4. El método del círculo

4.1. A vueltas con el círculo

El método del círculo es una poderosa técnica analítica que permite tratar muchos problemas aditivos en Teoría de Números. Apareció por primera vez en un artículo de Hardy y Ramanujan en 1918, y fue desarrollado por Hardy y Littlewood en los años subsiguientes. También es notable la contribución de H.D. Kloosterman a través de la introducción de una variante del método que empleó en el estudio de las formas cuadráticas cuaternarias.

El contexto general donde se aplica el método del círculo es en el tipo de problemas aditivos en los que se desea 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 números no negativos. Es decir, se busca una fórmula asintótica para

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

Como $\mathcal{B} \subset \mathbb{Z}^+ \cup \{0\}$, la función $F(z) = \sum_{b\in\mathcal{B}} z^b$ es holomorfa en el disco unidad y elevando a la potencia k se obtiene la función generatriz de $r_k(N)$, también holomorfa,

$$F^k(z) = \sum_{n=0}^{\infty} r_k(n) z^n.$$

Ahora se puede rescatar el coeficiente que nos interesa simplemente con la fórmula integral de Cauchy:

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

donde $\mathcal{C}$ es cualquier circunferencia de radio r, $0 < r < 1$.

La idea es obtener información sobre $r_k(N)$ a partir de las singularidades del integrando, en la línea de lo visto en el primer capítulo. El problema aquí es que la única singularidad encerrada por $\mathcal{C}$ 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 la circunferencia unidad es la frontera natural de F de modo que en general no tiene sentido extender $\mathcal{C}$ más allá en busca de nuevas singularidades que poder aprovechar, tratando de imitar el ejemplo de Cálculo I del primer capítulo.

El truco está en tomar r, el radio de $\mathcal{C}$, muy cercano a 1 para sentir la influencia de las "principales singularidades" de F en la circunferencia unidad, pero también 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 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 $N = b_1 + b_2 + \ldots + b_k \Rightarrow b_i \leq N$. 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.

En ciertos arcos de $\mathcal{C}$, llamados *arcos mayores*, podremos dar una buena fórmula aproximada para F debido a la gran influencia de singularidades cercanas en el círculo unidad, mientras que en el resto; en los llamados *arcos menores*, nos tendremos que contentar con una acotación. La idea es que juntando las aproximaciones de F en los arcos mayores podremos obtener un término principal para $r_k(N)$, y las acotaciones de F en los arcos menores darán lugar a un término de error.

Por ejemplo, supongamos $\mathcal{B} = \mathbb{Z}^+ \cup \{0\}$, entonces $r_3(N)$ es el número de representaciones de N como suma de tres enteros no negativos. En este caso es ridículo aplicar el método del círculo para estudiar el comportamiento asintótico de $r_3(N)$, ya que es fácil deducir combinatoriamente la fórmula explícita exacta $r_3(N) = (N+1)(N+2)/2$. Sin embargo vamos a indicar cómo se haría para mostrar los conceptos básicos sobre un ejemplo manejable. Si $\mathcal{B} = \mathbb{Z}^+ \cup \{0\}$, se tiene $F(z) = 1 + z + z^2 + \ldots = 1/(1-z)$ y (4.1) da lugar a la fórmula

$$r_3(N) = \frac{1}{2\pi i} \int_{\mathcal{C}} \frac{dz}{(1-z)^3 z^{N+1}}$$

con $\mathcal{C}$, digamos, la circunferencia de radio $r = 1 - 1/N$. De nuevo apreciamos lo tonto que es el ejemplo, porque F se extiende analíticamente fuera del disco unidad y una aplicación del teorema de los residuos en $\{z : |z| > r\}$ conduce a la fórmula explícita exacta para $r_3(N)$. Como F tiene su única singularidad en $z = 1$, sólo hay que considerar un arco mayor $\mathcal{M} = \{z \in \mathcal{C} : |\arg z| < \delta\}$ formado por los puntos de $\mathcal{C}$ cercanos a $z = 1$. Su complementario conformará el único arco menor $\mathbf{m} = \mathcal{C} - \mathcal{M}$. Por Taylor, $1 - re^{i\theta} = 1 - r - ir\theta + O(\theta^2)$, de modo que $|F(re^{i\theta})| \ll \theta^{-1}$ cuando $1/N < |\theta| < \pi$. En particular, para $\delta^{-1} = o(N)$

$$\frac{1}{2\pi i} \int_{\mathbf{m}} F^3(z) \frac{dz}{z^{N+1}} \ll \int_{\delta}^{\pi} \theta^{-3}\, d\theta = o(N^2).$$

Supongamos que $N^{1/2} = O(\delta^{-1})$, digamos por ejemplo $\delta = N^{-\kappa}$ con $1/2 < \kappa < 1$, entonces

para $re^{i\theta} \in \mathcal{M}$ se cumple $1 - re^{i\theta} \sim 1 - r - i\theta$. Tomando inversos, cuando $N \to \infty$ en $\mathcal{M}$ se tiene

$$F(z) \sim \frac{N}{1 + (N\arg z)^2} - i\frac{N^2 \arg z}{1 + (N\arg z)^2}.$$

La expresión de la derecha se comporta como una constante por N para $|\arg z| < 1/N$ y se hace menor cuando $|\arg z|$ crece, lo que sugiere que

$$\frac{1}{2\pi i}\int_{\mathcal{M}} F^3(z)\frac{dz}{z^{N+1}} \sim CN^3 \cdot \frac{1}{N} = CN^2.$$

Esto se puede probar rigurosamente con $C = 1/2$, aunque no lo haremos aquí. La contribución de los arcos mayores y menores lleva finalmente a $r_3(N) \sim \frac{1}{2}N^2$.

Trabajar con series infinitas puede conllevar algunas dificultades técnicas que se evitan con una formulación ligeramente distinta del método del círculo, que cronológicamente es posterior. Está basada en la sencilla observación, antes comentada, de que $N = b_1 + b_2 + \ldots + b_k \Rightarrow b_i \leq N$. 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:

$$r_k(N) = \int_0^1 S^k(x)\, e(-Nx)\, dx \qquad \text{con} \quad S(x) = \sum_{b \leq N,\ b \in \mathcal{B}} e(bx).$$

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 los resultados en un témino de error.

4.2. Sumas raras que se pueden calcular

En esta sección evaluaremos algunas sumas relacionadas con las siguientes expresiones:

$$c_q(M) = \sum_{\substack{n=1 \\ (n,q)=1}}^{q} e(Mn/q), \qquad G_q(a,l) = \sum_{n=1}^{q} e((an^2 + ln)/q).$$

En honor a los matemáticos que las introdujeron, se llaman *sumas de Ramanujan* a las primeras, y *suma de Gauss* (generalizadas) a las segundas.

Lema 4.1 . *La función $c_q(M)$ es multiplicativa en q, es decir, si q_1 y q_2 son coprimos, entonces $c_{q_1q_2}(M) = c_{q_1}(M) \cdot c_{q_2}(M)$.*

DEM.: Operando:

$$c_{q_1}(M) \cdot c_{q_2}(M) = \sum_{\substack{n=1 \\ (n,q_1)=1}}^{q_1} \sum_{\substack{m=1 \\ (n,q_2)=1}}^{q_2} e\big(M\frac{nq_2+mq_1}{q_1q_2}\big).$$

Por el teorema chino del resto, $k \equiv nq_2 \pmod{q_1}$, $k \equiv mq_1 \pmod{q_2}$ tiene solución única módulo q_1q_2, y evidentemente k es coprimo con q_1q_2 cuando n y m son coprimos con q_1 y q_2 respectivamente. Además cualquier k coprimo con q_1q_2 es solución de una de estas ecuaciones, porque si q_2' es el inverso de q_2 módulo q_1 y q_1' el de q_1 módulo q_2, se tiene $k \equiv (kq_2')q_2 \pmod{q_1}$, $k \equiv (kq_1')q_1 \pmod{q_2}$. Por tanto

$$c_{q_1}(M) \cdot c_{q_2}(M) = \sum_{\substack{k=1 \\ (k,q_1q_2)=1}}^{q_1q_2} e\big(m\frac{k}{q_1q_2}\big)$$

y ésta es la definición de $c_{q_1q_2}(M)$. ■

Proposición 4.2 . *Si M y q son coprimos entonces $c_q(M) = \mu(q)$. Y si $M/q = M'/q'$ con M' y q' coprimos entonces $c_q(M) = \mu(q')\phi(q)/\phi(q')$.*

DEM.: Por la multiplicidad basta considerar el caso $q = p^r$ con p primo. Si $r = 1$ y $p \not| M$ entonces $c_q(M)$ es la suma de las raíces q-ésimas de la unidad excepto la raíz 1, por tanto $c_q(M) = 0 - 1 = \mu(q)$. Si $r > 1$ y $p \not| M$

$$c_q(M) = \sum_{n=1}^{q} e(Mn/q) - \sum_{m=1}^{q/p} e(pMm/q)$$

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

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

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

La última igualdad se sigue porque $e(M'n/q')$ tiene periodo q', como función de n y por tanto podemos agrupar los $\phi(q)$ sumandos del sumatorio anterior de $\phi(q')$ en $\phi(q')$ términos. ■

Proposición 4.3 . *Para a y q coprimos $|G_q(a,l)| \leq (2q)^{1/2}$. Y además $(G_q(a,0))^k = (2q)^{k/2}\delta_q$ para k múltiplo de 8, donde*

$$\delta_q = \begin{cases} 2^{-k/2} & \text{si } 2 \not| q \\ 1 & \text{si } 4|q \\ 0 & \text{si } 4|q-2 \end{cases}$$

DEM.: Tomando módulos

$$|G_q(a,l)|^2 = \sum_{n=1}^{q}\sum_{m=1}^{q} e\left(a\frac{(n-m)(n+m)}{q} + l\frac{n-m}{q}\right).$$

Si q es impar, el cambio $u = n-m$, $v = n+m$ es lícito en $\mathbb{Z}_q \times \mathbb{Z}_q$ (la función inversa es $n = (u+v)/2$, $m = (v-u)/2$) y se llega a

$$|G_q(a,l)|^2 = \sum_{u=1}^{q}\left(\sum_{v=1}^{q} e\big(au\frac{v}{q}\big)\right)e\big(\frac{lu}{q}\big).$$

La suma entre paréntesis es no nula sólo si $q|au$ y esto implica $u = q$, por tanto $|G_q(a,l)|^2 = q$. En el caso con q par, el cambio es 2 a 1 (su núcleo es $\{(0,0),(q/2,q/2)\}$) siendo su imagen los u y v con la misma paridad. Por tanto

$$|G_q(a,l)|^2 = 2\sum_{\substack{u=1\\ 2\not| u}}^{q}\left(\sum_{\substack{v=1\\ 2\not| v}}^{q} e\big(au\frac{v}{q}\big)\right)e\big(\frac{lu}{q}\big) + 2\sum_{\substack{u=1\\ 2| u}}^{q}\left(\sum_{\substack{v=1\\ 2| v}}^{q} e\big(au\frac{v}{q}\big)\right)e\big(\frac{lu}{q}\big).$$

El primer sumatorio entre paréntesis es siempre nulo por ser la suma de todas las raíces impares q-ésimas de la unidad. Escribiendo en el segundo $v = 2v'$, se tiene que sólo puede ser no nulo si $u = q/2$ o $u = q$, en cuyo caso vale $q/2$, y el doble sumatorio está acotado, en módulo, por $q/2 + q/2 = q$.

Para evaluar $(G_q(a,0))^k$ utilizaremos el resultado debido a Gauss:

$$G_q(1,0) = \frac{1+i^{-q}}{1+i^{-1}}\sqrt{q}$$

que puede obtenerse como una indirecta y compleja consecuencia de la fórmula de sumación de Poisson ([**Da**] §2, [**Dy-Mc**]). De aquí se deduce que $G_q(1,0)$ es siempre una raíz de $x^k - (2q)^{k/2}\delta_q$. Consideremos el automorfismo del grupo de Galois $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ con $\xi = e(1/q)$, definido por $\sigma : \xi \mapsto \xi^a$. Aplicando σ, $G_q(1,0)$ se transforma en $G_q(a,0)$, y como los automorfismos permutan las raíces de los polinomios sobre el cuerpo base, se deduce que $\big(G_q(a,0)\big)^k - (2q)^{k/2}\delta_q = 0$. ■

Lema 4.4 . *Si δ_q es como en el resultado anterior, se cumple*

$$\sum_{q=1}^{\infty} \frac{\delta_q}{q^{k/2}}\, c_q(-N) = \frac{1}{(2^{k/2}-1)\zeta(k/2)} \sum_{d|N} (-1)^{N+N/d} d^{1-k/2}.$$

Dem.: Consideremos la función aritmética $g(q) = 2^{k/2} c_q(-N)\delta_q q^{-k/2}$. Por las propiedades de c_q y la definición de δ_q, esta función es multiplicativa y por tanto

$$\sum_{q=1}^{\infty} \frac{\delta_q}{q^{k/2}}\, c_q(-N) = 2^{-k/2} \prod_p (1 + g(p) + g(p^2) + g(p^3) + \ldots)$$

donde p recorre los primos. Llamemos F_p a cada uno de estos factores. Si p^l es la máxima potencia de p que divide a N, por las propiedades de c_q, para $p \neq 2$ se cumple

$$F_p = 1 + p^{-k/2}(p-1) + (p^2)^{-k/2}(p^2-p) + \ldots + (p^l)^{-k/2}(p^l - p^{l-1}) - (p^{l+1})^{-k/2} p^l$$

$$= (1 - p^{-k/2}) \left(1 + p^{1-k/2} + p^{2(1-k/2)} + \ldots + p^{l(1-k/2)}\right).$$

Y razonamientos similares conducen para $p = 2$ y N par, a

$$F_2 = 1 + 2^{1-k/2} + 2^{2(1-k/2)} + \ldots + 2^{l(1-k/2)} - 2 \cdot 2^{l(1-k/2)},$$

mientras que trivialmente $F_2 = 1$ para N impar.

Así pues

$$\sum_{q=1}^{\infty} \frac{\delta_q}{q^{k/2}}\, c_q(-N) = C\left(\sum_{d|N} d^{1-k/2} - 2 \sum_{d|N,\ 2\not| d} (2^l d)^{1-k/2} \right) \quad \text{con } C = 2^{-k/2} \prod_{p\neq 2} (1 - p^{-k/2})$$

donde $l > 1$ es la máxima potencia de 2 que divide a N y el segundo sumatorio se omite si N es impar. Es decir, la suma buscada es, salvo la constante C, la suma de los divisores

de N restando dos veces aquellos divisores que contienen una potencia máxima de 2 mayor que 1. Notando que $N+N/d$ es impar si y sólo si d es par y contiene esta máxima potencia de 2, se sigue

$$\sum_{q=1}^{\infty} \frac{\delta_q}{q^{k/2}}\, c_q(-N) = C \sum_{d|N} (-1)^{N+N/d} d^{1-k/2}.$$

Finalmente $C^{-1} = (2^{k/2}-1)\zeta(k/2)$ es consecuencia directa de la identidad de Euler para la función ζ. ■

Lema 4.5 . *Sean $N > 1$ y $k > 2$ enteros, entonces*

$$\sum_{q=1}^{\infty} \left(\frac{\mu(q)}{\phi(q)}\right)^k c_q(-N) = \prod_{p\not|N} \left(1 + \frac{(-1)^{k+1}}{(p-1)^k}\right) \prod_{p|N} \left(1 + \frac{(-1)^k}{(p-1)^{k-1}}\right).$$

DEM.: La evaluación de esta suma es muy similar a la del resultado anterior, pero técnicamente es más sencilla. La función multiplicativa a considerar ahora es $g(q) = c_q(-N)(\mu(q)/\phi(q))^k$. Como $g(p^r) = 0$ si $r > 1$, se tiene

$$\sum_{q=1}^{\infty} \left(\frac{\mu(q)}{\phi(q)}\right)^k c_q(-N) = \prod_{p} (1 + g(p)) = \prod_{p} \left(1 + \frac{(-1)^k c_p(-N)}{(p-1)^k}\right).$$

Y según las propiedades de las sumas de Ramanujan, si $p \not| N$, $c_p(-N) = \mu(p) = -1$, y si $p|N$, $c_p(-N) = p-1$. ■

4.3. Sumas de cuadrados

En esta sección vamos a aplicar el método del círculo en su versión clásica para estudiar el número de representaciones como suma de k cuadrados, esto es,

$$r_k(N) = \#\{(n_1, n_2, \ldots, n_k) \in \mathbb{Z}^k \,:\, n_1^2 + n_2 + \ldots + n_k^2 = N\}.$$

Nos vamos a restringir al caso en que k es múltiplo de 8 con el fin de simplificar algunos detalles técnicos y llegar a una fórmula final más sencilla; sin embargo esta condición no es esencial **[Va]**, **[Gr]**.

De acuerdo con (4.1)

$$r_k(N) = \frac{1}{2\pi i} \int_{\mathcal{C}} F^k(z) \frac{dz}{z^{N+1}} \qquad \text{con} \quad F(z) = \sum_{n=-\infty}^{\infty} z^{n^2} = 1 + 2\sum_{n=1}^{\infty} z^{n^2}.$$

Por razones de comodidad vamos a desplegar la circunferencia en un segmento a través del cambio $z \mapsto e(z)$, que da lugar a

$$r_k(N) = \int_L f(z) e(-Nz)\, dz \qquad \text{con} \quad f(z) = \Big(\sum_{n=-\infty}^{\infty} e(n^2 z) \Big)^k \tag{4.2}$$

y L el segmento horizontal $L = \{0 \le \operatorname{Re} z \le 1,\ \operatorname{Im} z = y\}$ donde $r = e^{-2\pi y}$. Escogeremos $y = 1/N$, lo que corresponde aproximadamente a $1 - r = 2\pi/N$.

Antes de efectuar la división en arcos mayores y menores, probaremos una aproximación de $f(z)$ en L que servirá en todos ellos. Por el resultado de Dirichlet que vimos en el capítulo anterior, $\mathbb{T}$ (el toro unidad unidimensional correspondiente al intervalo $[0,1]$ con los extremos identificados) queda cubierto por intervalos de la forma:

$$I_{a/q} = \big\{ x \,:\, |x - \frac{a}{q}| < \frac{1}{q\sqrt{N}} \big\}$$

con a/q fracciones irreducibles $0 \le a < q \le \sqrt{N}$.

Proposición 4.6 . *Si* $\operatorname{Re} z \in I_{a/q}$ *y* $\operatorname{Im} z = N^{-1}$, *se cumple*

$$f(z) = (qz - a)^{-k/2} \big(\delta_q + O(e^{-\Delta}) \big)$$

donde $\Delta = \frac{1}{2} \min(Nq^{-2}, N^{-1}(qx-a)^{-2})$ *y* δ_q *es como en la sección anterior, esto es,* $\delta_q = 1$ *si* $4|q$ *y* $\delta_q = 2^{-k/2-1}(1 - (-1)^q)$ *en otro caso.*

DEM.: Descomponiendo en clases de restos módulo q

$$\sum_{n=-\infty}^{\infty} e(n^2 z) = \sum_{m=0}^{q-1} e(am^2/q) \sum_{n \equiv m \,(\mathrm{mod}\, q)} e(n^2 (z - a/q)).$$

Para cada m se puede aplicar la fórmula de sumación de Poisson al último sumatorio:

$$\sum_{n \equiv m \,(\mathrm{mod}\, q)} e(n^2 (z - a/q)) = \frac{1}{q\sqrt{2i(z - a/q)}} \sum_{n=-\infty}^{\infty} e\big(\frac{n^2}{4q(a - qz)} \big)\, e(nm/q).$$

Al sustituir, separando la contribución de $n = 0$, se llega a

$$\sum_{n=-\infty}^{\infty} e(n^2 z) = \frac{1}{q\sqrt{-2i(z - a/q)}} \Big(G_q(a,0) + \sum_{n \neq 0} G_q(a,n)\, e\big(\frac{n^2}{4q(a - qz)} \big) \Big).$$

Sabemos que $|G_q(a,m)| = O(q^{1/2})$ y evidentemente $|e(w)| = O(e^{-\operatorname{Im} w})$. Así pues, notando que $\operatorname{Im}\big(q^{-1}(a-qz)^{-1}\big) = (N(qx-a)^2 + N^{-1}q^2)^{-1}$ y comparando la suma de la serie con una progresión geométrica, se sigue

$$\sum_{n=-\infty}^{\infty} e(n^2 z) = \frac{1}{q\sqrt{-2i(z-a/q)}}\big(G_q(a,0) + O(q^{1/2}e^{-\Delta})\big).$$

Elevando a k cada uno de los miembros y usando $G_q(a,0) = O(q^{1/2})$, se obtiene finalmente el resultado, ya que según la Proposición 4.3, $\delta_q = (2q)^{-k/2}G_q^k(a,0)$. ■

En principio podríamos tomar como arcos mayores los $I_{a/q}$, y como recubren todo $[0,1]$ no habría necesidad de arcos menores. Esta situación es típica de los problemas que provienen de las llamadas formas modulares (véanse los capítulos 11 y 12 de **[Gr]**). Sin embargo, para ser coherentes con la terminología, los $x \in I_{a/q}$ con $4|q-2$ deberían pertenecer a un arco menor ya que en ese caso el término principal en la proposición anterior se anula. Otro problema es que los intervalos $I_{a/q}$ no son estrictamente disjuntos. Una manera de resolver este problema es reemplazarlos por la subdivisión de Farey **[Ci-Co]**, **[Gr]**, pero aquí procederemos de una manera más simple pidiendo $0 \le a < q \le \sqrt{N}/2$ lo que asegura que los $I_{a/q}$ son disjuntos. En definitiva, la elección de los arcos mayores y menores es respectivamente

$$\mathcal{M} = \bigcup_{\substack{0\le a<q\le\sqrt{N}/2\\(a,q)=1\ \ 4\not|q-2}} I_{a/q} \qquad \text{y} \qquad \mathbf{m} = \mathbb{T} - \mathcal{M}.$$

Proposición 4.7 . *Si* $z = x + i/N$

$$\int_{\mathbf{m}} f(z)\, e(-Nz)\, dx = O(N^{k/4}).$$

Dem.: Si $x \in \mathbf{m}$, $x \in I_{a/q}$ con $4|q-2$ o $\sqrt{N}/2 < q \le \sqrt{N}$. En cualquiera de los dos casos el término principal en la proposición anterior es absorbido por el error. Por consiguiente

$$\int_{\mathbf{m}} f(z)\, e(-Nz)\, dx \ll \sum_{0\le a<q\le\sqrt{N}} \int_{I_{a/q}} |qz-a|^{-k/2} e^{-\Delta}\, dx.$$

Es fácil comprobar que $|qz-a|^{-1} \ll N^{1/2}\Delta^{1/2}$. Por otra parte la función $h(t) = t^{k/4}e^{-t}$

está acotada en $[0,\infty)$, así pues $|qz-a|^{-k/2}e^{-\Delta} \ll N^{k/4}$. Y se tiene

$$\int_{\mathbf{m}} f(z)\, e(-Nz)\, dx \ll \sum_{q\le\sqrt{N}} \sum_{0\le a<q} N^{k/4}|I_{a/q}| \ll \sum_{q\le\sqrt{N}} \sum_{0\le a<q} N^{k/4}N^{-1/2}q^{-1}$$

que claramente es $O(N^{k/4})$. ■

Proposición 4.8 . *Con la notación anterior se cumple la fórmula*

$$\int_{\mathcal{M}} f(z)\, e(-Nz)\, dx = \frac{(2\pi)^{k/2}N^{k/2-1}}{(k/2-1)!} \sum_{q\le\sqrt{N}/2} \frac{\delta_q}{q^{k/2}}\, c_q(-N) + O(N^{k/4}).$$

Dem.: La contribución del término de error de $f(z)$, esto es, $O(|qz-a|^{-k/2}e^{-\Delta})$, ha sido ya estudiada en los arcos menores, y da lugar a un término $O(N^{k/4})$. Por tanto

$$\int_{\mathcal{M}} f(z)\, e(-Nz)\, dx = \sum_{q\le\sqrt{N}/2} \sum_{\substack{a=0\\(a,q)=1}}^{q-1} \delta_q \int_{I_{a/q}} (qz-a)^{-k/2}\, dx + O(N^{k/4}). \tag{4.3}$$

Con el cambio de variable $u = N(x-a/q)$ y recordando que $z = x + i/N$,

$$\int_{I_{a/q}} (qz-a)^{-k/2}\, dx = N^{k/2-1}q^{-k/2}e(-aN/q) \int_{-\sqrt{N}/q}^{\sqrt{N}/q} (u+i)^{-k/2}e(-u-i)\, du.$$

Por el teorema de los residuos aplicado en el semiplano inferior

$$\int_{-\infty}^{\infty} (u+i)^{-k/2}e(-u-i)\, du = \frac{(-2\pi i)^{k/2}}{(k/2-1)!}.$$

Integrando por partes, la contribución a la integral de $|u| > \sqrt{N}/q$ es $O(q^{k/2}N^{-k/4})$. Por tanto

$$\int_{I_{a/q}} (qz-a)^{-k/2}\, dx = \frac{(2\pi)^{k/2}N^{k/2-1}}{q^{k/2}(k/2-1)!}\, e(-aN/q) + O(N^{k/4-1}).$$

Sustituyendo en (4.3), se concluye la prueba. ■

Con esto ya podemos probar el teorema que buscábamos:

Teorema 4.9. *Para cada k múltiplo de 8 se cumple la fórmula*

$$r_k(N) = C_k N^{k/2-1} \sum_{d|N} (-1)^{N+N/d} d^{1-k/2} + O(N^{k/4})$$

donde $C_k = (2\pi)^{k/2}/(\zeta(k/2)(2^{k/2}-1)(k/2-1)!)$.

DEM.: Por los resultados anteriores y (4.2)

$$r_k(N) = \frac{(2\pi)^{k/2} N^{k/2-1}}{(k/2-1)!} S + O(N^{k/4}) \qquad \text{con} \quad S = \sum_{q \le \sqrt{N}/2} \frac{\delta_q}{q^{k/2}} \, c_q(-N).$$

Los términos $q > \sqrt{N}/2$ se pueden añadir a la suma conservando el término de error porque

$$\sum_{q > \sqrt{N}/2} \frac{\delta_q}{q^{k/2}} \, c_q(-N) = O\Big(\sum_{q > \sqrt{N}/2} \frac{1}{q^{k/2}} \cdot q \Big) = O(N^{1-k/4}).$$

Y basta aplicar el Lema 4.4 a la suma S completada con estos términos. ■

4.4. Sumas de primos

En esta sección utilizaremos el método del círculo para deducir el comportamiento asintótico del número de representaciones como suma de primos. Es decir, fijado k estudiaremos:

$$r_k(N) = \#\{(p_1, p_2, \ldots, p_k) \in (\mathbb{Z}^+)^k \, : \, N = p_1 + p_2 + \ldots + p_k \text{ con } p_i \text{ primo}\}.$$

El método tendrá éxito para $k > 2$, lo cual nos deja con la miel en los labios a las puertas de poder alcanzar la celebérrima conjetura de Goldbach. Ésta proviene de una carta que envió C. Goldbach a Euler en 1742, y aunque la conjetura original es ligeramente diferente (entre otras cosas porque él consideraba el uno como primo), en términos actuales se podría formular diciendo que todo número par mayor que dos es suma de dos números primos, y todo número impar mayor que cinco es suma de tres primos; siendo la primera afirmación la conjetura de Goldbach por antonomasia. El método del círculo confirma la segunda aserción para números suficientemente grandes (teorema de Vinogradov), donde "grande" significa hoy por hoy "grandísimo", porque el número finito de casos restantes (actualmente del orden de 10^{43000}) está todavía enormemente lejos de las capacidades de las computadoras. De hecho es un problema profundo, relacionado con los ceros de Siegel, dar una cota explícita del número de casos que faltan por comprobar.

Antes de comenzar haremos dos precisiones de tipo técnico. La primera es que al igual que en el primer capítulo era más sencillo aproximar bien $\psi(x)$ que $\pi(x)$ (la función identidad es más simple que el logaritmo integral), aquí será conveniente estudiar

$$r_k^*(N) = \sum_{n_1+n_2+\ldots+n_k=N} \Lambda(n_1)\Lambda(n_2)\cdots\Lambda(n_k)$$

en lugar de $r_k(N)$. Más adelante veremos la relación entre la asintótica de ambas cantidades.

La segunda observación es que como sólo hay un número primo par, el dos, es natural intuir que cuando las paridades de N y k no coinciden $r_k(N)$ será como k veces $r_{k-1}(N-2)$. Por ejemplo, si supiésemos que todo número par mayor que cuatro es suma de tres primos, es fácil ver que habríamos probado la conjetura de Goldbach, en realidad estamos representando un par como suma de dos primos sin más que restar el dos que necesariamente debe haber. De este modo se muestra natural considerar sólo el caso en que N y k tienen la misma paridad, porque el otro es consecuencia de él.

Aplicaremos el método del círculo en su versión "finita", escribiendo

$$r_k^*(N) = \int_0^1 S^k(x)e(-Nx)\,dx \qquad \text{con} \qquad S(x) = \sum_{n\le N} \Lambda(n)e(nx).$$

Al final del segundo capítulo vimos cómo acotar sumas trigonométricas del tipo de $S(x)$, lo cual servirá para dar cuenta de los arcos menores. Por otra parte, los arcos mayores llevan necesariamente al estudio de la distribución de los primos en progresiones aritméticas. Por ejemplo, es fácil ver que

$$S(1/3) = \big[(\log N)/\log 3\big]\log 3 + e(1/3)\psi(N;3,1) + e(2/3)\psi(N;3,2),$$

y en general $S(a/q)$ depende de $\psi(N;q,b)$ con $1 \le b < a$, donde se ha usado la notación introducida en la sección 1.9. Sólo hay que sumar por partes (esencialmente aplicar el lema de Abel) para pasar de a/q a valores de x muy cercanos a a/q. El gran problema está en que se sabe muy poco de la dependencia en q del error en el teorema de los números primos en progresiones aritméticas. A este respecto, definiendo $\psi(x,\chi) = \sum_{n\le x}\Lambda(n)\chi(n)$, se conoce ([**Da**] §22) que si $\chi \neq \chi_0$, el carácter módulo q que vale uno en todos los coprimos con q, para cualquier A se cumple

$$\psi(x,\chi) = O\left(\frac{x}{\log^A x}\right) \tag{4.4}$$

uniformemente en q. De donde para a y q coprimos, empleando la ortogonalidad de los caracteres ($\sum_\chi \overline{\chi}(a)\chi(n) \neq 0 \Leftrightarrow q|n-a$ con a y q coprimos), se tiene

$$\psi(x;q,a) = \frac{1}{\phi(q)} \sum_{\substack{n\leq N \\ (n,q)=1}} \Lambda(n) + \frac{1}{\phi(q)} \sum_{\chi\neq\chi_0} \overline{\chi}(a)\psi(x,\chi) = \frac{x}{\phi(q)} + O\bigg(\frac{x}{\log^A x}\bigg).$$

Nótese sin embargo que a pesar de la uniformidad, esta versión del teorema de los números primos en progresiones aritméticas se vuelve trivial si q crece ligeramente más rápido que una potencia de logaritmo (se cumple $\phi(q) \gg q/\log q$). Esto y la pobreza del término de error, se traducirá en que sólo podemos aproximar $S(a/q+\delta)$ para q y $N|\delta|$ menores que una potencia de logaritmo. En definitiva, elegiremos los arcos mayores como

$$\mathcal{M} = \sum_{\substack{q\leq \log^B N \\ (a,q)=1,\ 0<a\leq q}} I_{a/q} \qquad \text{con} \qquad I_{a/q} = \{x \,:\, |x-a/q| < (\log^B N)/N\}$$

donde B es un número positivo. Es evidente que para N mayor que cierta constante, los $I_{a/q}$ son disjuntos.

Todo lo que necesitamos saber en los arcos mayores está recogido en el siguiente resultado:

Teorema 4.10 . *Si $x \in I_{a/q}$ con a y q coprimos y $q \leq \log^B N$, entonces*

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

Dem.: Por razones técnicas será útil descartar los sumandos de $S(x)$ correspondientes a $(n,q) \neq 1$. Es fácil ver que su contribución es pequeña, cumpliéndose

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

ya que q tiene $O(\log q)$ factores primos contando multiplicidades, y cada potencia de p aparece $O(\log N/\log p)$ veces hasta N.

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

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

y agrupando términos

$$S(x) = \frac{1}{\phi(q)} \sum_{\chi} \tau(\overline{\chi}, a)\psi_\delta(N, \chi) + O(\log^2 N), \tag{4.5}$$

donde

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

Por el lema de Abel y (4.4) con $A = 4B$, para $\chi \neq \chi_0$ (el carácter que vale idénticamente uno en $\mathbb{Z}_q^*$),

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

Además aplicando como antes las propiedades de los caracteres, se tiene que

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

Así pues, por la desigualdad de Cauchy-Schwarz, la contribución a (4.5) de $\chi \neq \chi_0$ es $O\big((1 + |\delta|N)q^{1/2}N/\log^{4B} N\big)$.

Por otra parte, si $\chi = \chi_0$,

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

y una nueva aplicación del lema de Abel y de (4.4) al segundo sumatorio, prueba que éste es $O(N/\log^{4B} N)$. Como $\tau(\overline{\chi_0}, a)$ coincide con la suma de Ramanujan $c_q(a) = \mu(q)$, se deduce finalmente de (4.5)

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

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 el complementario de los mayores, $\mathbf{m} = \mathbb{T} - \mathcal{M}$. Como hemos mencionado, la cota que emplearemos en ellos proviene de técnicas de sumas trigonométricas introducidas en el segundo capítulo.

Teorema 4.11 . *Se cumple la acotación*

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

DEM.: Aplicando la Proposición 2.13 con $N_1 = N_2 = N^{2/5}$ y $f(n) = nx$, se tiene

$$S(x) \ll N^{2/5} + M_1 \log N + M_2^{1/2} N^{1/2} \log^3 N \tag{4.6}$$

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

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

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

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

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

Por el Lema 3.11, existe una fracción irreducible a/q con $1 \le q \le N/\log^B N$ tal que $|x - a/q| < (\log^B N)/N$. Además debe ser $q > \log^B N$ porque en otro caso $x \in I_{a/q}$ y estamos bajo la hipótesis de que $x \in \mathbf{m}$. En resumen, se puede escribir $x = a/q + \delta$ con $qN|\delta| \le \log^B N$ y $\log^B N < q \le N/\log^B N$. Por tanto para $i \le N^{4/5}$ se tiene $|ix - ia/q| = i|\delta| = o(1/q)$, de manera que $\operatorname{sen}(2\pi i x)$ y $\operatorname{sen}(2\pi i a/q)$ son comparables (su cociente está acotado) siempre que $2i/q \notin \mathbb{Z}$. Bajo esta hipótesis, según varía i, $|\operatorname{sen}(2\pi i a/q)|^{-1}$ 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 $2i/q \in \mathbb{Z}$ es claramente $Nq^{-1}\log N$, con lo cual

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

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

Una vez completado nuestro análisis de los arcos mayores y menores sólo hay que unir las piezas para deducir una fórmula asintótica.

Teorema 4.12 . *Dado $A > 0$ y un entero $k > 2$, se cumple*

$$r_k^*(N) = \mathcal{P}_N \frac{N^{k-1}}{(k-1)!} + O\Big(\frac{N^{k-1}}{\log^A N}\Big) \quad con \quad \mathcal{P}_N = \prod_{p\nmid N}\Big(1+\frac{(-1)^{k+1}}{(p-1)^k}\Big)\prod_{p\mid N}\Big(1+\frac{(-1)^k}{(p-1)^{k-1}}\Big).$$

Además $\mathcal{P}_N$ permanece entre dos constantes absolutas positivas si N y k tienen la misma paridad.

DEM.: Veamos la contribución de cada uno de los $I_{a/q}$ pertenecientes a los arcos mayores. Según el Teorema 4.10

$$\int_{I_{a/q}} S^k(x)e(-Nx)\,dx = \int_{I_{a/q}} \Big(\frac{\mu(q)}{\phi(q)}\sum_{n\le N} e((x-a/q)n)\Big)^k e(-Nx)\,dx + O\Big(\frac{N^{k-1}}{\log^B N}\Big).$$

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

Un sencillo argumento combinatorio para contar el número de representaciones de un entero positivo como suma de otros, prueba

$$\int_{-1/2}^{1/2}\Big(\sum_{n\le N} e((x-a/q)n)\Big)^k e(-Nx)\,dx = e(-Na/q)\int_{-1/2}^{1/2}\Big(\sum_{n\le N} e(nt)\Big)^k e(-Nt)\,dt$$

$$= e(-Na/q)\binom{N-1}{k-1} = e(-Na/q)\frac{N^{k-1}}{(k-1)!} + O(N^{k-2}).$$

Así pues, sumando la contribución de todos los $I_{a/q}$, se tiene

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

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 el Lema 4.5 prueba

$$\int_{\mathcal{M}} S^k(x)e(-Nx)\,dx = \mathcal{P}_N\frac{N^{k-1}}{(k-1)!} + O\Big(\frac{N^k}{\log^B N}\Big).$$

Por otra parte, por el Teorema 4.11 se tiene

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

Por la identidad de Parseval, la última integral es

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

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 $\mathcal{P}_N$ son estrictamente positivos (sólo hay que examinar el caso $p = 2$), y demostrar que $\mathcal{P}_N$ está entre dos constantes absolutas positivas equivale a ver que $|\log \mathcal{P}_N|$ está uniformemente acotado, lo cual se sigue de

$$|\log \mathcal{P}_N| \leq \sum_p \frac{2}{(p-1)^{k-1}},$$

donde se ha usado la desigualdad $|\log(1+x)| \leq 2|x|$ válida en $[-1/2, 1]$. ■

Como hemos mencionado al principio, hemos trabajado con $r_k^*(N)$ únicamente para simplificar los argumentos. Una vez que hemos probado lo que queríamos, podemos volver a nuestra función favorita $r_k(N)$.

Corolario 4.13. *Dado un entero $k > 2$, para $N \equiv k \pmod 2$ se verifica la fórmula asintótica*

$$r_k(N) \sim \mathcal{P}_N \frac{N^{k-1}}{(k-1)! \log^k N}.$$

En particular, todo número impar suficientemente grande es suma de tres primos (teorema de Vinogradov).

DEM.: Es fácil deducir del teorema de los números primos que hay $O(N^{1/2})$ potencias de primos de exponente mayor que uno en $[1, N]$. Por consiguiente

$$r_k^*(N) = \sum_{p_1+p_2+\ldots+p_k=N} (\log p_1)(\log p_2)\cdots(\log p_k) + O(N^{k-3/2}\log^k N),$$

ya que, por ejemplo, hay $O(N^{(k-2)+1/2})$ posibilidades paa $(p_1, p_2, \ldots, p_{k-1})$ si sabemos que p_{k-1} es una potencia de primo como antes. Es evidente que el sumatorio está mayorado por $r_k(N)\log^k N$. Por otra parte, la contribución de los sumandos con algún $p_i \leq N^{1-\epsilon}$, $0 < \epsilon < 1$, es $O(N^{(k-2)+1-\epsilon}\log^k N)$, de forma que el sumatorio vale

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

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

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

Uniendo estos resultados,

$$(1-\epsilon)^k r_k(N)\log^k N + O(N^{k-1-\epsilon}\log^k N) \leq r_k^*(N) \leq r_k(N)\log^k N + O(N^{k-3/2}\log^k N).$$

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

Si creemos en la preponderancia de la contribución de los arcos mayores, el corolario anterior debería ser cierto también para $k = 2$, lo cual probaría la conjetura de Goldbach para números pares mayores que cierta constante. Sin embargo hay serias dificultades teóricas que hacen poco creíble un acercamiento definitivo a la conjetura con el método del círculo. Si queremos conservar el esquema de la prueba con unos arcos menores que tienen la mayor parte de la medida, la cota del Teorema 4.11 debería ser de orden menor que $N^{1/2}$ para que $|S(x)|^2$ no interfiriese con el término principal $\mathcal{P}_N N^{2-1}/(2-1)! \gg N$. Esto choca frontalmente con la filosofía de las sumas trigonométricas (véase el segundo capítulo) que muestra la raíz cuadrada de los términos como un límite natural de la cancelación.

En el lado positivo, el método del círculo sí permite probar (véase **[Va]**) que la fórmula asintótica conjeturada para $r_2(N)$ es cierta quizá omitiendo un subconjunto de los pares muy fino, de densidad nula. Además J.-R. Chen demostró utilizando técnicas de criba que el número de representaciones de un número par como suma de dos primos o como suma de un primo y un producto de dos primos es comparable a $N/\log^2 N$. Aquí también aparecen dificultades teóricas aparentemente irreparables que impiden descontar las representaciones correspondientes al segundo caso.