_2 = N^{2/5}$ y $f(n) = nx$, se tiene

$$(4.6)\qquad S^*(x) \ll N^{1/2} + M_1\log N + M_2^{1/2}N^{1/2}(\log N)^3$$

donde M_1 y M_2 son, respectivamente, los máximos valores posibles de las sumas

$$\sum_{n\le N^{4/5}} \Big| \sum_{k\le N/n} e(nkx)\Big| \qquad \text{y} \qquad \sum_{N^{2/5}<k\le N/I} \Big| \sum_{I<n\le 2I} e(n(j-k)x)\Big|$$

con $N^{2/5} < I \le N^{3/5}$ y $N^{2/5} \le j \le N/I$. Operando las sumas geométricas interiores, se deduce

$$M_1 \ll \sum_{n\le N^{4/5}} \min(N/n, |\operatorname{sen}(2\pi nx)|^{-1}),\ M_2 \ll N^{3/5} + \sum_{k'\le N^{3/5}} \min(N/k', |\operatorname{sen}(2\pi k'x)|^{-1})$$

donde se ha escrito $k' = |j-k|$, separando el caso $k' = 0$, y se ha empleado $I \le N/k'$.

Dado $x \in \mathfrak{m}$ sea a/q la fracción irreducible con $1 \le q \le N/(\log N)^B$ más cercana a x, entonces $q \ge (\log N)^B$ porque en otro caso $x \in \mathfrak{M}$, así pues $x = a/q + \delta$ con $qN|\delta| \le (\log N)^B$ y $(\log N)^B \le q \le N/(\log N)^B$. Por tanto para $n \le N^{4/5}$ se tiene $|nx - na/q| = n|\delta| = o(1/q)$, de manera que $\operatorname{sen}(2\pi nx)$ y $\operatorname{sen}(2\pi na/q)$ son comparables (su cociente está acotado) siempre que $2n/q \notin \mathbb{Z}$. Bajo esta hipótesis, según varía n, $|\operatorname{sen}(2\pi na/q)|^{-1}$ tomará $O(1 + N^{4/5}/q)$ veces periódicamente valores acotados por $q/1$, $q/2$, $q/3$,... q/q (ya que $|\operatorname{sen} t|^{-1} \ll |t|^{-1}$ en $[-\pi/2, \pi/2]$). La contribución a M_1 de los términos con $2n/q \in \mathbb{Z}$ es claramente $Nq^{-1}\log N$, con lo cual

$$M_1 \ll Nq^{-1}\log N + (1 + N^{4/5}q^{-1})(q/1 + q/2 + \cdots + q/q) \ll N/(\log N)^{B-1}.$$

Este razonamiento evidentemente también se aplica a M_2 obteniéndose la misma cota. Sustituyendo en (4.6), el teorema queda probado. □

Combinando los resultados anteriores se tiene el análogo del Teorema 4.2.1 pero con asteriscos.

Teorema 4.2.7 *Dado $A > 0$ y un entero $k > 2$, se cumple*

$$r_k^*(N) = \mathfrak{G}_k(N)\frac{N^{k-1}}{(k-1)!} + O\left(\frac{N^{k-1}}{(\log N)^A}\right).$$

Además $\mathfrak{G}_k(N)$ permanece entre dos constantes absolutas positivas si N y k tienen la misma paridad (y $\mathfrak{G}_k(N) = 0$ si no la tienen).

Demostración: Veamos la contribución de cada uno de los $\mathfrak{M}_{a/q}$ pertenecientes a los arcos mayores. Según la Proposición 4.2.4

$$\int_{\mathfrak{M}_{a/q}} (S^*(x))^k e(-Nx)\,dx = \int_{\mathfrak{M}_{a/q}} \left(\frac{\mu(q)}{\phi(q)}\sum_{n\le N} e((x-a/q)n)\right)^k e(-Nx)\,dx + O\left(\frac{N^{k-1}}{(\log N)^{2B}}\right).$$

Como $\sum e(nt) \ll |t|^{-1}$ en $[-1/2, 1/2]$, se puede completar la segunda integral a este intervalo perdiendo $O\big(((\log N)^B/N)^{-k+1}\big)$ que es absorbido por el término de error.

Como se mencionó en la primera sección, un sencillo argumento combinatorio para contar el número de representaciones de un número natural como suma de otros, prueba

$$\begin{aligned}\int_{-1/2}^{1/2}\left(\sum_{n\le N} e((x-a/q)n)\right)^k e(-Nx)\,dx &= e(-Na/q)\int_{-1/2}^{1/2}\left(\sum_{n\le N} e(nt)\right)^k e(-Nt)\,dt \\ = e(-Na/q)\binom{N-1}{k-1} &= e(-Na/q)\frac{N^{k-1}}{(k-1)!} + O(N^{k-2}).\end{aligned}$$

Así pues, sumando la contribución de todos los $\mathfrak{M}_{a/q}$, se tiene (es fácil ver que son disjuntos, ejercicio)

$$\int_{\mathfrak{M}} (S^*(x))^k e(-Nx)\,dx = \sum_{q<(\log N)^B}\left(\frac{\mu(q)}{\phi(q)}\right)^k c_q(-N)\frac{N^{k-1}}{(k-1)!} + O\left(\frac{N^{k-1}}{(\log N)^B}\right).$$

Notando que $\phi(q) \gg q/\log q$ (de hecho se tiene algo mejor, Th. 328 [Ha-Wr]), se puede completar la sumación hasta infinito con un término de error despreciable, y empleando que $g(q) = c_q(-N)\big(\mu(q)/\phi(q)\big)^k$ es una función multiplicativa,

$$\int_{\mathfrak{M}} (S^*(x))^k e(-Nx)\, dx = \mathfrak{G}_k(N)\frac{N^{k-1}}{(k-1)!} + O\bigg(\frac{N^k}{(\log N)^B}\bigg).$$

ya que $\prod_p(1+g(p)) = \mathfrak{G}_k(N)$.

Por otra parte, por la Proposición 4.2.6 se tiene

$$\int_{\mathfrak{m}} (S(x))^k e(-Nx)\, dx \ll \bigg(\frac{N}{(\log N)^{B/2-4}}\bigg)^{k-2} \int_{-1/2}^{1/2} |S^*(x)|^2 dx.$$

Por la identidad de Parseval, la última integral es

$$\sum_{p\le N} (\log p)^2 \le \log N \sum_{n\le N} \Lambda(n) \ll N \log N.$$

Combinando la contribución de los arcos mayores y menores, y eligiendo adecuadamente B, se deduce la fórmula del enunciado.

Si N y k tienen la misma paridad, entonces todos los factores de $\mathfrak{G}_k(N)$ son estrictamente positivos y demostrar que $\mathfrak{G}_k(N)$ está entre dos constantes absolutas positivas equivale a ver que su logaritmo está uniformemente acotado, lo cual es muy sencillo. Evidentemente el factor correspondiente a $p = 2$ se anula si la paridad es distinta. □

Demostración del Teorema 4.2.1: Evidentemente $r_k(N)(\log N)^k$ mayora a $r_k^*(N)$. Por otro lado, la contribución de los sumandos en la definición de $r_k^*(N)$ con algún $p_i \le N^{1-\epsilon}$, $0 < \epsilon < 1$, es $O(N^{(k-2)+1-\epsilon}(\log N)^k)$, de forma que

$$r_k^*(N) \ge (1-\epsilon)^k (\log N)^k \sum_{\substack{p_1+p_2+\cdots+p_k=N \\ p_1,p_2,\ldots,p_k \ge N^{1-\epsilon}}} 1 + O(N^{k-1-\epsilon}(\log N)^k).$$

De la misma forma, podemos añadir los términos con $p_i \le N^{1-\epsilon}$ al último sumatorio con una pérdida comparable al término de error.

Combinando estas acotaciones,

$$(1-\epsilon)^k r_k(N)(\log N)^k + O(N^{k-1-\epsilon}(\log N)^k) \le r_k^*(N) \le r_k(N)(\log N)^k.$$

Diviendo entre $\mathfrak{G}_k(N)N^{k-1}/(k-1)!$ y aplicando el teorema anterior, se deduce que los límites superior e inferior de $(k-1)!r_k(N)(\log N)^k/(\mathfrak{G}_k(N)N^{k-1})$ están acotados entre 1 y $(1-\epsilon)^{-k}$, y basta tomar $\epsilon \to 0$. □

Demostración del Teorema 4.2.3: Nuestro objetivo es acotar

$$T(N) = \sum_{n\le N/2} \big|r_2^*(2n) - 2n\mathfrak{G}_2(2n)\big|^2$$

Empleando la Proposición 4.2.4 se tiene como en la prueba del Teorema 4.2.7

$$\int_{\mathfrak{M}} (S^*(x))^2 e(-2nx)\, dx = 2n \sum_{q<(\log N)^B} \left(\frac{\mu(q)}{\phi(q)}\right)^2 c_q(-2n) + O\Big(\frac{N}{(\log N)^B}\Big).$$

A partir de (4.3) y de la descomposición en arcos mayores y menores $[-1/2, 1/2] = \mathfrak{M} \cup \mathfrak{m}$, se deduce

$$T(N) \le T_1 + T_2 + O\Big(\frac{N}{(\log N)^B}\Big)$$

con

$$\begin{aligned} T_1 &= 4 \sum_{n\le N/2} n^2 \Big| \mathfrak{G}_2(2n) - \sum_{q<(\log N)^B} \left(\frac{\mu(q)}{\phi(q)}\right)^2 c_q(-2n) \Big|^2, \\ T_2 &= \sum_{n\le N/2} \Big| \int_{\mathfrak{m}} (S^*(x))^2 e(-2nx)\, dx \Big|^2. \end{aligned}$$

No es difícil probar ([Ha-Wr] Th. 324,329) que $\sum_{n\asymp N} (\phi(n))^{-2} \ll N^{-1}$ (también se podría aplicar el Teorema de Wirsing) y usando el Lema 4.2.5

$$\begin{aligned} \sum_{q\ge(\log N)^B} \left(\frac{\mu(q)}{\phi(q)}\right)^2 c_q(-2n) &= \sum_{d|2n} \frac{\mu(d)}{\phi(d)} \sum_{\substack{q\ge(\log N)^B/d \\ (q,2n)=1}} \left(\frac{\mu(q)}{\phi(q)}\right)^2 \\ &\ll \sum_{d|2n} \frac{(\mu(d))^2}{\phi(d)} \operatorname{mín}\big(\frac{d}{(\log N)^B}, 1\big). \end{aligned}$$

Empleado $\phi(d) \gg d/\log d$ se tiene también la desigualdad más débil:

$$\sum_{q\ge(\log N)^B} \left(\frac{\mu(q)}{\phi(q)}\right)^2 c_q(-2n) \ll \sum_{d|2n} \frac{(\mu(d))^2}{\phi(d)} \ll (\log n)^2.$$

Multiplicando ambas desigualdades se tiene

$$T_1 \ll N^2 (\log N)^2 \sum_{n\le N/2} \sum_{d|2n} \frac{(\mu(d))^2}{\phi(d)} \operatorname{mín}\big(\frac{d}{(\log N)^B}, 1\big).$$

Intercambiando el orden de sumación (y usando $\sum_{n\asymp N} (\phi(n))^{-1} \ll 1$) se deduce

$$T_1 = O(N^3 (\log N)^{3-B}).$$

Por otra parte la identidad de Parseval aplicada a $(S^*(x))^2$ multiplicada por la función característica de $\mathfrak{m}$ implica

$$T_2 \le \int_{\mathfrak{m}} |S^*(x)|^4\, dx$$

y procediendo como en la prueba del Teorema 4.2.7,

$$T_2 \ll \min_{x\in\mathfrak{m}} |S^*(x)|^2 \int_{-1/2}^{1/2} |S^*(x)|^2\, dx \ll \frac{N^2}{(\log N)^{B-8}} \cdot N \log N.$$

Con ello hemos demostrado que para cualquier $A > 0$

$$T(N) = O\big(N^3 (\log N)^{-A}\big).$$

Si en un intervalo $[N/2, N]$ hubiera una proporción positiva de números pares con $r_2(2n) = 0$, como $\mathfrak{G}_2(2n) \gg 1$, se tendría

$$T(N) \gg \sum_{n\asymp N} n^2 \gg N^3$$

que contradice lo que acabamos de probar. □

Bibliografía

[Cr] E. Cristóbal. El método del círculo. Trabajo de iniciación a la investigación para obtener el DEA en la UAM. Madrid 2003.

[El] W.J. Ellison. Les nombres premiers. En collaboration avec Michel Mendès France. Publications de l'Institut de Mathématique de l'Université de Nancago, No. IX. Actualités Scientifiques et Industrielles, No. 1366. Hermann, Paris, 1975.

[Ha-Ra] G.H. Hardy, S. Ramanujan. Asymptotic formulae in combinatorial analysis. Proc. London Math. Soc., ser. 2, 17 (1918) 75–115.

[Ha-Wr] G.H. Hardy, E. Wright. An introduction to the theory of numbers. Fifth edition. The Clarendon Press, Oxford University Press, New York, 1979.

[Kl] H.D. Kloosterman. On the representation of numbers in the form $ax^2+by^2+cz^2+dt^2$. Acta Mathematica 49 (1926), 407–464.

[Mo-Va] H.L. Montgomery, R.C. Vaughan. The exceptional set in Goldbach's problem. Acta Arith. 27 (1975), 353–370.

[Pe] A. Perelli. Goldbach numbers represented by polynomials. Rev. Mat. Iberoamericana 12 (1996), no. 2, 477–490.

[Ru] W. Rudin. Análisis real y complejo McGraw-Hill, 1987.

[Va] R.C. Vaughan. The Hardy-Littlewood method. Cambridge tracts in Mathematics 80. Cambridge University Press, 1981.