El Método del Círculo

Elena Cristóbal Rodríguez

$A.m.p$

Índice

1. Historia **1**

2. Un ejemplo sencillo **2**

3. El teorema de Vinogradov **8**

4. El problema binario de Goldbach **29**

5. Representación de enteros como suma de cuadrados **33**

5.1. Introducción 33

5.2. Aplicación del método del círculo para estudiar el número de representaciones de un entero como suma de k cuadrados 34

6. Otro problema relacionado con el método del círculo. El problema de Waring **48**

7. Apéndice **49**

1. Historia

¿De cuántas formas podemos expresar un número como suma de otros números? A esta simple pregunta que hasta un niño entendería, es difícil darle respuesta, es un problema de Teoría de Números, en general lo que nos planteamos es si un número puede ser expresado como suma de otros números, todos ellos pertenecientes a algún subconjunto de los enteros. Algunos de los problemas de este tipo son los más conocidos de Teoría de Números, por ejemplo, el famosísimo Último Teorema de Fermat, que dice que no existen tres números enteros positivos que cumplan la siguiente ecuación

$$x^n + y^n = z^n, \quad \text{donde} \quad n \quad \text{representa} \quad 3, 4, 5, \ldots$$

Pierre de Fermat planteó este problema en 1637 y su demostración no se logró hasta 1995, tres siglos después[1], lo que nos puede dar una idea de la dificultad de estas cuestiones. Otro famoso resultado de este tipo es la conjetura de Goldbach que dice que todo número impar suficientemente grande se puede escribir como suma de tres primos y todo número par como suma de dos primos. Esta conjetura data de 1742 y hoy en día la segunda parte continua siendo un problema abierto. (En este trabajo profundizaremos en la demostración de la primera parte, conocida como teorema de Vinogradov).

El Método del Círculo es una herramienta que sirve para tratar cierto tipo de problemas aditivos. Fue creado por Hardy y Ramanujan, [Har], quienes lo aplicaron al conocido problema de las particiones que consiste en saber de cuántas formas se puede escribir un número entero, N, como suma de otros números sin importar el orden de los sumandos, ni si son repetidos o no, ni el número de sumandos en los que se descompone N, (cada forma de escribirlo es lo que se llama una partición). Su artículo de 1918, [Har], es el resultado de un intento de aplicar a los principales problemas de teoría de particiones la teoría de funciones analíticas que ya había sido aplicada con éxito al estudio de la distribución de los números primos y a ramas relacionadas de la teoría analítica de números. Si denotamos $p(n)$ al número de particiones de n, según la siguiente fórmula debida a Euler [Ha-Wr] $p(n)$ es el coeficiente de x^n en el desarrollo de Taylor de la función

$$f(x) = 1 + \sum_{1}^{\infty} p(n)x^n = \frac{1}{(1-x)(1-x^2)(1-x^3)\ldots},$$

$p(n)$ se puede expresar, aplicando el Teorema de Cauchy (véase apéndice o [Pes]), con una integral

$$p(n) = \frac{1}{2\pi i}\int_{\Gamma} \frac{f(z)}{z^{n+1}} dz,$$

[1]El teorema fue demostrado por Andrew Wiles.

donde Γ es un camino que rodea una sola vez al origen y está contenido en el círculo unidad. A partir de la integral podemos obtener una fórmula para $p(n)$. Esta idea de aplicar la teoría de funciones analíticas a los principales problemas de Teoría de Números dominó la investigación moderna del s.XIX en teoría analítica de números y parecía extraño que no hubiera sido aplicada antes a este problema particular de las particiones. Hardy y Ramanujan dan dos explicaciones para esto en su artículo, [Har]:

- La teoría de particiones había recibido sus más importantes desarrollos desde su fundación por Euler de la mano de una serie de matemáticos que tenían sus intereses principales en el Álgebra. Era hasta el momento un compendio de identidades formales, la mayoría ingeniosas y bonitas.

- La razón más fundamental es que en la teoría de particiones se trataba con funciones que no están definidas fuera del círculo unidad. Todo punto del círculo es una singularidad esencial de la función y no podemos deformar el camino sobre el que integramos de ninguna forma para que su contribución se haga insignificante. Por lo que parecía el problema sería demasiado complejo.

La clave para que esto funcione es extraer información aritmética a partir de las singularidades. Podemos contrastar este problema con otros conocidos de teoría de números como por ejemplo el estudio de la distribución de los primos que depende fuertemente de las singularidades de ς/ς'.

El método del círculo apareció por primera vez en el ya citado artículo de Hardy y Ramanujan cuando trataban el problema de las particiones pero luego fue desarrollado por Hardy y Littlewood (por esto a veces es también conocido como método de Hardy y Littlewood) y aplicado a muchos problemas de Teoría de Números de naturaleza aditiva. Ellos introdujeron la terminología que hoy se usa de *arcos mayores* y *arcos menores*. Estos son divisiones de la circunferencia. Los arcos mayores se toman alrededor de singularidades "principales" y su influencia nos lleva a una buena aproximación de la integral con la que obtenemos una buena fórmula asintótica. En los arcos menores se emplea una cota.

A continuación veremos cómo aplicar el método para resolver un sencillo problema aditivo y así familiarizarnos con las ideas fundamentales.

2. Un ejemplo sencillo

Si N es un número mayor o igual que tres, ¿de cuántas formas podemos escribir N como suma de tres enteros positivos? Al número de formas lo lla-

maremos $r(N)$, es decir

$$r(N) = \#\{(n_1, n_2, n_3) \in (\mathbb{Z}^+)^3 \ : \ n_1 + n_2 + n_3 = N\}.$$

Primero encontraremos solución exacta a este problema usando la matemática discreta:

Un número cualquiera N lo podemos escribir:

$$N = 1 + 1 +^{N)} \ldots + 1 \tag{1}$$

Queremos escribir N como suma de tres enteros y saber de cuántas formas posibles podemos hacerlo, esto es lo mismo que dividir los unos que aparecen en (21) en tres grupos y ver de cuantas formas posibles podemos hacer estos grupos.

$$N = 1 \smile 1 \smile^{N)} \ldots \smile 1$$

Para hacer los grupos y separarlos usaremos la siguiente regla:
En los huecos que hay entre los unos, simbolizados con $\smile$, pondremos el signo $\square$ si dos unos consecutivos pertenecen al mismo grupo y pondremos $\star$ si dos unos consecutivos pertenecen a distinto grupo. Tenemos $N-1$ huecos para poner $\square$ o $\star$, pero sólo queremos colocar $\star$ en dos huecos de los $N-1$ que hay, así que el número de formas de dividir los unos en tres grupos es igual a las posibles maneras que tenemos de elegir dos entre $N-1$ y a su vez como ya hemos dicho, esto es el número de formas de escribir N como suma de tres enteros positivos. Por lo tanto

$$r(N) = \binom{N-1}{2} = \frac{(N-1)(N-2)}{2}. \tag{2}$$

En la siguiente parte del ejemplo veremos cómo el método del círculo en una versión sencilla nos permite concluir

$$r(N) = \frac{1}{2}N^2 + O(N). \tag{3}$$

Para dar esta fórmula asintótica no es necesario usar el método del círculo ya que como hemos visto conocemos un resultado exacto, pero utilizarlo nos servirá para ilustrar como funciona y familiarizarnos con él.

Sea[2]

$$S(x) = \sum_{n=1}^{N} e(nx)$$

siendo $e(nx) = e^{2\pi nix}$. Elevemos nuestra función al cubo,

$$S^3(x) = \sum_{n_1=1}^{N}\sum_{n_2=1}^{N}\sum_{n_3=1}^{N} e(x(n_1+n_2+n_3)) = \sum_{n=1}^{N} r(n)e(nx) + \sum_{n=1}^{3N} a_n e(nx), \tag{4}$$

[2]En la observación 2.1 explicamos por qué el sumatorio anterior sólo llega hasta N.

donde $r(n)$ es el número de representaciones de n como suma de tres números naturales y los términos del último sumando no influyen en los desarrollos posteriores. Hemos conseguido escribir $r(n)$ de tal forma que sea el coeficiente de una serie, ahora es fácil expresar $r(n)$ como función de $S^3(x)$. Tenemos

$$S^3(x)e(-Nx) = \sum_{n=1}^{N} e((n-N)x),$$

intengrando sobre cualquier intervalo unidad y observando que $\int_I e((n-N)x)dx$ es 1 si $n = N$ y 0 en el resto de los casos llegamos a

$$r(N) = \int_{-1/2}^{1/2} S^3(x)e(-Nx)dx.$$

Como estamos trabajando con funciones de periodo uno, el intervalo[3] $[-1/2, 1/2]$ se puede ver como una circunferencia identificando los extremos. A esta circunferencia la dividimos en un *arco mayor* y *un arco menor* (los nombres no se corresponden al tamaño) de la siguiente forma,

$$I = I_M \cup I_m \ \text{ con } \ I_M = (-N^{-1/2}, N^{-1/2}) \ e \ I_m = I - I_M,$$

donde I representa el intervalo $[-1/2, 1/2]$, I_M a los arcos mayores e I_m a los menores. Con esto

$$r(N) = \int_{-1/2}^{1/2} S^3(x)e(-Nx)dx = \int_{I_m} S^3(x)e(-Nx)dx + \int_{I_M} S^3(x)e(-Nx)dx. \tag{5}$$

Para la integral sobre los *arcos menores* podemos hacer una acotación. Teniendo en cuenta que $S(x)$ se puede ver como una serie geométrica, que $x \in [-1/2, 1/2]$ y que $e^{\pi i\alpha} - e^{-\pi i\alpha}$
$= 2i\text{sen}\alpha$,

$$|S(x)| = \left|\frac{e^{2\pi ix(N+1)} - e^{2\pi ix}}{e^{2\pi ix} - 1}\right| = \left|\frac{e^{\pi ix}[e^{2\pi ixN} - 1]}{e^{\pi ix} - e^{\pi} ix}\right| \leq \frac{C}{|sen\pi x|} \leq \frac{C'}{|x|},$$

es decir, $|S(x)| \ll |x|^{-1}$, y con esto,

$$\int_{I_m} S^3(x)e(-Nx)dx \ll \int_{I_m} \frac{1}{|x|^3}dx = 2\int_{1/\sqrt{N}}^{1/2} \frac{1}{|x|^3}dx = O(N).$$

Para enfrentarnos a $\int_{I_M} S^3(x)e(-Nx)dx$ antes haremos algunas consideraciones,

[3]Tomamos el interavalo $[-1/2, 1/2]$ en vez del $[0, 1]$ porque $S(x)$ no es buena, (es grande), en los puntos 1 y 0, es decir, escogiendo el intervalo $[0, 1]$ tendríamos dos puntos "malos" mientras que tomando el intervalo $[-1/2, 1/2]$ sólo tenemos uno, el cero.

1. Para x pequeño,

$$S(x)^3 e(-Nx) = h_N(x)(1+O(x)) \quad \text{con} \quad h_N(x) = \frac{sen^3(\pi Nx)}{\pi^3 x^3} e(Nx/2), \tag{6}$$

ya que

$$S(x) = \frac{e^{\pi ix} e^{\pi iNx}(e^{\pi iNx} - e^{-\pi iNx})}{e^{\pi ix} - e^{-\pi ix}} = \frac{e^{\pi ix} e^{\pi iNx} \text{sen}(\pi Nx)}{\text{sen}(\pi x)},$$

y por tanto

$$S^3(x)e(-Nx) = \frac{\text{sen}^3(\pi Nx)}{(\pi x)^3} \left(\frac{\pi x}{\text{sen}(\pi x)}\right)^3 e(3Nx/2)e(-Nx)e(3x/2),$$

simplificando y teniendo en cuenta que $e(3x/2) = 1 + O(x)$ y $\left(\frac{\pi x}{\text{sen}(\pi x)}\right)^3 = 1 + O(x)$ obtenemos (6).

2. Si $|x| \leq N^{-1}$ entonces $|h_N(x)| \ll N^3$ ya que $|sen(\pi Nx)| \leq \pi Nx$.

3. En el resto del intervalo $|h_N(x)| \ll |x|^{-3}$, porque $|sen^3(\pi Nx)e(Nx/2)| \leq 1$.

De todo lo anterior tenemos que

$$\int_{I_M} S^3(x)e(-Nx)dx = \int_{I_M} h_N(x)dx + \int_{I_M} |h_N(x)|O(x)dx, \tag{7}$$

aproximemos la segunda integral, para ello utilizamos los puntos dos y tres que acabamos de ver, y nos queda

$$\int_{I_M} |h_N(x)|O(x)dx \leq \int_{-1/\sqrt{N}}^{-1/N} \frac{C'}{x^2}dx + N^3 \int_{-1/N}^{1/N} C'|x|dx + \int_{1/N}^{1/\sqrt{N}} C\frac{C'}{x^2}dx \equiv O(N),$$

sólo resta calcular

$$\int_{I_M} h_N(x)dx = \int_{I_M} \frac{sen^3(\pi Nx)}{\pi^3 x^3} e(Nx/2)dx.$$

Hacemos el cambio de variable $t = Nx$, $dt = Ndx$ y $x = t/N$, con lo que

$$\int_{I_M} \frac{sen^3(\pi Nx)}{\pi^3 x^3} e(Nx/2)dx = \frac{N^2}{\pi^3} \int_{-\sqrt{N}}^{\sqrt{N}} \frac{sen^3(\pi t)}{t^3} e(t/2)dt$$

$$= \frac{N^2}{\pi^3} \int_{-\sqrt{N}}^{\sqrt{N}} \frac{sen^3(\pi t)cos(\pi t)}{t^3}dt + i \int_{-\sqrt{N}}^{\sqrt{N}} \frac{sen^4(\pi t)}{t^3}dt.$$

La última integral de la expresión anterior es una función impar en un intervalo simétrico, así que es cero. Por lo tanto tenemos que solucionar:

$$Int = \frac{N^2}{\pi^3} \int_{-\sqrt{N}}^{\sqrt{N}} \frac{sen^3(\pi t)cos(\pi t)}{t^3}dt,$$

integramos por partes, con $u = t^{-3}$ y $dv = sen^3(\pi t)cos(\pi t)$, y nos queda

$$Int = O(\sqrt{N}) + \frac{3N^2}{4}\int_{-\sqrt{N}}^{\sqrt{N}} \frac{sen^4(\pi t)}{\pi^4 t^4} dt$$

Nos encontramos muy cerca de hallar una expresión asintótica para $r(N)$. Sustituyamos los resultados obtenidos hasta ahora en la expresión (5),

$$r(N) = \int_{-1/2}^{1/2} S^3(x)e(-Nx)dx = \int_{I_m} S^3(x)e(-Nx)dx + \int_{I_M} S^3(x)e(-Nx)dx$$

$$= O(N) + \frac{3N^2}{4}\int_{-\sqrt{N}}^{\sqrt{N}} \frac{sen^4(\pi t)}{\pi^4 t^4} dt$$

y veamos cómo es la última integral,

$$\frac{3N^2}{4}\int_{-\sqrt{N}}^{\sqrt{N}} \frac{sen^4(\pi t)}{\pi^4 t^4} dt = \frac{3N^2}{4}\int_{-\infty}^{\infty}(\qquad) - \frac{3N^2}{4}\int_{-\infty}^{-\sqrt{N}}(\qquad) - \frac{3N^2}{4}\int_{\sqrt{N}}^{\infty}(\qquad),$$

el integrando es $O(|t|^{-4})$, así que la contribución de las dos últimas integrales sería
$N^2 O((\sqrt{N})^{-3})$ y al añadirla es absorbida por el término de error. Por tanto

$$r(N) = CN^2 + O(N) \qquad \text{con} \quad C = \frac{3}{4}\int_{-\infty}^{\infty} \frac{sen^4(\pi t)}{\pi^4 t^4} dt.$$

La constante C debe ser $1/2$ según la fórmula exacta. Esto puede comprobarse,

la transformada de Fourier de $f(x) = \frac{\sqrt{3}}{2} max(0, 1-|x|)$ es $\hat{f}(\xi) = \frac{\sqrt{3}}{2}(\pi\xi)^{-2} sen^2(\pi\xi)$

y aplicando la identidad de Plancherel

$$C = \int_{-\infty}^{\infty} |\hat{f}|^2 = \int_{-\infty}^{\infty} |f|^2 = 1/2.$$

Por lo tanto hemos obtenido la fórmula asintótica deseada,

$$r(N) = \frac{N^2}{2} + O(N)$$

y se comprueba que coincide con la que habíamos hallado al principio del ejercicio usando la matemática discreta.

Observación 2.1 *El sumatorio de $S(x)$ llega exactamente hasta N y no más allá debido a que si no los errores acomulados en los cálculos aumentarían y en la expresión final de $r(N)$ en vez de tener un error de $O(N)$ tendríamos un error mayor.*

Observación 2.2 *Sólo cogemos un arco mayor porque estos se eligen alrededor de los puntos singulares, y aquí sólo tenemos un único punto singular que es el cero.*

Observación 2.3 *Si escogiéramos $I_M = (-N^{-\theta}, N^{-\theta})$ con $\theta > \frac{1}{2}$, al integrar en los arcos menores cambiaría el orden del error, sería más grande. El ideal es $\theta = 1/2$ porque así es como se compensan los errores de los arcos mayores y de los arcos menores.*

A partir de este ejemplo surge la pregunta natural de qué cambios habría que hacer para estudiar el número de representaciones de un entero como suma de k enteros positivos, $r_k(N)$. Como $S(x)$ sólo es grande cerca del origen, parece lógico elegir, como antes, un único arco mayor, en principio no conocemos su tamaño, lo denotamos $I_M = (-N^{-\theta}, N^{-\theta})$, para algún $\theta > 0$. El resto del intervalo serán los arcos menores.

Como antes, se tiene

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

Hagamos la integral sobre los arcos menores, utilizando, como en el caso $k = 3$ que $|S(x)| \ll |x|^{-1}$ para $x \in [1/2, -1/2]$, llegamos a

$$\int_{I_m} S^k(x)e(-Nx)dx \ll \int_{I_m} \frac{1}{|x|^k}|e(-Nx)|dx$$

$$\ll \int_{I_m} \frac{1}{|x|^k}dx = 2\int_{1/N^\theta}^{1/2} \frac{1}{|x|^k}dx = O(N^{k\theta-\theta}).$$

Busquemos ahora una aproximación para x pequeño de $S^k(x)e(-Nx)$. Procedemos de la misma forma que con $k = 3$, es decir, usamos que $S(x)$ se puede expresar como una serie geométrica, que $e^{\pi i\alpha} - e^{-\pi i\alpha} = 2isen\alpha$ y que $e^{\pi ix} = 1 + O(x)$ y $sen(x) = x + O(x^3)$ para llegar a

$$S^k(x)e(-Nx) = h_n(x)(1+O(x)), \text{ donde } h_n(x) = \frac{sen^k(\pi Nx)}{(\pi x)^k}e\left(\frac{(k-2)Nx}{2}\right)^{k-2}.$$

Resolvamos ahora la integral en los arcos mayores,

$$\int_{I_M} S^k(x)e(-Nx)dx = \int_{I_M} h_N(x)dx + \int_{I_M} h_N(x)O(x)dx$$

En los $x \in [-1/2, 1/2]$ tal que $|x| > \frac{1}{N}$, se tiene

$$|h_N(x)| = \left|\frac{sen^k(\pi Nx)}{(\pi x)^k}e\left(\frac{(k-2)Nx}{2}\right)\right| \leq \left|\frac{1}{\pi^k x^k}\right|,$$

y si $|x| \leq 1/N$ entonces $|h_N(x)| \ll N^k$. Así que operando como en el caso $k = 3$ nos queda

$$\int_{I_M} |h_N(x)|O(x)dx = O(N^{\theta k-2\theta}) + O(N^{k-2}).$$

Si $\theta < 1$ lo anterior será $O(N^{k-2})$ y si $\theta > 1$ será $O(N^{\theta k-2\theta})$.

Calculemos ahora, $\int_{I_M} h_N(x)dx$, haciendo el cambio de variable $t = Nx$, $dt = Ndx$, y resolviendo de la misma manera en la que lo hicimos para $k = 3$ resulta,

$$\int_{I_M} h_N(x)dx = N^{k-1} \int_{-N^{-\theta+1}}^{N^{-\theta+1}} \frac{k}{\pi^{k+1}(k-2)} \frac{sen^k(\pi t)sen(\pi(k-2)t)}{t^{k+1}}dt + O(N^{\theta k-1})$$

Si llamamos

$$f(x) \text{ a } \frac{k}{\pi^{k+1}(k-2)} \frac{sen^k(\pi t)sen(\pi(k-2)t)}{t^{k+1}},$$

procediendo de forma análoga al caso $k = 3$ se obtiene,

$$\int_{I_M} h_N(x)dx = N^{k-1} \int_{-\infty}^{\infty} f(x)dx + O(N^{k\theta-1}).$$

La integral de f no se evalúa fácilmente, denotaremos C_k a la constante que se obtendría al calcularla.

Con todo esto,

$$\begin{aligned} r_k(N) &= \int_{I_m} S^k(x)e(-Nx)dx + \int_{I_M} S^k(x)e(-Nx)dx \\ &= C_k N^{k-1} + O(N^{k\theta-\theta}) + O(N^{k-2}) + O(N^{\theta k-1}), \end{aligned}$$

y escogeremos

$$\theta \leq \frac{k-2}{k-1}$$

para que el error sea lo más pequeño posible.

Una vez visto este ejemplo sencillo, que nos ha enseñado como funciona el método del círculo, veremos una versión más realista del método tratando el problema del número de representaciones de un número $N \geq 3$ como suma de tres primos.

3. El teorema de Vinogradov

En una carta a Euler fechada en junio de 1742, Goldbach escribió (considerando al 1 como primo) que todo número par es suma de dos primos y

todo número mayor que 2 es suma de tres primos, esta frase ha dado lugar a la que hoy conocemos como conjetura de Goldbach, (véase la sección 1). Durante los siglos XVIII y XIX no se avanzó mucho en su demostración, ya que aún no se tenían métodos adecuados para tratar los complicados problemas aditivos, sin embargo desde comienzos del siglo XX se han sucedido muchos resultados parciales. Hardy y Littlewood en 1923 se dieron cuenta de que su método se podía aplicar a estos problemas con éxito suponiendo la hipótesis de Riemann generalizada y consiguieron demostrar (condicionalmente) que todo número impar "grande" es suma de tres primos y que casi todo número par es suma de dos primos. En 1937 Vinogradov logró probar lo mismo sin tener que suponer la hipótesis de Riemann generalizada, por ello conocemos hoy como teorema de Vinogradov el siguiente resultado.

Teorema 1 *Todo número N suficientemente grande se puede expresar como suma de tres primos, es decir, si $N \geq C$ podemos escribir*

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

siendo p_1, p_2 y p_3 números primos.

En está sección demostraremos el teorema, pero antes de comenzar veremos otros teoremas, lemas y una definición que posteriormente nos harán falta en demostración.

Empezaremos viendo un teorema que nos dice que todo número real, α, se aproxima por racionales.

Teorema 2 (Teorema de Dirichlet) *Dado $N \geq 1$ existen enteros a y $1 \leq q \leq N$ con $(a, q) = 1$ tales que se verifica*

$$\mid \alpha - \frac{a}{q} \mid < \frac{1}{qN}.$$

Demostración

Sea $N \geq 1$, $N \in [1, \infty)$. Al igual que todo número real, N se podrá descomponer en $N = [N] + frac(N)$, donde $[N]$ es la parte entera de N. Tenemos $[N]$ números $\alpha q = [\alpha q] + frac(\alpha q)$, ya que $(q = 1, 2, \ldots, [N])$. Llamaremos β_q a $frac(\alpha q)$, los $[N]$ números β_q pertenecen a $[0, 1)$. Consideremos $[N] + 1$ intervalos

$$B_r = \left[\frac{r-1}{[N]+1}, \ \frac{r}{[N]+1} \right) \quad (r = 1, 2, \ldots, [N]+1).$$

Si β_q está en el primer o en el último intervalo se ve claramente que

$$|q\alpha - [q\alpha]| < \frac{1}{[N]+1}$$

con lo que la prueba estaría concluida. Si no, uno de los $m-1$ intervalos que nos quedan contendrá al menos dos de los β_q, supongamos que contiene a β_u y a β_v con $u < v$. Si tomamos $q = v - u$ y $a = [\alpha v] - [\alpha u]$ finalizamos la demostración. □

Definamos $r_3(N) = \sum_{p_1+p_2+p_3=N} 1$ como el número de representaciones de un entero como suma de tres primos, denotaremos ahora

$$r_3^*(N) = \sum_{n_1+n_2+n_3=N} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3) \text{ y } r_3^{**}(N) = \sum_{p_1+p_2+p_3=N} \log p_1 \log p_2 \log p_3,$$

donde[4]

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

Con el método del círculo veremos que si N es impar $r_3^*(N) \gg N^2$ y bajo esta hipótesis tenemos el siguiente lema:

Lema 3 *Para N impar*

$$r_3^*(N) \sim r_3^{**}(N) \sim r_3(N)(\log N)^3.$$

Demostración

Comenzaremos probando que

$$r_3^*(N) \sim r_3^{**}(N) \tag{8}$$

Por definición tenemos

$$r_3^*(N) = \sum_{p_1^k+p_2^k+p_3^k=N} \log p_1 \log p_2 \log p_3, \text{ como } \quad r_3^{**}(N) = \sum_{p_1+p_2+p_3=N} \log p_1 \log p_2 \log p_3,$$

podemos escribir,

$$r_3^*(N) = r_3^{**}(N) + \sum_{\substack{p_1^k+p_2^k+p_3^k=N \\ k>2}} \log p_1 \log p_2 \log p_3,$$

La idea es demostrar que el último sumatorio es $O(N^\alpha)$ con $\alpha < 2$, ya que si luego dividimos toda la expresión por $r_3^*(N)$, se tiene

$$1 = \frac{r_3^{**}(N)}{r_3^*(N)} + \frac{O(N^\alpha)}{r_3^*(N)},$$

y como sabemos que $r_3^*(N) \gg N^2$ y $\alpha < 2$, nos quedará

$$1 = lim_{N \longrightarrow \infty} \frac{r_3^{**}(N)}{r_3^*(N)},$$

[4] $\Lambda(n)$ se conoce con el nombre de símbolo de Von Mangoldt.

con lo se demuestra que $r_3^{**}(N) \sim r_3^*(N)$.

Veamos pues que

$$\sum_{\substack{p_1^k+p_2^k+p_3^k=N \\ k>2}} \log p_1 \log p_2 \log p_3 \ \text{ es } o(N^2). \tag{9}$$

Conozcamos un poco como se comporta este sumatorio para los distintos k.

Para $k = 2$,

$$\sum_{p_1^2+p_2^2+p_3^2=N} \log p_1 \log p_2 \log p_3 \ll (\log N)^3 \sum_{p_1^2+p_2^2+p_3^2=N} 1,$$

ya que $p_i < N$. Como $p_1^2 + p_2^2 + p_3^2 = N$, se cumple que $p_1^2 < N$ y $p_2^2 < N$, que es lo mismo que decir $p_1 < \sqrt{N}$ y $p_2 < \sqrt{N}$, y por lo tanto

$$(\log N)^3 \sum_{p_1^2+p_2^2+p_3^2=N} 1 = (\log N)^3 \sum_{p_1 \le \sqrt{N}} \sum_{p_2 \le \sqrt{N}} \eta(\sqrt{N - p_1^2 - p_2^2}), \tag{10}$$

donde

$$\eta(x) = \begin{cases} 1 & \text{si} \quad x \text{ es primo} \\ 0 & \qquad \text{en otro caso} \end{cases}$$

con lo que la expresión (10) queda

$$\ll (\log N)^3 \sqrt{N}\sqrt{N} = O(N(\log N)^3).$$

Para $k = 3$ tenemos,

$$\sum_{p_1^3+p_2^3+p_3^3=N} \log p_1 \log p_2 \log p_3 \ll (\log N)^3 \sum_{p_1^3+p_2^3+p_3^3=N} 1,$$

usando que $p_1^3 < N$ la ecuación anterior queda igual a

$$(\log N)^3 \sum_{p_1 \le N^{1/3}} \sum_{p_2 \le N^{1/3}} \eta((N - p_1^3 - p_2^3)^{\frac{1}{3}})$$

y acotando se llega a

$$\sum_{p_1^3+p_2^3+p_3^3=N} \log p_1 \log p_2 \log p_3 \ll (\log N)^3 N^{1/3} N^{1/3} = O((\log N)^3 N^{2/3}).$$

El mismo razonamiento que hemos utilizado para $k = 2$ y $k = 3$ funciona para potencias mayores. Además $p_1^k + p_2^k + p_3^k = N$ implica $k \le \gamma = \frac{\log N}{\log 2}$ porque $2^k \le p_1^k < N$. Por lo tanto

$$\sum_{\substack{p_1^k+p_2^k+p_3^k=N \\ k>2}} \log p_1 \log p_2 \log p_3 \ll N^{2/2}(\log N)^3 + N^{2/3}(\log N)^3 + \ldots N^{2/\gamma}(\log N)^3$$

$$\leq N(\log N)^3(\gamma - 1) \ll N(\log N)^4,$$

en esta última desigualdad hemos aplicado que $\gamma \ll \log N$.

Finalmente como $N(\log N)^4$ es $o(N^2)$ se verifica (9) y se concluye que $r_3^*(N) \sim r_3^{**}(N)$.

Probemos ahora que

$$r_3^{**}(N) \sim r_3(N)(\log N)^3,$$

para empezar veamos que los sumandos de $r_3^{**}(N)$ con algún $p_i < N/(\log N)^3$ contribuyen $o(N^2)$ y por lo tanto son despreciables,

sea $\bar{r}_3(N) = \sum_{p_1+p_2+p_3} \log p_1 \log p_2 \log p_3$ con alg*ún* $p_i < N/(\log N)^3$, entonces

$$\bar{r}_3(N) \leq \log\left(\frac{N}{(\log N)^3}\right)(\log N)^2 \sum_{p_3 \leq N/(\log N)^3} \sum_{p_1+p_2=N-p_3} 1 \qquad (11)$$

utilizando que

$$\sum_{p_1+p_2=N-p_3} 1 = \sum_{p_2 \leq N-p_3} \eta(N - p_3 - p_2) \cdot 1$$

la expresión (11) queda

$$\ll \log\left(\frac{N}{(\log N)^3}\right)(\log N)^2 \left(\frac{N}{(\log N)^3}\right)\left(\frac{N}{\log N}\right) \cdot 1 = o(N^2),$$

con lo que se verifica que podemos despreciar los sumandos con algún $p_i < N/(\log N)^3$ ya que son $o(N^2)$. Definamos,

$$\widehat{r}_3^{**}(N) = \sum_{p_1+p_2+p_3=N} \log p_1 \log p_2 \log p_3 \text{ tal que } \frac{N}{(\log N)^3} \leq p_i \leq N,$$

se tiene que

$$\lim_{N \longrightarrow \infty} \frac{r_3^{**}(N)}{r_3(N)(\log N)^3} = \lim_{N \longrightarrow \infty} \frac{\widehat{r}_3^{**}(N)}{\sum_{p_1+p_2+p_3=N}(\log N)^3}.$$

Como $N/(\log N)^3 \leq p_i \leq N$ al tomar logaritmos resulta

$$\log N - 3\log(\log N) \leq \log p_i \leq \log N$$

y con esto podemos mayorar y minorar los sumandos de $\widehat{r}_3^{**}(N)$ y obtenemos,

$$(\log N - 3\log(\log N))^3(\sum_{p_1+p_2+p_3=N} 1) \leq \widehat{r}_3^{**}(N) \leq (\sum_{p_1+p_2+p_3=N} 1)(\log N)^3,$$

finalmente como $(\log N - 3\log(\log N))^3 \sim (\log N)^3$, se deduce

$$r_3^{**}(N) \sim r_3(N)(\log N)^3$$

y el lema queda demostrado.□

A continuación conoceremos algunas funciones que serán necesarias para poder entender el siguiente teorema

- La función $\mu(n)$ de Möbius es,

$$\mu(n) = \begin{cases} (-1)^r, & \text{si} \quad n = p_1 \dots p_r \\ 1, & \text{si} \quad n = 1 \\ 0, & \text{si} \quad p^2 | n \end{cases}$$

- La función $\phi(n)$ de Euler es la cantidad de números menores que n y coprimos con él. Analíticamente escribimos,

$$\phi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

  o la expresión equivalente,

$$\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}.$$

- La siguiente función

$$\psi(x, \chi) = \sum_{n \leq x} \chi(n)\Lambda(n)$$

  se utiliza en la demostración del teorema del número primo en progresiones aritméticas[5], $(\pi(x; q, b) \sim Li(x)/\phi(q))$, véase [Ell]. Existe una estrecha relación entre el crecimiento de esta función y el error del teorema del número primo en progresiones aritméticas. Hoy en día sólo se sabe tratar el caso en el que q es extremadamente pequeño en comparación con x debido a que no se conoce la ausencia de ciertos ceros reales de la función $L(s, \chi) = \sum_{n=1}^{\infty} \chi(n)/n^s$ llamados ceros de Siegel que hacen necesario suponer que q sea mucho menor que x para que así el término de error de la ecuación (16) sea mayor que el primer término, (en el cual aparece el cero de Siegel), véase [Ell].

Teorema 4 *Sea* $S(x) = \sum_{n \leq N} \Lambda(n)e(nx)$, *si* $x \in \mathcal{M}_{a/q}$ *entonces*

$$S(x) = \frac{\mu(q)}{\phi(q)} \sum_{n \leq N} e((x - \frac{a}{q})n) + O(Ne^{-C\sqrt{\log N}})$$

para cierta constante $C > 0$.

[5]donde $Li(x) = \int_2^x dt/\log t$.

Antes de empezar la demostración del teorema veremos un lema y otro teorema que nos harán falta en la misma.

Lema 5 *Sea*

$$\tau(\chi) = \sum_{n=1}^{q-1} \chi(n) e(n/q),$$

donde χ son los caracteres módulo q, entonces se verifica que

$$\frac{1}{\phi(q)} \sum_{\chi} \tau(\bar{\chi})\chi(h) = \begin{cases} e(h/q), & si \quad (h,q) = 1 \\ 0 & si \quad (h,q) > 1 \end{cases}.$$

Demostración

Sustituyendo $\tau(\bar{\chi})$ por su definición obtenemos,

$$\frac{1}{\phi(q)} \sum_{\chi} \sum_{n} \bar{\chi}(n)\chi(h)e(n/q),$$

multiplicando los caracteres de la suma interior y aplicando que

$$\sum_{\chi} \chi(r) = \begin{cases} 0 & \text{si} \quad r \not\equiv 1 \ (q) \\ \phi(q) & \text{si} \quad r \equiv 1 \ (q) \end{cases}$$

se llega al resultado requerido.□

Teorema 6 (Teorema de Siegel) *Sea β_1 un cero de Siegel. Para todo $\varepsilon > 0$ existe $C_1(\varepsilon)$ tal que*

$$\beta_1 < 1 - C_1(\varepsilon) q^{-\varepsilon}.$$

Aquí no demostraremos este teorema, la prueba puede encontrarse en [Dav].

Demostración (teorema 4)

Sea $x = a/q + \beta$, con $(a,q) = 1$, aplicando el lema 5 y haciendo un sencillo cálculo se ve que

$$\sum_{\substack{k \le N \\ (k,q)=1}} \Lambda(k)e(kx) = \frac{1}{\phi(q)} \sum_{\chi} \tau(\bar{\chi})\chi(a) \sum_{k \le N} \chi(k)\Lambda(k)e(k\beta).$$

Como $S(x) = \sum_{n \le N} \Lambda(n)e(nx)$ podemos separar el sumatorio entre los k y q que son coprimos y los que no lo son.

La suma en los k que no son coprimos con q es $O((\log N)^2)$. Para ver esto supongamos que $q = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ y acotemos la suma,

$$\Big| \sum_{\substack{k \le N \\ (k,q)>1}} \Lambda(k)e(kx) \Big| \le \sum_{\substack{k \le N \\ (k,q)>1}} \Lambda(k) = \Lambda(p_1) + \Lambda(p_1^2) + \dots + \Lambda(p_1^{\beta_1}) + \dots + \Lambda(p_i^{\beta_i}) + \dots + \Lambda(p_r^{\beta_r}),$$

donde β_i, $i = 1 \dots r$ es la máxima potencia a la que aparecen elevados los factores de q para que se cumpla $p_j^{\beta_j} \leq N$; así que $\beta_j \leq \log N / \log p_j$, con lo que la suma anterior queda, [6]

$$\log N \cdot \text{ el número de factores de } q < \log N \log q \ll (\log N)^2$$

y se verifica que la suma en los k que no son coprimos con q es $O((\log N)^2)$.

Por lo tanto

$$S(x) = \frac{1}{\phi(q)} \sum_{\chi} \tau(\bar{\chi}) \chi(a) \sum_{k \leq N} \chi(k) \Lambda(k) e(k\beta) + O((\log N)^2). \tag{12}$$

Veamos qué ocurre al sumar en los k que son coprimos con q, llamemos S a la siguiente suma

$$\frac{1}{\phi(q)} \sum_{\chi} \tau(\bar{\chi}) \chi(a) \sum_{k \leq N} \chi(k) \Lambda(k) e(k\beta), \tag{13}$$

al aplicar el lema de Abel, (véase apéndice o [Ell]), se ve fácilmente que la suma interior es

$$= e(N\beta)\psi(N, \chi) - 2\pi i \beta \int_1^N e(u\beta)\psi(u, \chi) du. \tag{14}$$

Acotemos (14), para ello tendremos que hacer algunas consideraciones previas,

- Si $\chi \neq \chi_0$ supongamos que

  $$q \leq \exp[C(\log u)^{1/2}], \tag{15}$$

  donde C es una constante positiva, entonces por la demostración del teorema del número primo en progresiones aritméticas, (véase [Dav]),

  $$\psi(u, \chi) = -\frac{u^{\beta_1}}{\beta_1} + O\{u \exp[-C'(\log u)^{1/2}]\}, \tag{16}$$

  siendo C' una constante positiva que depende sólo de C y β_1 el posible cero de Siegel.

- Utilizando el teorema de Siegel se tiene

  $$u^{\beta_1} < u \exp[-C_1(\varepsilon)(\log u) q^{-\varepsilon}]. \tag{17}$$

[6] Para ver que el número de factores de q es menor que $\log q$, basta tomar logaritmos y acotar,

$$\log q = \beta_1 \log p_1 + \beta_2 \log p_2 + \ldots \geq \beta_1 + \beta_2 + \ldots + \beta_r.$$

Comencemos acotando la integral de (14), para ello veamos que

$$|\psi(u,\chi)| \ll u\exp[-C_3(\log u)^{1/2}], \tag{18}$$

para todo carácter no principal $\chi \pmod q$. Nos interesará que (17) sea pequeña comparada con x para que el término de error en (16) tenga más importancia que el primer sumando. Para conseguir esto se debe imponer una restricción sobre q más severa que la expresada en (15). Supongamos ahora que

$$q \leq (\log u)^D, \tag{19}$$

para alguna constante positiva D. Entonces eligiendo $\varepsilon = (2D)^{-1}$, obtenemos $q^\varepsilon \leq (\log u)^{1/2}$ y de (16) y (17) se deduce (18) para todo carácter no principal $\chi \pmod q$. Aplicando (18) la integral de (14) ya se puede acotar,

$$\int_1^N (\quad) = \int_1^{Ne^{-c\sqrt{\log N}}} (\quad) + \int_{Ne^{-c\sqrt{\log N}}}^N (\quad) \ll N^2 e^{-2C\sqrt{\log N}} + Ne^{\tilde{C}\sqrt{\log N}}$$

y a partir de aquí es fácil ver que la suma interior de (13) es

$$\ll (1+|\beta|N)N\exp(-C\sqrt{\log N}), \tag{20}$$

donde hemos renombrado, $C_3 = C$.

Para tratar χ_0, tenemos en cuenta que

$$\psi(u,\chi_0) = \sum_{n\leq u}\Lambda(n)\chi_0(n) \leq \sum_{n\leq u}\Lambda(n) = \psi(u),$$

y esto por el teorema del número primo es

$$u + O(ue^{-c(\log u)^{1/2}}) = [u] + R(u),$$

donde $R(u) = O(ue^{-c(\log u)^{1/2}}) + Frac(u) = O(ue^{-c(\log u)^{1/2}})$.

Sea $T(\beta) = \sum_{k\leq N} e(k\beta)$. De nuevo, aplicando el lema de Abel es fácil ver que

$$T(\beta) = e(N\beta)N - 2\pi i\int_1^N e(n\beta)[u]du.$$

Utilizando esto y (14) evaluemos,

$$\sum_{k\leq N}\chi_0(k)\Lambda(k)e(k\beta) = T(\beta) + e(N\beta)R(N) - 2\pi i\int_1^N e(N\beta)R(u)du$$

$$= T(\beta) + O((1+|\beta|N)N\exp(-c(\log N)^{1/2})).$$

Sabemos, ver [Dav], capítulo 9, que $\tau(\chi_0) = \mu(q)$ y que $|\tau(\chi)| \leq q^{1/2}$ para cualquier carácter χ (mod q). Combinando estas estimaciones en (12) concluimos que [7]

$$S(x) = \frac{\mu(q)}{\phi(q)} T(\beta) + O((1 + |\beta|N)q^{1/2} N \exp(-c(\log N)^{1/2}).$$

Como $q \leq P$ y $|\beta| \leq 1/Q$ para todo x perteneciente a los arcos mayores, entonces

$$S(x) = \frac{\mu(q)}{\phi(q)} T(\beta) + O((N \exp(-c_1(\log N)^{1/2}),$$

para todo $x \in \mathcal{M}_{a/q}$. □

Teorema 7 *Si*

$$\left| x - \frac{a}{q} \right| \leq \frac{1}{q^2} \quad \text{con} \quad (a, q) = 1, \tag{21}$$

entonces

$$S(x) \ll (Nq^{-1/2} + N^{4/5} + (Nq)^{1/2})(\log N)^4$$

Antes de probar el teorema veamos un lema y una proposición que utilizaremos en la prueba.

Lema 8 *Si x satisface (21) entonces*

$$\sum_{t \leq T} \text{mín}(\frac{N}{t}, \frac{1}{\|tx\|}) \ll \left(\frac{N}{q} + T + q \right) \log(2qT)$$

Para demostrar este lema nos hará falta un pequeño lema auxiliar,

Lema 9 *Supongamos que h está dado y sea $I = [A, B]$, un intervalo en $[0, 1]$ de longitud $1/q$. Hay como mucho 4 valores de r, $1 \leq r \leq q$, para los cuales*

$$\frac{ra}{q} + hq\beta + r\beta \in I \text{ (mod 1)}.$$

Demostración

Sabemos que $|r\beta| \leq 1/q$. Si r es tal que se cumple el enunciado entonces $\exists m$ tal que

$$A \leq \frac{a}{q} r + hq\beta + r\beta - m \leq B, \text{ por tanto } A - hq\beta - \frac{1}{q} \leq \frac{a}{q} r - m \leq B - hq\beta + \frac{1}{q}.$$

[7] La razón por la que q debe ser pequeño es que en caso contrario no podríamos aplicar el teorema de los números primos en progresiones aritméticas y no habría cancelación en la fórmula anterior.

Como $B - A = 1/q$, se tiene $(B - hq\beta + 1/q) - (A - hq\beta - 1/q) = 3/q$ y por consiguiente existe s tal que $s/q \leq (a/q)r - m \leq (s+3)/q$. Multiplicando por q esto equivale a $ar \equiv s, s+1, s+2, s+3 \bmod q$, por lo tanto r toma cuatro valores.□

Demostración (lema 8)

Sea $t = hq + r$ con $1 \leq r \leq q$, y $\beta = x - a/q$. Entonces

$$\sum_{t \leq T} \text{mín}(\frac{N}{t}, \frac{1}{\|tx\|}) \ll \sum_{h=0}^{T/q} \sum_{r=1}^{q} \text{mín}(\frac{N}{hq+r}, \frac{1}{\|ra/q + r\beta + hq\beta\|}).$$

Consideraremos a continuación los términos con $h = 0$ y $1 \leq r \leq q/2$, para estos r se cumple que $|r\beta| \leq 1/2q$, así que mayorando con el criterio de la integral vemos que la contribución de estos términos es

$$\ll \sum_{r=1}^{q/2} \frac{1}{\|\frac{ra}{q}\| - \frac{1}{2q}} \ll q \log q \ .$$

En los términos restantes se verifica que $hq + r \gg (h+1)q$, supongamos que h está dado y sea I un intervalo en $[0,1]$ de longitud $1/q$ por el lema 9 sabemos que hay a lo más cuatro valores de r, $1 \leq r \leq q$, para los cuales

$$\frac{ra}{q} + hq\beta + r\beta \in I \ (\text{mod } 1).$$

Por lo tanto procediendo como antes nos queda,

$$\sum_{h=0}^{T/q} \sum_{r=1}^{q} \text{mín}(\frac{N}{(h+1)q}, \frac{1}{\|ra/q + r\beta + hq\beta\|}) \ll \sum_{h=0}^{T/q} \left(\frac{N}{(h+1)q} + q \log(2q) \right) \tag{22}$$

y como

$$\sum_{h=0}^{T/q} \frac{N}{(h+1)q} \ll \frac{N}{q} \log \frac{T}{q} \quad \text{y} \quad \sum_{h=0}^{T/q} q \log 2q \ll (\frac{T}{q} + 1) q \log(2q)$$

entonces (22) queda

$$\ll \left(\frac{N}{q} + T + q \right) \log 2qT.$$

y se concluye la demostración del lema.□

Proposición 3.1 *Si* $|f(n)| \leq 1$ *para todo* n, $U \geq 2$, $V \geq 2$, $UV \leq N$, *entonces*

$$\sum_{n \leq N} f(n)\Delta(n) \ll U + (\log N) \sum_{t \leq UV} \max_{w} \left| \sum_{r=w}^{T/q} f(rt) \right|$$

$$+N^{1/2}(\log N)^3 \max_{U\le M\le N/V}\max_{V\le j\le N/M}\Big(\sum_{V\le k\le N/M}\Big|\sum_{\substack{M\le m\le 2M\\ m\le N/k\\ m\le N/j}} f(mj)\overline{f(mk)}\Big|\Big)^{1/2} \quad (23)$$

La prueba de esta proposición se puede encontrar en [Dav].

Demostración (teorema 7)

Para probar el teorema 7 utilizaremos la siguiente desigualdad,

$$\sum_{N_1}^{N_2} e(n\beta) = \frac{e((N_2+1)\beta) - e(N_1\beta)}{e(\beta)-1)} \ll \min\left(N_2 - N_1, \frac{1}{\|\beta\|}\right), \quad (24)$$

donde $\|\beta\|$ denota la distancia de β al entero más cercano. Por lo tanto

$$\sum_{t\le T}\max_{w}\left|\sum_{r=w}^{N/T} e(rtx)\right| \ll \sum_{t\le T}\min\left(\frac{N}{t}, \frac{1}{\|tx\|}\right). \quad (25)$$

Aplicando la proposición 3.1 y el lema 8 obtenemos,

$$S(x) \ll U + \left(\frac{N}{q} + UV + q\right)(\log 2qN)^2$$

$$+N^{1/2}(\log N)^3 \max_{U\le M\le N/V}\max_{V<j\le N/M}\left(\sum_{V<k\le N/M}\min\left(M, \frac{1}{\|(k-j)x\|}\right)\right)^{1/2}. \quad (26)$$

El último término de la ecuación anterior es

$$\ll N^{1/2}(\log N)^3 \max_{U\le M\le N/V}\left(M + \sum_{m=1}^{N/M}\min\left(\frac{N}{m}, \frac{1}{\|mx\|}\right)\right)^{1/2}$$

y aplicando el lema 8 este último término resulta ser

$$\ll (NV^{-1/2} + NU^{-1/2} + Nq^{-1/2} + (Nq)^{1/2})(\log qN)^4.$$

Así que si unimos los dos sumandos de (26) obtenemos

$$S(x) \ll (UV + q + NV^{-1/2} + NU^{-1/2} + Nq^{-1/2} + (Nq)^{1/2})(\log qN)^4,$$

por tanto si $q > N$ la tesis de nuestro teorema es trivial, por lo que suponemos que $q \le N$ en este caso $q \le (Nq)^{1/2}$ y tomando $U = V = N^{2/5}$ el teorema queda demostrado.□

Por último veremos una definición y con ella ya estaremos preparados para demostrar el teorema de Vinogradov,

Definición 3.1 *Se conoce como suma de Ramanujan a la siguiente expresión*

$$c_q(N) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e\left(\frac{Na}{q}\right).$$

Es una función multiplicativa, (como veremos posteriormente), y por los teoremas 67 y 272 de [Ha-Wr] verifica

$$c_q(N) = \frac{\mu(q/(q,N))\phi(q)}{\phi(q/(q,N))},$$

donde (q, N) es el máximo común divisor de q y N.

Sea

$$r_3(N) = \sum_{p_1+p_2+p_3=N} 1,$$

y sea

$$f_N(x) = \sum_{p\leq N} e(px), \tag{27}$$

donde p recorre los primos. Por lo tanto,

$$r_3(N) = \int_0^1 (\sum_{p\leq N} e(px))^3 e(-Nx)dx. \tag{28}$$

Si conseguimos información sobre $(\sum_{p\leq N} e(px))^3$, podemos esperar deducir información sobre $r_3(N)$ a partir de la integral anterior. Con un buen análisis de las singularidades del integrando, es decir, usando el método del círculo, podremos obtener grandes conclusiones.

Así pues, comenzamos estudiando las singularidades de (27), para ello analizaremos la función en algunos valores racionales[8] de x :

$$f_N\left(\frac{0}{1}\right) = \sum_{p\leq N} 1 = \pi(N)$$

$$f_N\left(\frac{1}{2}\right) = \sum_{p\leq N} e^{i\pi p} = e^{2\pi i} + e^{3\pi i} + e^{5\pi i} + \ldots = 1 + e^{2\pi i\frac{1}{2}}\pi(N, 2, 1),$$

[8]Estudiamos la función en algunos valores racionales porque en estos valores podremos estimar $f_N(a/q)$ usando información sobre la densidad de los primos en progresiones aritméticas.

siendo $\pi(N,q,r)$ la cantidad de primos menores que N en la progresión aritmética
$\{qn+r\}_{n=1}^{\infty}$ con q y r primos entre sí.

$$f_N\left(\frac{1}{3}\right) = \sum_{p\leq N} e^{\frac{2\pi i p}{3}} = e^{\frac{4\pi i}{3}} + e^{2\pi i} + e^{\frac{10\pi i}{3}} + e^{\frac{14\pi i}{3}} + \dots$$

$$= 1 + e^{2\pi i\frac{1}{3}}\pi(N,3,1) + e^{2\pi i\frac{2}{3}}\pi(N,3,2).$$

$$f_N\left(\frac{2}{3}\right) = \sum_{p\leq N} e^{2\pi i p\frac{2}{3}} = e^{\frac{8\pi i}{3}} + e^{4\pi i} + e^{\frac{20\pi i}{3}} + e^{\frac{28\pi i}{3}} + \dots$$

$$= 1 + e^{2\pi i\frac{2}{3}}\pi(N,3,1) + e^{2\pi i\frac{1}{3}}\pi(N,3,2).$$

Si a/q es una fracción irreducible con $a \neq 0$ podemos escribir,

$$f_N\left(\frac{a}{q}\right) = \sum_{r=1}^{q} e^{2\pi i\frac{ra}{q}}\pi(N,q,r) + \sum_{p|q} e^{2\pi i\frac{pa}{q}}, \tag{29}$$

donde $(r,q) = 1$ son coprimos entre sí y el segundo sumando se extiende a factores primos p de q. Esperamos que $f_N(x)$ alcance los valores mayores cuando q es pequeño ya que el primer sumatorio de la ecuación anterior tiene pocos términos y no es muy probable que induzcan mucha cancelación. Para estos valores $f_N(x)$ se puede aproximar de forma precisa.

Como ya dijimos en la sección 1 el método del círculo consiste en dividir el intervalo de integración $[0,1]$, en dos subconjuntos para nosotros ya conocidos, los arcos mayores, $\mathcal{M}$, y los arcos menores, m. Los arcos mayores contienen valores singulares de $f_N(x)$ y por ello contribuyen más a la integral, los arcos menores están formados por los valores donde $f_N(x)$ no es muy grande.

El que el método del círculo funcione se debe a que se obtiene una aproximación muy precisa de la integral en los arcos mayores y a la vez se consigue que estos arcos sean suficientemente grandes para minimizar así la influencia de los arcos menores en los que "sólo" conseguimos una cota.

En el problema concreto que nosotros estamos tratando ahora, M contiene los puntos cercanos a los racionales de denominador pequeño (ya que en estos puntos podemos obtener una fórmula asintótica que nos permitirá aproximar la integral) y m al resto de puntos del intervalo $[0,1]$.

Antes de definir explícitamente los arcos mayores, recordemos utilizando el teorema 2, que dados dos números reales x y Q existe un único racional, a/q, tal que $|x - a/q| \leq 1/qQ$, para algunos x, q será muy pequeño, (estos x estarán muy bien aproximados) y para otros, q estará más cercano a Q; una vez recordado esto podemos definir los arcos mayores.

La forma típica de los arcos mayores es

$$\mathcal{M}_{a/q} = \{x \in \mathbb{T} \ : \ |x - a/q| < 1/Q\} \quad \text{con} \ \ 1 \leq a \leq q \leq P, \ y \ (a,q) = 1,$$

(sólo existe un número finito de racionales a/q que cumpla las condiciones anteriores). También conviene recordar que el toro $\mathbb{T}$ es el intervalo $[0,1]$ con los extremos identificados. Así $|x| < \varepsilon$ es $[0,\varepsilon) \cup (1-\varepsilon, 1]$.

Si $P < \sqrt{Q/2}$ entonces $\mathcal{M}_{a/q}$ son disjuntos.

Veámoslo, en $\mathcal{M}_{a/q}$ tenemos $|x - a/q| < 1/Q$. Para que dos intervalos sean disjuntos la distancia entre centros debe ser mayor que dos radios, es decir, $|a/q - a'/q'| > 2/Q$, por otra parte $|(q'a - qa')/qq'| \geq 1/P^2$, ya que $q < P$, así que si $1/P^2 > 2/Q$ los centros estarán separados por más de dos radios y por lo tanto los intervalos serán disjuntos.

En nuestro caso, tomaremos los arcos mayores correspondientes a $Q = N/(\log N)^{20}$ y $P = (\log N)^{20}$. (Se puede sustituir 20 por un número grande cualquiera).

Demostración (teorema 1)

Por el lema 3 sabemos que $r_3^*(N) \sim r_3(N)(\log N)^3$, así que podemos trabajar con $r_3^*(N)$ en vez de $r_3(N)$, aunque $r_3^*(N)$ es un función menos natural que $r_3(N)$, nos facilitará las cosas técnicamente.

Sea $S(x) = \sum_{n \leq N} \Lambda(n) e(nx)$, podemos escribir $r_3^*(N)$ en términos $S(x)$. Como

$$r_3^*(N) = \sum_{p_1^k + p_2^k + p_3^k = N} \log p_1 \log p_2 \log p_3,$$

al elevar $S(x)$ al cubo observamos que,

$$S(x)^3 = \sum_{m=0}^{N} \sum_{n_1+n_2+n_3=m} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3) e(mx) + \sum_{m=N+1}^{3N} a_m e(mx),$$

donde los términos del último sumando no influyen en los desarrollos posteriores. Multiplicando por $e(-xN)$ e integrando sobre cualquier intervalo unidad obtenemos

$$r_3^*(N) = \int_{-1/2}^{1/2} S(x)^3 e(-Nx) dx. \tag{30}$$

Usemos la fórmula asintótica dada por el teorema 4 y (30) para calcular cuál es la contribución de todos los arcos mayores.

$$\int_{\mathcal{M}_{a/q}} S(x)^3 e(-Nx) dx =$$

$$= \int_{\mathcal{M}_{a/q}} \left(\frac{\mu(q)}{\phi(q)} \sum_{n \leq N} e((x - \frac{a}{q})n) + O(Ne^{-C\sqrt{\log N}}) \right)^3 e(-Nx)dx.$$

Utilizando que $(A+B)^3 = A^3 + O(|A|^2|B| + |B|^3)$, se tiene

$$\int_{\mathcal{M}_{a/q}} \left(\frac{\mu(q)}{\phi(q)} \sum_{n \leq N} e((x - \frac{a}{q})n) + O(Ne^{-C\sqrt{\log N}}) \right)^3 e(-Nx)dx$$

$$= \int_{\mathcal{M}_{a/q}} \left(\frac{\mu(q)}{\phi(q)} \sum_{n \leq N} e((x - \frac{a}{q})n) \right)^3 e(-Nx)dx + \int_{\mathcal{M}_{a/q}} O(N^3 e^{-C\sqrt{\log N}})dx.$$

Llamemos I_1 a la primera integral e I_2 a la segunda integral, tras el cambio de variable, $x = a/q + u$, $dx = du$,

$$I_1 = \int_{-1/Q}^{1/Q} \left(\frac{\mu(q)}{\phi(q)} \right)^3 \left(\sum_{n \leq N} e(un) \right)^3 e(-Na/q - Nu)du$$

$$= \left(\frac{\mu(q)}{\phi(q)} \right)^3 e(-Na/q) \int_{-1/Q}^{1/Q} \left(\sum_{n \leq N} e(xn) \right)^3 e(-Nx)dx.$$

Vayamos ahora con la segunda integral,

$$I_2 \ll \int_{\mathcal{M}_{a/q}} N^3 e^{-C\sqrt{\log N}} dx = N^2 O(e^{-C'\sqrt{\log N}}).$$

Denotaremos $\mathcal{A}_M$ a la contribución de todos los arcos mayores, por todo lo anterior deducimos que

$$\mathcal{A}_M = \sum_{q \leq P} \left(\frac{\mu(q)}{\phi(q)} \right)^3 c_q(-N) \int_{-1/Q}^{1/Q} \left(\sum_{n \leq N} e(xn) \right)^3 e(-Nx)dx + N^2 O(e^{-C'\sqrt{\log N}}),$$

con $C' > 0$ y $c_q(-N) = \sum_a e(-Na/q)$, donde la suma se restringe a aquellos a entre 1 y q tales que sean coprimos con q. Por otro lado,

$$\int_{-1/Q}^{1/Q} \left(\sum_{n \leq N} e(xn) \right)^3 e(-Nx)dx = \int_{-1/2}^{1/2} (\quad) - \int_{1/Q}^{1/2} (\quad) - \int_{1/2}^{-1/Q} (\quad),$$

la primera integral la conocemos por la sección 2, es $N(N+1)/2$, y las dos integrales restantes se pueden acotar. Sabemos que $|\sum_{n \leq N} e(nx)| \ll |x|^{-1}$, por lo que

$$\int_{1/Q}^{1/2} \left(\sum_{n \leq N} e(xn) \right)^3 e(-Nx)dx \ll \int_{1/Q}^{1/2} \frac{1}{|x|^3} dx = O(Q^2),$$

la integral que queda se acota igual, por lo tanto

$$\int_{-1/Q}^{1/Q}\left(\sum_{n\leq N}e(xn)\right)^3 e(-Nx)dx=\frac{N^2}{2}+O\left(\frac{N^2}{(\log N)^{40}}\right).$$

Con esto

$$\mathcal{A}_M=\sum_{q\leq P}\left(\frac{\mu(q)}{\phi(q)}\right)^3 c_q(-N)\frac{N^2}{2}+$$

$$+\sum_{q\leq P}\left(\frac{\mu(q)}{\phi(q)}\right)^3 c_q(-N)O\left(\frac{N^2}{(\log N)^{40}}\right)+N^2O(e^{-C'\sqrt{\log N}}),$$

el segundo sumando se puede operar,

$$\sum_{q\leq P}\left(\frac{\mu(q)}{\phi(q)}\right)^3 c_q(-N)O\left(\frac{N^2}{(\log N)^{40}}\right)=O\left(\frac{N^2}{(\log N)^{40}}\sum_{q\leq P}\frac{1}{\phi^2(q)}\right)=O\left(\frac{N^2}{(\log N)^{40}}P\right)$$

$$=O\left(\frac{N^2}{(\log N)^{20}}\right),$$

así que $\mathcal{A}_M$ queda,

$$\mathcal{A}_M=\left(\frac{N^2}{2}\right)\sum_{q\leq P}\left(\frac{\mu(q)}{\phi(q)}\right)^3 c_q(-N)+O\left(\frac{N^2}{(\log N)^{20}}\right)+N^2O(e^{-C'\sqrt{\log N}})$$

y el último sumando se puede despreciar, (tomando logaritmos se ve que es es más pequeño que el resto). Extendiendo el sumatorio hasta infinito

$$\sum_{q=1}^{\infty}\left|\frac{\mu(q)}{\phi(q)}\right|^3|c_q(-N)|\leq\sum_{q=1}^{\infty}\frac{1}{\phi(q)^2},$$

y se puede comprobar que esta suma es convergente, para ello observemos que $\phi(q)\gg q/\log q$, lo que implica que

$$\sum_{q=1}^{\infty}\frac{1}{\phi(q)^2}\ll\sum_{q=1}^{\infty}\left(\frac{\log q}{q}\right)^2<\infty.$$

Así que podemos escribir,

$$\mathcal{A}_M=\frac{N^2}{2}\sum_{q=1}^{\infty}\left(\frac{\mu(q)}{\phi(q)}\right)^3 c_q(-N)-\frac{N^2}{2}\sum_{q=P}^{\infty}\left(\frac{\mu(q)}{\phi(q)}\right)^3 c_q(-N)$$

$$+O\left(\frac{N^2}{(\log N)^{20}}\right),$$

$$\text{pero}\ \ \sum_{q=P}^{\infty}\left(\frac{\mu(q)}{\phi(q)}\right)^3 c_q(-N)\ \ \text{es}\ O(\frac{N^2}{(\log N)^{19}})\ \ \text{ya que,}$$

$$\sum_{q=P}^{\infty}\left(\frac{\mu(q)}{\phi(q)}\right)^3 c_q(-N) \ll \sum_{q=P}^{\infty}\frac{(\log q)^2}{q^2} \ll \sum_{q=P}^{\infty}\frac{1}{q^{2-\varepsilon}} \ll P^{-1+\varepsilon} \tag{31}$$

y tomando $\varepsilon = 1/20$ llegamos a que la ecuación anterior es como $O((\log N)^{-19})$ con lo que se concluye que

$$\mathcal{A}_M = \frac{N^2}{2}\sum_{q=1}^{\infty}\left(\frac{\mu(q)}{\phi(q)}\right)^3 c_q(-N) + O\left(\frac{N^2}{(\log N)^{19}}\right).$$

La expresión que tenemos para $\mathcal{A}_M$ se puede simplificar, para ello utilizaremos algunas propiedades de las sumas de Ramanujan.

1. La función $c_q(-N)$ cumple que es una función multiplicativa en q, esto es, si q_1 y q_2 son coprimos $c_{q_1q_2}(-N) = c_{q_1}(-N)c_{q_2}(-N)$, veámoslo:

$$c_{q_1}(-N)c_{q_2}(-N) = \sum_{\substack{a=1\\(a,q_1)=1}}^{q_1} e\left(\frac{-Na}{q_1}\right)\sum_{\substack{a=1\\(a,q_2)=1}}^{q_2} e\left(\frac{-Na}{q_2}\right)$$

$$= \sum_{\substack{a=1\\(a,q_1)=1}}^{q_1}\sum_{\substack{a=1\\(a,q_2)=1}}^{q_2} e\left(\frac{-Na}{q_1}\right)e\left(\frac{-Na}{q_2}\right) = \sum_{\substack{a=1\\(a,q_1)=1}}^{q_1}\sum_{\substack{a=1\\(a,q_2)=1}}^{q_2} e\left(\frac{-Na(q_2-q_1)}{q_1q_2}\right),$$

definamos $\tilde{a} = a(q_2 - q_1)$, entonces la expresión anterior será igual a

$$\sum_{\substack{\tilde{a}=1\\(\tilde{a},q_1q_2)=1}}^{q_1q_2} e\left(\frac{-N\tilde{a}}{q_1q_2}\right) = c_{q_1q_2}(-N)$$

y queda demostrado que la función $c_q(-N)$ es multiplicativa.

2. Si p es primo y $p|N$ entonces $c_p(-N) = p - 1$, ya que

$$c_p(-N) = \sum_{\substack{a=1\\(a,p)=1}}^{p} 1 = \phi(p) = p - 1.$$

3. Si $p \nmid N$,

$$c_p(-N) = \sum_{\substack{a=1\\(a,p)=1}}^{p-1} e(-Na/p) = \sum_{\substack{a=1\\(a,p)=1}}^{p} e(-Na/p) - e(-N) = 0 - 1 = -1,$$

donde el primer sumatorio es 0 ya que es la suma de las raíces p-ésimas de la unidad y éstas suman cero.

Sea $f(n) = \left(\frac{\mu(n)}{\phi(n)}\right)^3 c_n(-N)$, entonces f es multiplicativa (está compuesta por funciones multiplicativas) y $f(p^k) = 0$ para $k \geq 2$ (debido a la definición de $\mu(n)$), por tanto

$$\sum_{n=1}^{\infty} f(n) = \prod_{p}(1 + f(p)) = \prod_{p}\left(1 + \left(\frac{\mu(p)}{\phi(p)}\right)^3 c_p(-N)\right)$$

y a partir las definiciones de $\mu(p)$ y $\phi(p)$, y de aplicar las propiedades que acabamos de ver sobre $c_q(-N)$ se deduce que la expresión anterior es igual a

$$\sum_{n=1}^{\infty} f(n) = \prod_{p|N}\left(1 - \frac{1}{(p-1)^2}\right)\prod_{p\nmid N}\left(1 + \frac{1}{(p-1)^3}\right). \tag{32}$$

La expresión de $\mathcal{A}_M$ se simplifica notablemente teniendo en cuenta (32), obteniéndose

$$\mathcal{A}_M = \frac{N^2}{2}\prod_{p|N}\left(1 - \frac{1}{(p-1)^2}\right)\prod_{p\nmid N}\left(1 + \frac{1}{(p-1)^3}\right) + O\left(\frac{N^2}{(\log N)^{19}}\right). \tag{33}$$

Para seguir con la demostración del teorema de Vinogradov, veamos cuanto contribuyen los arcos menores. A la cantidad que contribuyen los arcos menores la llamaremos, $\mathcal{A}_m$. Por el teorema de Dirichlet, sabemos que $|x - a/q| < 1/qN$ con $1 \leq q \leq N$, aplicando este teorema teniendo en cuenta que $P < q \leq Q$, (si $q \leq P$ estaríamos en un arco mayor), obtenemos

$$|x - a/q| < 1/qQ < 1/q^2,$$

con lo que se deduce que para todo x en los arcos menores debe existir a/q que cumpla la desigualdad anterior y aplicando el teorema 7 se tiene

$$S(x) \ll (Nq^{-1/2} + N^{4/5} + (Nq)^{1/2})(\log N)^4,$$

así que en los arcos menores, $S(x) = O(N/\log^6 N)$. A partir de lo anterior, concluimos que la contribución en los arcos menores es,

$$\mathcal{A}_m = \int_m S^3(x)e(-Nx)dx \ll \frac{N}{\log^6 N}\int_0^1 |S(x)|^2 dx.$$

Recordando que $S(x) = \sum_{p^k \leq N} \log p \; e(xp^k)$ y utilizando la identidad de Parseval y el teorema de los números primos obtenemos

$$\int_0^1 |S(x)|^2 = \sum_{p^k \leq N}(\log p)^2 \ll (\log N)^2 \sum_{p^k \leq N} 1 \ll \frac{N}{\log N}(\log N)^2 = N \log N,$$

por lo que

$$\mathcal{A}_m = \int_m S^3(x)e(-Nx)dx \ll \frac{N}{\log^6 N}\int_0^1 |S(x)|^2 dx \ll \frac{N^2}{\log^5 N} = o(N^2).$$

Una vez que conocemos la contribución de los arcos menores y de los arcos mayores resulta

$$r_3(N) = \frac{N^2}{2} \prod_{p|N} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p\nmid N} \left(1 + \frac{1}{(p-1)^3}\right) + o(N^2) \qquad (34)$$

El primer producto para N par "no funciona", se anula, (ya que si N es par 2 divide a N y $(1-1/(p-1)^2)$ sería 0), y por tanto no obtenemos una fórmula asintótica. Además como $N = p_1 + p_2 + p_3$, para que N sea par forzosamente algún p_i debe ser 2 ya que la suma de tres impares es impar y el resto de los primos son impares; suponiendo que $p_1 = 2$ tendríamos $N = 2 + p_2 + p_3$ lo que implica que $N - 2 = p_2 + p_3$, $N - 2$ será un número par, llamémosle $\widetilde{N}$, entonces $\widetilde{N} = p_2 + p_3$ y esta igualdad nos dice que un número par es suma de dos primos, es decir, nos hemos encontrado aquí con la conjetura de Goldbach.

Si N es impar,

$$\prod_{p\nmid N} \left(1 + \frac{1}{(p-1)^3}\right) \geq 2$$

y

$$\prod_{p|N} \left(1 - \frac{1}{(p-1)^2}\right) \geq \text{ cte} > 0, \qquad (35)$$

para comprobar esta última desigualdad, si tomamos logaritmos tenemos,

$$\log \prod_{p|N}(\quad) = \sum \log(\quad), \text{y como } \log\left(1 - \frac{1}{(x-1)^2}\right) \sim \frac{1}{x^2}$$

y la expresión (35) queda verificada.

Por otra parte,

$$\prod_{p|N} \left(1 - \frac{1}{(p-1)^2}\right) \leq 1$$

y

$$\prod_{p\nmid N} \left(1 + \frac{1}{(p-1)^3}\right) \leq \prod_{n=2}^{\infty} \left(1 + \frac{1}{(n-1)^3}\right) = \text{cte}, \qquad (36)$$

comprobemos que el último producto que hemos utilizado para mayorar converge y es realmente una constante. Para ver si converge, tomamos logaritmos, sabemos que

$$\prod_{n=2}^{\infty}(\quad) \text{ converge y no es nulo } \iff |\sum_{n=2}^{\infty} \log(\quad)| \neq \infty$$

Por lo tanto veamos que

$$\sum_{n=2}^{\infty} \log\left(1 + \frac{1}{(n-1)^3}\right) \neq \infty,$$

utilizando el criterio de comparación con

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

que es mayor, concluimos que converge.

Con esto podemos afirmar que si N es impar

$$\prod_{p|N} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p\nmid N} \left(1 + \frac{1}{(p-1)^3}\right)$$

está entre dos constantes positivas (independientes de N), por tanto el primer sumando de la expresión (34) es mayor que cero y el otro sumando se puede despreciar, (es menor que N^2). Así que finalmente hemos obtenido que $r_3(N)$ es mayor que cero , de hecho $r_3(N) \gg N^2$, lo que quiere decir que exite al menos una forma de representar N como suma de tres primos, con lo que queda demostrado el teorema de Vinogradov y por lo tanto una parte de la conjetura original de Goldbach.□

El teorema de Vinogradov se puede generalizar para un número, $k > 3$, es decir, podemos hallar una fórmula asintótica para el número de representaciones de un entero suficientemente grande como suma de k primos.

Teorema 10 *Sea $r_k(N)$ el número de formas de escribir un entero, N, como suma de k primos. Si $k \geq 3$ y $N \equiv k \pmod 2$, entonces*

$$r_k(N) = \Xi_k(N) \frac{N^{k-1}}{(\log N)^k} + O\left(\frac{N^{k-1} \log\log N}{(\log N)^{k+1}}\right),$$

donde

$$\Xi_k(N) = \frac{2}{(k-1)!} \prod_{p>2} \left(1 - \left(\frac{-1}{p-1}\right)^k\right) \prod_{\substack{p|N \\ p>2}} \frac{(p-1)^k + (-1)^k(p-1)}{(p-1)^k - (-1)^k}$$

$$= \frac{1}{(k-1)!} \prod_{p\nmid N} \left(1 - \frac{(-1)^k}{(p-1)^k}\right) \prod_{p|N} \left(1 + \frac{(-1)^k}{(p-1)^{k-1}}\right)$$

y $C_1(k) < \Xi_k(N) < C_2(k) < \infty$ para todo N.

La demostración de este teorema es muy similar a la del caso $k = 3$, (los resultados para $k = 3$ se generalizan para $k > 3$,) se puede encontrar en [Ell], (capítulo 9).

4. El problema binario de Goldbach

Como sabemos, la conjetura de Goldbach, "todo número par mayor que dos se puede representar como suma de dos primos", está avalada por extensas tablas numéricas pero todavía constituye un problema abierto. Su dificultad radica en que, a diferencia de lo que ocurre con $r_k(N)$ para $k > 3$, al aplicar el método del círculo, la contribución de los arcos menores supera al término principal con los conocimientos actuales. No obstante, es posible probar una fórmula en promedio que permite concluir que casi todo par es suma de dos primos (de muchas formas distintas). Concretamente estudiaremos la cantidad,

$$\sum_{N=1}^{\hat{N}} \left| r_2(N) - N \prod_{p\nmid N} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p|N} \left(1 + \frac{1}{(p-1)}\right) \right|^2 ,$$

donde

$$r_2(N) = \sum_{p_1+p_2=N} 1.$$

Teorema 11

$$\sum_{N=1}^{\hat{N}} |r_2(N) - N\Xi(N)|^2 \ll \frac{\hat{N}^3}{(\log \hat{N})^{11}}.$$

Demostración (teorema 11)

Análogamente al problema ternario, usando los mismos razonamientos, podemos decir que

$$r_2(N) = \int_{\mathcal{M}} (\sum_{p\leq N} e(px))^2 e(-Nx)dx + \int_m (\sum_{p\leq N} e(px))^2 e(-Nx)dx.$$

En toda esta sección los arcos mayores y menores, así como las funciones denotadas con las mismas letras coincidirán con las de la sección anterior y se podría demostrar al igual que antes que si $r_2^*(N) \gg N$

$$r_2^*(N) \sim r_2^{**}(N) \sim r_2(N) \log^2(N).$$

Veamos la integral sobre los arcos mayores, como en el caso anterior si $S(x) = \sum_{n\leq N} \Lambda(n)e(nx)$, podemos escribir $r_2^*(N)$ en términos de $S(x)$, veámoslo

$$r_2^*(N) = \sum_{n_1+n_2=N} \Lambda(n_1)\Lambda(n_2),$$

y al elevar $S(x)$ al cuadrado observamos que,

$$S(x)^2 = \sum_{m=1}^{N} \sum_{n_1+n_2=m} \Lambda(n_1)\Lambda(n_2)e(mx) + \sum_{m=N+1}^{2N} a_m e(mx),$$

donde, como ya sabemos, los términos del último sumando no influyen en los siguientes desarrollos. Por lo tanto

$$r_2^*(N) = \int_{-1/2}^{1/2} S(x)^2 e(-Nx)dx$$

Volvamos a usar la fórmula asintótica que conocemos para $S(x)$ en los arcos mayores siendo $P = (\log \hat{N})^{20}$ y $Q = \hat{N}/(\log \hat{N})^{20}$,

$$\int_{\mathcal{M}_{a/q}} S(x)^2 e(-Nx)dx =$$

$$= \int_{\mathcal{M}_{a/q}} \left(\frac{\mu(q)}{\phi(q)} \sum_{n \leq N} e((x - \frac{a}{q})n) + O(\hat{N} e^{-C\sqrt{\log \hat{N}}}) \right)^2 e(-Nx)dx,$$

sabemos que $(A+B)^2 = A^2 + O(AB) + O(B^2)$ con lo que la integral anterior queda

$$\int_{\mathcal{M}_{a/q}} \left(\frac{\mu(q)}{\phi(q)} \sum_{n \leq N} e((x - \frac{a}{q})n) \right)^2 e(-Nx)dx + \int_{\mathcal{M}_{a/q}} O(\hat{N}^2 e^{-C\sqrt{\log \hat{N}}})dx.$$

Resolvamos la primera integral, a la que llamaremos $\hat{I}_1$ haciendo el cambio de variable $x = a/q + u$, $dx = du$,

$$\hat{I}_1 = \left(\frac{\mu(q)}{\phi(q)} \right)^2 e(-Na/q) \int_{-1/Q}^{1/Q} \left(\sum_{n \leq N} e(xn) \right)^2 e(-Nx)dx.$$

La segunda integral,

$$\hat{I}_2 \ll \int_{\mathcal{M}_{a/q}} N^2 e^{-C'\sqrt{\log \hat{N}}} dx = O(\hat{N} e^{-C'\sqrt{\log \hat{N}}}).$$

Así que la contribución de los arcos mayores es,

$$\mathcal{A}_M(N) = \sum_{q \leq P} \left(\frac{\mu(q)}{\phi(q)} \right)^2 c_q(-N) \int_{-1/Q}^{1/Q} \left(\sum_{n \leq N} e(xn) \right)^2 e(-Nx)dx + O(\hat{N} e^{-C'\sqrt{\log \hat{N}}}),$$

al igual que antes, con $C' > 0$. Por tanto sólo nos queda ver cómo es la integral que aparece en la expresión anterior,

$$\int_{-1/Q}^{1/Q} \left(\sum_{n \leq N} e(xn) \right)^2 e(-Nx)dx = \int_{-1/2}^{1/2} (\quad) - \int_{1/Q}^{1/2} (\quad) - \int_{1/2}^{-1/Q} (\quad),$$

la primera integral es igual al número de formas en las que podemos poner un número N como suma de dos enteros positivos, será $N-1$, es decir, es $O(N)$. Haciendo cálculos se puede ver que

$$\int_{1/Q}^{1/2}\left(\sum_{n\leq N}e(xn)\right)^2 e(-Nx)dx \ll \int_{1/Q}^{1/2}\frac{1}{|x|^2}dx = O(Q) = O\left(\frac{\hat{N}}{(\log\hat{N})^{20}}\right),$$

y la integral restante se acotaría de la misma forma, así que la contribución de los arcos mayores queda,

$$\mathcal{A}_M(N) = N\sum_{q\leq P}\left(\frac{\mu(q)}{\phi(q)}\right)^2 c_q(-N) + O\left(\frac{\hat{N}}{(\log\hat{N})^{20}}\right)\sum_{q\leq P}\left(\frac{\mu(q)}{\phi(q)}\right)^2 c_q(-N), \tag{37}$$

Si llamamos T al último sumando de la ecuación anterior se tiene,

$$T \ll O\left(\frac{\hat{N}}{(\log\hat{N})^{20}}\right)\sum_{q\leq P}\frac{1}{\phi(q)} \ll \left(\frac{\hat{N}}{(\log\hat{N})^{20}}\right)\log\hat{N} = O\left(\frac{\hat{N}}{(\log\hat{N})^{19}}\right),$$

por tanto

$$\mathcal{A}_M(N) = N\sum_{q\leq P}\left(\frac{\mu(q)}{\phi(q)}\right)^2 c_q(-N) + O\left(\frac{\hat{N}}{(\log\hat{N})^{19}}\right). \tag{38}$$

Utilizando la fórmula explícita para las sumas de Ramanujan, tras algunas manipulaciones tenemos

$$\sum_{q\geq P}\left(\frac{\mu(q)}{\phi(q)}\right)^2 c_q(-N) = \sum_{d|N}\frac{\mu(d)^2}{\phi(d)}\sum_{\substack{q\geq P/d\\(q,N)=1}}\frac{\mu(q)}{\phi(q)^2}$$

y usando que $\sum_{q>z}\phi(q)^{-2} \ll z^{-1}$, (esto es consecuencia de los teoremas 324 y 329 de [Ha-Wr]), podemos acotar la expresión anterior obteniendo

$$\sum_{q\geq P}\left(\frac{\mu(q)}{\phi(q)}\right)^2 c_q(-N) \ll \sum_{d|N}\frac{\mu(d)^2}{\phi(d)}\,\text{mín}\left(\frac{d}{P},1\right).$$

Por lo tanto, utilizando lo anterior es claro que

$$\Xi(N) = \sum_{q=1}^{\infty}\left(\frac{\mu(q)}{\phi(q)}\right)^2 c_q(-N) \tag{39}$$

converge y que si $\Xi(N,P) = \sum_{q\leq P}\left(\frac{\mu(q)}{\phi(q)}\right)^2 c_q(-N)$, se tiene que

$$\Xi(N,P) - \Xi(N) \ll \log N$$

y

$$\sum_{N=1}^{\hat{N}} |\Xi(N,P) - \Xi(N)|^2 \ll (\log \hat{N}) \sum_{d \leq N} \frac{\mu(d)^2 \hat{N}}{\phi(d)d} \text{ mín} \left(\frac{d}{P}, 1 \right)$$

$$\ll \frac{\hat{N}(\log \hat{N})}{P} \sum_{d \leq N} \frac{\mu(d)^2}{\phi(d)} \ll \frac{\hat{N}(\log \hat{N})^2}{P} = \frac{\hat{N}}{(\log \hat{N})^{18}}.$$

Calculemos pues, el error en promedio que se produce en la contribución de los arcos mayores,

$$\sum_{N=1}^{\hat{N}} |\mathcal{A}_M(N) - N\Xi(N)|^2 \ll \sum_{N=1}^{\hat{N}} |\mathcal{A}_M - N\Xi(N,P)|^2 +$$

$$+ \sum_{N=1}^{\hat{N}} |N\Xi(N,P) - N\Xi(N)|^2 \ll \frac{\hat{N}^3}{(\log \hat{N})^{18}}$$

De nuevo empleando las definiciones de $\mu(q)$, $\phi(q)$ y $c_q(-N)$ tenemos que

$$\Xi(N) = \sum_{q=1}^{\infty} \left(\frac{\mu(q)}{\phi(q)} \right)^2 c_q(-N) = \prod_{p \nmid N} \left(1 - \frac{1}{(p-1)^2} \right) \prod_{p|N} \left(1 + \frac{1}{(p-1)} \right).$$

Vayamos ahora con los arcos menores,

$$\mathcal{A}_m(N) = \int_m \left(\sum_{n \leq N} e(nx) \right)^2 e(-Nx)dx.$$

Por la desigualdad de Bessel, (véase [Fol] o apéndice), se tiene

$$\sum_{N=1}^{\hat{N}} |\mathcal{A}_m(N)|^2 \ll \int_m |S(x)|^4 dx. \tag{40}$$

En la sección anterior vimos que $S(x)$ en los arcos menores es $O(\frac{\hat{N}}{(\log \hat{N})^6})$, aplicando esto junto con la identidad de Parseval obtenemos el error promedio en los arcos menores,

$$\sum_{N=1}^{\hat{N}} |\mathcal{A}_m(N)|^2 \ll \int_m |S(x)|^4 dx \ll \frac{\hat{N}^3}{(\log \hat{N})^{11}}.$$

Claramente se ve que

$$\sum_{N=1}^{\hat{N}} |\mathcal{A}_M(N) - N\Xi(N)|^2 \ll \frac{\hat{N}^3}{(\log \hat{N})^{11}}$$

por lo que el teorema 11 queda demostrado.□

Observación 4.1 $\Xi(N) \gg 1$ *cuando* N *es par y* $\Xi(N) = 0$ *cuando es impar.*

Corolario 12 *El número* $E(\hat{N})$ *de números pares* N *menores que* $\hat{N}$ *para los cuales* N *no es la suma de dos primos cumple,*

$$E(\hat{N}) \ll \frac{\hat{N}}{(\log \hat{N})^{11}}.$$

Demostración

Sea

$$F(N) = \frac{|r_2^*(N) - N\Xi(N)|^2}{N^2},$$

si $r_2^*(N) = 0 \Longrightarrow F(N) \gg 1$, es decir, en los números pares no representables como suma de dos primos $F(N) \gg 1$, así que

$$\sum_{N=1}^{\hat{N}} \frac{|r_2 * (N) - N\Xi(N)|^2}{N^2} \gg \sum_{\substack{N \ no \\ representables}} 1 \gg E(\hat{N}).$$

□

5. Representación de enteros como suma de cuadrados

5.1. Introducción

¿Qué tienen en común las siguientes expresiones?

1. $3^2 = 2^2 + 2^2 + 1^2$,
2. $4 = 1^2 + 1^2 + 1^2 + 1^2 = 2^2$,
3. $7 \neq a^2 + b^2 + c^2$

Fácilmente se ve que los miembros de la derecha son todos sumas de cuadrados.

Estudiar las representaciones de un número como suma de cuadrados puede ayudar a resolver otros problemas matemáticos, por ejemplo cuestiones relacionadas con la función zeta de Epstein o el problema del círculo. También es útil para otras disciplinas como la cristalografía, la electrostática, la mecánica clásica... (véase [Gro]).

Tampoco hay que negar que el estudio de las reprentaciones de un entero como suma de cuadrados no sólo se ha desarrollado por su utilidad en otras

áreas, también se debe a que es un problema atrayente que despierta curiosidad y ganas de entenderlo. Muchos matemáticos han contribuido al estudio de este problema, entre ellos Diofanto y Bachet, Vieta y Fermat, Lagrange, Gauss, Artin, Hardy, Littlewood, Ramanujan y muchos más. Entre nuestros contemporáneos encontramos los nombres de Siegel, Pfister o Hooley. Desde Fermat cada generación de matemáticos ha encontrado interesante el estudio de este problema u otros relacionados con él. Actualmente la investigación en este campo permanece abierta y muchos problemas aún no tienen solución.

5.2. Aplicación del método del círculo para estudiar el número de representaciones de un entero como suma de k cuadrados

Nuestro objetivo es hallar una fórmula asintótica que nos diga de cuántas formas podemos representar un número entero como suma de k cuadrados, es decir, fijado $k > 4$ hallaremos una fórmula asintótica para

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

Para ello se introduce la función $F(z) = \sum_{n\in\mathbb{Z}} z^{n^2}$. Elevando $F(z)$ a k se ve que $r_k(N)$ es el coeficiente de z^N en $(F(z))^k$ y aplicando la fórmula integral de Cauchy podemos escribir,

$$r_k(N) = \frac{1}{2\pi i}\int_C (F(z))^k \frac{dz}{z^{N+1}}, \tag{41}$$

donde $C = \{z \in \mathbb{C} : |z| = r\}$ con $0 < r < 1$. Haciendo el cambio de variable $z \mapsto e(z)$, la ecuación (41) queda

$$r_k(N) = \int_L (\theta(z))^k e(-Nz)dz, \tag{42}$$

con $\theta(z) = \sum_{n=-\infty}^{\infty} e(n^2 z)$ y L el segmento horizontal, $\{0 \leq Re(z) \leq 1, Im(z) = y\}$, donde $r = e^{-2\pi y}$. Elegimos $y = \frac{1}{N}$ porque así penalizamos los términos con $n^2 > N$ que no aportan nada para representar N como suma de cuadrados. Así que $z = x + i/N$.

Podemos dar una aproximación para $\theta(z)$ que sirva simultáneamente en arcos mayores y menores. La razón teórica última para ello es que θ es lo que se llama una forma modular. Aunque no entraremos aquí en la definición de este concepto (véase [Gro]), diremos que es un tipo especial de funciones con ciertas simetrías que relacionan los valores tomados en diferentes arcos. Recordemos que cada $x \in \mathbb{T}$ pertenece a algún intervalo $I_{a/q} = \{x : |x - a/q| < 1/(q\sqrt{N})\}$ con $0 < a/q \leq 1$ irreducible y $1 \leq q \leq \sqrt{N}$. La aproximación viene dada por el siguiente teorema,

Teorema 13 *Si $z = x + i/N$ y $x \in I_{a/q}$ entonces,*

$$\theta(z) = (qz-a)^{-1/2}(\alpha_{a/q} + O(e^{-\Delta})), \quad \text{con} \quad \alpha_{a/q}^8 = \begin{cases} 2^{-4}, & si \quad 2 \nmid q \\ 0 & si \quad 4 \mid q-2 \\ 1 & si \quad 4 \mid q \end{cases}$$

y $\Delta^{-1} = 2N^{-1}q^2 + 2N(qx-a)^2$.

Por supuesto que $\alpha_{a/q} = \xi \sqrt[8]{\alpha_{a/q}^8}$, con ξ una raíz octava de la unidad, pero la determinación de esta raíz es complicada y no la trataremos aquí. A partir de la prueba deduciremos que $\alpha_{a/q} = G_q(a,0)/\sqrt{-2iq}$, donde
$G_q(a,l) = \sum_{n=0}^{q-1} e((an^2+ln)/q)$ éstas son las conocidas sumas de Gauss (generalizadas).

Antes de empezar la demostración veremos algunos lemas que nos serán de gran utilidad en la misma,

Lema 14

$$\sum_{n=0}^{q-1} e(An/q) = \begin{cases} 0, & si \quad q \nmid A \\ q & si \quad q \mid A \end{cases}$$

Demostración Si $q \mid A$ podemos escribir $An/q = k$ siendo k un entero, por lo tanto es inmediato que $\sum_{n=0}^{q-1} e(k) = q$, (es sumar q veces 1).
Si $q \nmid A$ escribimos $An = k$ y $\sum_{k=0}^{q-1} e(k/q) = 0$ ya que es la suma de las raíces q-ésimas de la unidad.□

Lema 15 *La aplicación $\mathbb{Z}_q \times \mathbb{Z}_q \longrightarrow \mathbb{Z}_q \times \mathbb{Z}_q$ dada por $(x,y) \mapsto (x+y, x-y)$ es 1 a 1 (biyectiva) si q es impar, y es 2 a 1 si q es par, en este caso la imagen esta formada por los pares de clases con la misma paridad.*

Demostración Si q es impar digamos que

$$x + y = z_1 \quad \text{y} \quad x - y = z_2 \quad \text{lo que implica que } x = \frac{z_1+z_2}{2} \quad \text{e} \quad y = \frac{z_1-z_2}{2},$$

por lo tanto $\forall (z_1, z_2)\ \exists!\ (x,y)$ tal que $f(x,y) = (z_1, z_2)$ y queda demostrado que la aplicación es biyectiva.

Si q es par el argumento anterior no funciona debido a que en $\mathbb{Z}_q$ con q par no se puede dividir por dos, x e y dejan de ser únicos. Por ejemplo en $\mathbb{Z}_6$ digamos que $x = 0/2$, entonces $0 \equiv 2 \cdot x\ (6) \iff 6 \mid 2 \cdot x \iff 3 \mid x$, así que x podría ser 0 ó 3, no es único. Veamos que en este caso la aplicación es 2 a 1. Es fácil observar que los pares de la forma (x,y) y $(x+q/2, y+q/2)$ tienen la misma imagen. Llamemos f a nuestra aplicación, utilizando el primer teorema de isomorfía tenemos que $\mathbb{Z}_q \times \mathbb{Z}_q / Ker f \approx Im f$, los pares de la forma $(0,0)$ y $(q/2, q/2)$

pertenecerán al núcleo, así que fijándonos en el teorema de isomorfía se deduce que la dimensión de Imf, será la mitad que la del espacio inicial, por lo tanto hemos llegado a que la aplicación es 2 a 1. Si $q = 2n$, $\mathbb{Z}_q = \{0, 1, 2, \ldots 2n-1\}$ es el sistema de residuos, es fácil ver que la imagen esta formada por elementos de la misma paridad, las posibles opciones son:

$$(\text{par}, \text{par}) \longrightarrow (\underbrace{\text{par} + \text{par}}_{\text{par}}, \underbrace{\text{par} - \text{par}}_{\text{par}}),$$

$$(\text{impar}, \text{impar}) \longrightarrow (\underbrace{\text{impar} + \text{impar}}_{\text{par}}, \underbrace{\text{impar} - \text{impar}}_{\text{par}}),$$

$$(\text{impar}, \text{par}) \longrightarrow (\underbrace{\text{impar} + \text{par}}_{\text{impar}}, \underbrace{\text{impar} - \text{par}}_{\text{impar}}),$$

$$(\text{par}, \text{impar}) \longrightarrow (\underbrace{\text{par} + \text{par}}_{\text{impar}}, \underbrace{\text{par} - \text{par}}_{\text{impar}}),$$

como vemos los elementos de los pares resultantes son de la misma paridad, y al ser q par la paridad se conserva al pasar a nuestro sistema de residuos.□

Lema 16 *Si* $(a, q) = 1$ *entonces,*

$$|G_q(a, l)| \leq \sqrt{2q}, \tag{43}$$

Demostración Para demostrar el lema probaremos que

$$|G_q(a, l)|^2 \leq 2q, \tag{44}$$

así que empezaremos escribiendo la expresión para $|G_q(a, l)|^2$,

$$|G_q(a, l)|^2 = \sum_n \sum_m e((a(n-m)(n+m) + l(n-m))/q). \tag{45}$$

Utilizando el cambio de variable $u = n + m$, $v = n - m$, la ecuación anterior queda,

$$\sum_{v=0}^{q-1} e(lv/q) \sum_{u=0}^{q-1} e(avu/q). \tag{46}$$

- Si q es impar, $q \mid v \iff v = 0$ y aplicando el lema 14 se sigue que el sumatorio interior de (46) vale q si $v = 0$ y 0 en caso contrario, con lo que se deduce

  $$|G_q(a, l)|^2 = q$$

  y por lo tanto para q impar ha quedado demostrado (43), es más, hemos conseguido algo mejor que esa cota.

- Si q es par, u y v son de la misma paridad y la aplicación dada por $(n, m) \mapsto (u, v)$ es 2 a 1 como hemos demostrado en el lema 15. Así que la ecuación (45) se puede expresar como

  $$2 \sum_{u=0,\ 2|u}^{q-1} \sum_{v=0,\ 2|v}^{q-1} e(avu + lv/q) + 2 \sum_{u=0,\ 2\nmid u}^{q-1} \sum_{v=0,\ 2\nmid v}^{q-1} e(auv + lv/q), \tag{47}$$

apliquemos el cambio de variable $u = 2t,\ v = 2\hat{t}$ para la parte de la ecuación anterior donde u y v son pares y $u = 2t+1,\ v = 2\hat{t}+1$, para la parte donde son impares. Llamemos S_1 a la parte con u y v pares de (47),

$$S_1 = 2\sum_{t=0}^{q/2-1}\sum_{\hat{t}=0}^{q/2-1} e\left(\frac{4at\hat{t}+2l\hat{t}}{q}\right) = 2\sum_{\hat{t}=0}^{q/2-1} e(2l\hat{t}/q)\sum_{t=0}^{q/2-1} e(4at\hat{t}/q), \quad (48)$$

veamos cuánto vale S_1,

$$\sum_{t=0}^{q/2-1} e(4at\hat{t}/q) = \sum_{t=0}^{q/2-1} e(2at\hat{t}/q/2), \quad \text{aplicamos el lema 14, } \frac{q}{2} \mid 2\hat{t} \ \ si$$

$\hat{t} = 0$ ó $\hat{t} = q/4$, así que se deduce

$$S_1 = 2\cdot\frac{q}{2} + 2ke(\frac{l}{2})\cdot\frac{q}{2}, \quad \text{con } \ k = \begin{cases} 0 & \text{si } \ 4 \nmid q \\ 1 & \text{si } \ 4 \mid q \end{cases} \quad (49)$$

y por tanto $|S_1| \leq 2q$.

Sea S_2 la parte con u y v impares de (47),

$$S_2 = 2\sum_{\hat{t}=0}^{q/2-1} e(l(2\hat{t}+1)/q)\sum_{t=0}^{q/2-1} e(a(2\hat{t}+1)(2t+1)/q), \quad (50)$$

fijándonos en la expresión anterior observamos que el sumatorio interior equivale a sumar las raíces impares de la unidad, (elevadas a $2\hat{t}+1$). Llamemos s_2 a este sumatorio,

$$s_2 = \sum_{t=0}^{q/2-1} \xi^{2t+1}, \ \ \text{donde } \xi = e\left(\frac{a(2\hat{t}+1)}{q}\right),$$

sumando s_2 como una serie geométrica de razón ξ^2 llegamos a

$$s_2 = \sum_{t=0}^{q/2-1} \xi^{2t+1} = \frac{\xi}{\xi^2-1}\underbrace{(\xi^q-1)}_{0} = 0, \quad (51)$$

por lo tanto $S_2 = 0$ y en consecuencia

$$|G_q(a,l)|^2 = S_1 + S_2 = 2\cdot\frac{q}{2} + 2e(\frac{l}{2})\cdot\frac{q}{2} \leq 2q,$$

con lo que el lema ha quedado probado.□

Para continuar la demostración del teorema 13 a partir de lo que deduciremos aplicando los lemas anteriores necesitaremos una variante de la fórmula de sumación de Poisson (véase el apéndice) que viene dada en el siguiente lema.

Lema 17

$$\sum_{n\equiv m \pmod q} f(n) = \frac{1}{q}\sum_{n=-\infty}^{\infty} e(nm/q)\hat{f}(n/q).$$

Demostración

En la prueba del lema aplicaremos el lema 14, más exactamente lo que se requiere es una fórmula equivalente que se deduce fácilmente de él y sirve para detectar congruencias,

$$\frac{1}{q}\sum_{h=1}^{q} e(h(n-m)/q) = \begin{cases} 0, & \text{si} \quad n \not\equiv m \ (mod\ q) \\ 1 & \text{si} \quad n \equiv m \ (mod\ q) \end{cases}. \tag{52}$$

Usaremos esta fórmula para pasar de "sumar en congruencias a sumar de menos infinito a infinito" en la siguiente ecuación

$$\sum_{n\equiv m \pmod q} f(n) = \sum_{n=-\infty}^{\infty} \frac{1}{q}\sum_{1\le h\le q} e(h(n-m)/q)f(n) =$$

$$= \frac{1}{q}\sum_{1\le h\le q}\sum_{n=-\infty}^{\infty} e(h(n-m)/q)f(n) = \frac{1}{q}\sum_{1\le h\le q} e(-hm/q)\sum_{n=-\infty}^{\infty} F(n), \tag{53}$$

donde $F(x) = e(hx/q)f(x)$. La transformada de Fourier de $F(n)$ es $\hat{f}(N/q)$ con $N = qn - h$. Aplicando la fórmula de sumación de Poisson a la expresión (53) tenemos,

$$\sum_{n\equiv m \pmod q} f(n) = \frac{1}{q}\sum_{1\le h\le q} e(-hm/q)\sum_{n=-\infty}^{\infty} \hat{f}(N/q) \tag{54}$$

pero $\forall N,\ \exists\,!\ n \in \mathbb{Z}, h \in [1,q]$ tal que $N = qn - h$, es decir, fijado q, cada N da lugar a un único par (n,h), y cuando h y n varían, N recorre todos los enteros y además $-h \equiv N \pmod q$ por lo que la ecuación anterior equivale a

$$\sum_{n\equiv m \pmod q} f(n) = \frac{1}{q}\sum_{n=-\infty}^{\infty} e(nm/q)\hat{f}(n/q),$$

y así el lema 17 ha quedado demostrado.□

Para terminar la demostración del teorema 13 nos hace falta un último lema que aplicaremos para la evaluación de $\alpha^8_{a/q}$.

Lema 18

$$(G_q(a,0))^8 = \begin{cases} q^4, & si \quad 2 \nmid q \\ 0 & si \quad 4 \mid q-2 \\ 16q^4 & si \quad 4 \mid q \end{cases}$$

Demostración

Para demostrar el lema partiremos del valor de $G_q(1,0)$, éste es un resultado clásico (y difícil) que se remonta a Gauss y cuya prueba puede encontrarse por ejemplo en [Dav] p.13. Aquí no necesitaremos el valor exacto de $G_q(1,0)$ sino algo más débil. Concretamente que para q impar es una de las raíces de x^8-q^4, para $4 \mid q$, es raíz de x^8-16q^4 y para q par no múltiplo de cuatro es cero.

A continuación utilizamos un resultado de la Teoría de Galois que dice que al aplicar automorfismos de un grupo de Galois sobre las raíces de un polinomio, éstas se permutan, (véase [Ste]). En particular si tenemos un automorfismo, $\sigma \in Gal(\mathbb{Q}(e(1/q))/\mathbb{Q})$, definido de la siguiente manera,

$$\sigma : \xi \longrightarrow \xi^a \quad \text{siendo} \quad \xi = e(1/q)$$

según este resultado, σ sólo podrá permutar las raíces de los polinomios sobre $\mathbb{Q}$. Así que como $G_q(1,0)$ es raíz de x^8-q^4 si q es impar, y raíz de x^8-16q^4 si $4 \mid q$, al aplicar el automorfismo σ sobre $G_q(1,0)$, la imagen,
$\sigma(G_q(1,0)) = G_q(a,0)$, también será raíz de estos polinomios.

En el caso en el que $4 \mid q-2$, también se puede ver de otra forma, como $q/2$ es impar y

$$e(an^2/q) + e(a(n+q/2)^2/q) = e(an^2/q)(1+e(aq/4)) = 0,$$

los sumandos de $G_q(a,0)$ se anulan dos a dos. $\square$

Una vez enunciados todos estos lemas tenemos los ingredientes necesarios para poder comenzar la demostración del teorema.

Demostración (teorema 13)

Empezaremos demostrando la fórmula para $\theta(z)$ dada en el enunciado del teorema, partiremos de que

$$\theta(z) = \sum_{n=-\infty}^{\infty} e(n^2 z) = \sum_{m=0}^{q-1} e\left(\frac{am^2}{q}\right) \sum_{n \equiv m \pmod q} \underbrace{e\left(n^2\left(z-\frac{a}{q}\right)\right)}_{e(n^2 z)e(-n^2 a/q)}. \qquad (55)$$

Sea $f(n) = e\left(n^2\left(z-\frac{a}{q}\right)\right)$, su transformada de Fourier es,

$$\hat{f}(n) = \frac{e^{\pi i/4}}{\sqrt{2(z-a/q)}} e\left(\frac{-n^2}{4(z-a/q)}\right),$$

(véase [Fol]).

Aplicando el lema 17 a la expresión (55) se tiene,

$$\theta(z) = \frac{e^{\pi i/4}}{q\sqrt{2(z-a/q)}} \sum_{n=-\infty}^{\infty} \sum_{m=0}^{q-1} e\left(\frac{am^2}{q} + \frac{nm}{q}\right) e\left(\frac{n^2}{4q(a-zq)}\right) \qquad (56)$$

y llegamos a

$$\theta(z) = \frac{1}{q\sqrt{-2i(z-a/q)}} \sum_{n=-\infty}^{\infty} G_q(a,n) e\left(\frac{n^2}{4q(a-zq)}\right). \tag{57}$$

A continuación separamos la contribución de $n=0$ y acotamos el resto utilizando el lema 16 y comparando con una serie geométrica de razón $e\left(\frac{1}{4q(a-qz)}\right)$,

$$\theta(z) = \frac{G_q(a,0)}{\sqrt{-2iq}\sqrt{q(z-a/q)}} + \frac{1}{q\sqrt{-2i(z-a/q)}} \sum_{n=-\infty,\ n\neq 0}^{\infty} G_q(a,n) e\left(\frac{n^2}{4q(a-zq)}\right)$$

$$= \frac{1}{\sqrt{q(z-a/q)}} \left[\alpha_{a/q} + O\left(\left|\frac{2e\left(\frac{1}{4q(a-qz)}\right)}{1-e\left(\frac{1}{4q(a-qz)}\right)}\right|\right)\right], \tag{58}$$

donde $\alpha_{a/q} = G_q(a,0)/\sqrt{-2qi}$. Si $1 - e\left(\frac{1}{4q(a-qz)}\right) \leq \frac{1}{2}$, (para lo que hace falta $q \leq \sqrt{N}$), el último denominador de la expresión anterior lo podemos incorporar en la "O" y basta demostrar que

$$e\left(\frac{1}{4q(a-qz)}\right) = O(e^{\Delta}), \tag{59}$$

recordemos que $|e(w)| = O(e^{-2\pi Imw})$, por lo tanto sólo hace falta probar que $Im\left(\frac{1}{4q(a-qz)}\right)$ es como Δ,

$$Im\left(\frac{1}{4q(a-qz)}\right) = Im\left(\frac{1}{q(a-qx-qi/N)}\right),$$

y desarrollando la expresión anterior se llega a que

$$Im\left(\frac{1}{4q(a-qz)}\right) = \frac{1}{N(a-qx)^2 + q^2/N} = -2\Delta,$$

y con esto queda demostrado que

$$\theta(z) = q(z-a/q)^{-1/2}(\alpha_{a/q} + O(e^{-\Delta})).$$

Pasemos a la evaluación de $\alpha_{a/q}^8$. Todo se reduce a la expresión para $(G_q(a,0))^8$ que hemos hallado en el lema 18, a partir de ella se deduce inmediatamente que $\alpha_{a/q}^8 = \frac{(G_q(a,0))^8}{(2iq)^4}$, es decir,

$$\alpha_{a/q}^8 = \begin{cases} 2^{-4}, & \text{si} \quad 2 \nmid q \\ 0 & \text{si} \quad 4 \mid q-2 \\ 1 & \text{si} \quad 4 \mid q \end{cases},$$

con lo que la demostración del teorema 13 queda terminada.□

Teniendo en cuenta la fórmula para $\theta(z)$ dada en el teorema 13, los $I_{a/q}$ con $4|q-2$ y aquellos con $C\sqrt{N} \leq q \leq \sqrt{N}$, donde C es cierta constante positiva deberían considerarse arcos menores ya que

- si $4|q-2$, $\theta(z) \simeq 0$ y en la integral no hay singularidades.
- en el caso $C\sqrt{N} \leq q \leq \sqrt{N}$ si los $I_{a/q}$ fueran arcos mayores tendríamos que hallar una fórmula asintótica a partir de

$$\theta(z) = (q(z-a/q))^{-1/2}(\alpha_{a/q} + O(e^{-\Delta})), \tag{60}$$

  para deducir una fórmula asintótica de la ecuación anterior, $\alpha_{a/q}$ debe ser grande comparado con $O(e^{-\Delta})$. ¿Cuándo es $O(e^{-\Delta}) \ll \alpha_{a/q}$? Cuando q^2 es mucho menor que N, ya que sólo en este caso $\Delta = \frac{1}{2q^2/N+2N(qx-a)^2}$ puede ser grande y por lo tanto $e^{-\Delta}$ pequeño. Así que los q que estamos considerando ahora son demasiado grandes como para estar en un arco mayor porque con ellos no conseguiríamos una fórmula asintótica.

Así pues, la división de los arcos menores y mayores será:

$$\mathcal{M} = \bigcup_{\substack{0<a\leq q<C\sqrt{N} \\ 4\nmid q-2}} I_{a/q} \quad \text{y} \quad m = \mathbb{T} - \mathcal{M}.$$

El siguiente teorema nos da la fórmula asintótica para $r_k(N)$, la suma infinita que aparece en dicha fórmula converge rápido si k es grande. En el caso $8 \mid k$ simplificaremos drásticamente y resultará una expresión más sencilla.

Teorema 19 *Si $k > 4$ es par*

$$r_k(N) = \frac{(-2\pi i)^{k/2} N^{k/2-1}}{\Gamma(k/2)} \left(\sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \alpha_{a/q}^k q^{-k/2} e(-aN/q) \right) + O(N^{k/4}).$$

A continuación veamos dos lemas que nos servirán para realizar la prueba del teorema 19.

Lema 20 *Si $x \in I_{a/q}$ entonces $|qz-a|^{-1} \ll N^{1/2}\Delta^{1/2}$.*

Demostración

$$|qz-a|^{-1} = \frac{1}{|qz-a|} = \frac{1}{|qx+qi/N-a|} = \frac{1}{\sqrt{(qx-a)^2+q^2/N^2}} = cte\sqrt{N}\sqrt{\Delta}.\square$$

Corolario 21

$$\sum_{q\leq\sqrt{N}}\sum_{\substack{a=1\\(a,q)=1}}^{q}\int_{I_{a/q}}|qz-a|^{-k/2}e^{-\Delta}dx\ll N^{k/4}$$

Demostración

A partir del lema 20 se tiene $|qz-a|^{-k/2}\ll N^{k/4}\Delta^{k/4}$, de aquí podemos deducir que $|qz-a|^{-k/2}e^{-\Delta}\ll N^{k/4}$, ya que $f(\Delta)=e^{-\Delta}\Delta^{k/4}$ es una función que para $\Delta>0$ esta acotada superiormente por cierta constante dependiente de k, por tanto,

$$\sum_{q\leq\sqrt{N}}\sum_{\substack{a=1\\(a,q)=1}}^{q}\int_{I_{a/q}}|qz-a|^{-k/2}e^{-\Delta}dx\ll\sum_{q\leq\sqrt{N}}\sum_{\substack{a=1\\(a,q)=1}}^{q}N^{k/4}\frac{2}{q\sqrt{N}}$$

$$=\frac{2N^{k/4}}{\sqrt{N}}\sum_{q\leq\sqrt{N}}\underbrace{\phi(q)/q}_{\leq 1}\ll N^{k/4}.\square$$

Lema 22 *Se cumple*

$$\theta^k(z)=(qz-a)^{-k/2}(\alpha_{a/q}^k+O(e^{-\Delta})). \tag{61}$$

Demostración

Por el teorema 13 para demostrar el lema tendremos que ver que $(\alpha_{a/q}+O(e^{-\Delta}))^k=(\alpha_{a/q}^k+O(e^{-\Delta}))$, renombremos $A=\alpha_{a/q}$ y $B=O(e^{-\Delta})$, sabemos que $|A|\leq 1$, así que por el binomio de Newton

$$(A+B)^k=A^k+O(|B^k|+|B|^{k-1}+\ldots+|B|)=A^k+O(|B|),$$

ya que $|B|\gg|B|^k.\square$

Demostración (teorema 19)

Recuperemos la expresión anterior que teníamos para $r_k(N)$,

$$r_k(N)=\int_0^1(\theta(z))^k e(-Nz)dx, \tag{62}$$

dividiendo el intervalo $[0,1]$ en arcos mayores y arcos menores,

$$r_k(N)=\int_{\mathcal{M}}(\theta(z))^k e(-Nz)dx+\int_m(\theta(z))^k e(-Nz)dx. \tag{63}$$

Llamemos I_1 a la primera integral de la ecuación anterior e I_2 a la segunda. Sustituyendo la definición de $(\theta(z))^k$ se tiene

$$I_1=\sum_{q\leq C\sqrt{N}}\sum_{\substack{a=1\\(a,q)=1}}^{q}\alpha_{a/q}^k\int_{I_{a/q}}(qz-a)^{-k/2}e(-Nz)dx$$

$$+\sum_{q\le C\sqrt{N}}\sum_{\substack{a=1\\(a,q)=1}}^{q}\int_{I_{a/q}}(qz-a)^{-k/2}O(e^{-\Delta})e(-Nz)dx$$

y teniendo en cuenta el corolario 21 se llega a

$$I_1=\sum_{q\le C\sqrt{N}}\sum_{\substack{a=1\\(a,q)=1}}^{q}\alpha_{a/q}^k\int_{I_{a/q}}(qz-a)^{-k/2}e(-Nz)dx+O(N^{k/4}). \tag{64}$$

Veamos que ocurre en los arcos menores. O bien $4\mid q-2$ y entonces $\alpha_{a/q}=0$, o bien $C\sqrt{N}\le q\le\sqrt{N}$ y en este caso $O(e^{-\Delta})\gg\alpha_{a/q}$, por lo tanto

$$I_2=\int_m(qz-a)^{-k/2}O(e^{-\Delta})e(-Nz)dx\ll N^{k/4}. \tag{65}$$

De (64) y (65) se deduce que

$$r_k(N)=\sum_{q\le C\sqrt{N}}\sum_{\substack{a=1\\(a,q)=1}}^{q}\alpha_{a/q}^k\int_{I_{a/q}}(qz-a)^{-k/2}e(-Nz)dx+O(N^{k/4}). \tag{66}$$

Para simplificar esta aproximación asintótica vamos a calcular la integral,

$$\int_{I_{a/q}}(qz-a)^{-k/2}e(-Nz)dx=\int_{a/q-1/q\sqrt{N}}^{a/q+1/q\sqrt{N}}(qx+qi/N-a)^{-k/2}e(-Nx-i)dx, \tag{67}$$

utilizamos el cambio de variable $u=N(x-a/q)$ y la integral queda

$$\frac{N^{k/2-1}}{q^{k/2}}\int_{-\sqrt{N}/q}^{\sqrt{N}/q}(u+i)^{-k/2}e(-i)e(-u-aN/q)du \tag{68}$$

y de aquí se sigue que

$$\int_{I_{a/q}}(qz-a)^{-k/2}e(-Nz)dx=\frac{N^{k/2-1}}{q^{k/2}}e(-aN/q)I\ \text{ con}$$

$$I=\int_{-\sqrt{N}/q}^{\sqrt{N}/q}(u+i)^{-k/2}e(-u-i)du,$$

pero

$$I=\int_{-\infty}^{\infty}(u+i)^{-k/2}e(-u-i)du-\int_{\sqrt{N}/q}^{\infty}(\quad)du-\int_{-\infty}^{-\sqrt{N}/q}(\quad)du,$$

integrando por partes se estiman $\int_{\sqrt{N}/q}^{\infty}$ y $\int_{-\infty}^{-\sqrt{N}/q}$, las dos integrales son $O(q^{k/2}N^{-k/4})$, y con esto

$$I=\int_{-\infty}^{\infty}(u+i)^{-k/2}e(-u-i)du+O(q^{k/2}N^{-k/4}). \tag{69}$$

Denotemos $\widetilde{I}$ a la integral de la igualdad anterior, la calcularemos en el caso de k par, para ello utilizaremos el teorema de los residuos en el semiplano inferior (véase [Pes] o apéndice). Tendremos que hallar

$Res\left(\frac{e(-u-i)}{(u+i)^{k/2}}, u=-i\right)$, lo haremos utilizando series de Laurent,

$$e(-u-i) = e^{-2\pi i(u+i)} = 1+\frac{(-2\pi i)}{1!}(u+i)+\frac{(-2\pi i)^2}{2!}(u+i)^2+\frac{(-2\pi i)^3}{3!}(u+i)^3+\dots$$

así que

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

con lo que ya hemos calculado el residuo,

$$Res\left(\frac{e(-u-i)}{(u+i)^{k/2}}, u=-i\right) = \frac{(-2\pi i)^{k/2-1}}{(k/2-1)!} = (-1)^{k/2-1}\frac{(2\pi i)^{k/2-1}}{(k/2-1)!}, \qquad (70)$$

y ahora aplicando el teorema de los residuos en el semiplano inferior,

$$\tilde{I} = 2\pi i Res\left(\frac{e(-u-i)}{(u+i)^{k/2}}, u=-i\right) = (-1)^{k/2}\frac{(2\pi i)^{k/2}}{\Gamma(k/2)},$$

siendo $\Gamma(k/2) = (k/2-1)!$.

En definitiva hemos llegado a que,

$$\int_{I_{a/q}} (qz-a)^{-k/2}e(-Nz)dx = \frac{N^{k/2-1}}{q^{k/2}}e(-aN/q)\left(\frac{(-2\pi i)^{k/2}}{\Gamma(k/2)}+O(q^{k/2}N^{-k/4})\right). \qquad (71)$$

Sustituyendo la aproximación en (63) se obtiene,

$$r_k(N) = \sum_{q\le C\sqrt{N}}\sum_{\substack{a=1\\(a,q)=1}}^{q}\alpha_{a/q}^k\frac{N^{k/2-1}}{q^{k/2}}e(-aN/q)\frac{(-2\pi i)^{k/2}}{\Gamma(k/2)}$$

$$+\sum_{q\le C\sqrt{N}}\sum_{\substack{a=1\\(a,q)=1}}^{q}\alpha_{a/q}^k\frac{N^{k/2-1}}{q^{k/2}}e(-aN/q)O(q^{k/2}N^{-k/4})+O(N^{k/4}). \qquad (72)$$

Llamemos T al penúltimo término de la ecuación anterior, T es $O(N^{k/4})$, ya que

$$T \ll \sum_{q\le C\sqrt{N}}\sum_{\substack{a=1\\(a,q)=1}}^{q}\alpha_{a/q}^k\frac{N^{k/2-1}}{N^{k/4}} \ll C\sqrt{N}\sqrt{N}N^{k/4-1} = O(N^{k/4}).$$

Los términos con $q \geq C\sqrt{N}$ se pueden añadir a (72) siempre que $k > 4$ porque su contribución no supera $O(N^{k/4})$, veámoslo

$$\sum_{q>C\sqrt{N}}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \alpha_{a/q}^{k} \frac{N^{k/2-1}}{q^{k/2}} e(-aN/q) \frac{(-2\pi i)^{k/2}}{\Gamma(k/2)} \ll N^{k/2-1} \sum_{q>C\sqrt{N}}^{\infty} q^{-(k/2)+1} \quad (73)$$

y aplicando el criterio de la integral $\sum a_n \leq \int f(x)dx$ se concluye

$$N^{k/2-1} \sum_{q>C\sqrt{N}}^{\infty} q^{-(k/2)+1} \leq \int_{C\sqrt{N}}^{\infty} q^{-(k/2)+1} dq \ll N^{k/4},$$

y por tanto queda probado que los términos con $q \geq C\sqrt{N}$ se pueden incorporar, con lo que se tiene

$$r_k(N) = \frac{(-i)^{k/2}(2\pi)^{k/2}N^{k/2-1}}{\Gamma(k/2)} \left(\sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \alpha_{a/q}^{k} q^{-k/2} e(-aN/q) \right) + O(N^{k/4}) \quad (74)$$

y el teorema queda demostrado.□

La doble suma entre paréntesis se puede simplificar, debido a la definición de $\alpha_{a/q}$ hay que discutir muchos casos, (véase [Gro], (capítulo 12, sección 3)). Aquí lo haremos para el caso en el que k es múltiplo de 8, en este caso $\alpha_{a/q}^{k}$ toma tres posibles valores de forma periódica y al evaluar la serie se obtiene el siguiente teorema.

Teorema 23 *Si k es múltiplo de 8 entonces*

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

Para $k = 8$ esta fórmula es exacta sin el término de error y no lo es para ningún otro múltiplo de 8, (véase teorema 4 del capítulo 13 de [Gro]), esto se puede probar usando la teoría de formas modulares.

Demostración (teorema 23)

La clave para hacer la simplificación está en las conocidas sumas de Ramanujan. Sabemos que son multiplicativas, es decir, $c_{q_1q_2}(-N) = c_{q_1}(-N)c_{q_2}(-N)$ si $(q_1, q_2) = 1$. También conocemos que $c_q(-N) = \begin{cases} p-1, & \text{si} \quad p \mid N \\ -1 & \text{si} \quad p \nmid N \end{cases}$. Pero además de las propiedades anteriores para evaluar $c_q(-N)$ existen otras propiedades elementales.

Sea p un número primo, $l \in \mathbb{Z}^+$ tal que $p^l \mid N$ y $p^{l+1} \nmid N$ entonces:

- Si $0 < l < m \Longrightarrow c_{p^m}(-N) = p^l c_{p^{m-l}}(-N/p^l)$, porque

$$c_{p^m}(-N) = \sum_{\substack{a=1 \\ p\nmid a}}^{p^m} e(\frac{-aN}{p^m}) = \sum_{\substack{a=1 \\ p\nmid a}}^{p^m} e(\frac{-aN'}{p^{m-l}})$$

$$= \frac{p^m}{p^{m-l}} \sum_{\substack{a=1 \\ p\nmid a}}^{p^{m-l}} e(\frac{-aN'}{p^{m-l}}) = p^l c_{p^{m-l}}(\frac{-N}{p^l}),$$

  donde $N = p^l N'$ y $p \nmid N'$.

- Si $0 < l \leq m$, $p^m \mid N \implies c_{p^m}(-N) = p^m - p^{m-l}$, ya que

$$c_{p^m}(-N) = \sum_{\substack{a=1 \\ (a,p^m)=1}}^{p^m} e(\frac{-aN}{p^m}) = \phi(p^m) = p^m - p^{m-l}.$$

- Si $0 = l < m$, $p \nmid N$ y como ya conocemos $c_p(-N) = -1$, y $c_{p^{m+1}}(-N) = 0$.

Por la multiplicatividad y la última propiedad, para cualquier función aritmética multiplicativa, bajo buenas condiciones de convergencia,

$$\sum_{q=1}^{\infty} f(q) c_q(-N) = \prod_p (1 + f(p)c_p(-N) + f(p^2)c_{p^2}(-N) + \ldots).$$

Sea $\mathcal{F}_p$ el término entre paréntesis, tomemos $f(q) = q^{-k/2}\alpha_{a/q}^k 2^{k/2}$ y veamos qué ocurre con $\mathcal{F}_p$ según si p divide a N o no

- Si $p \nmid N \implies c_p(-N) = -1$ y $c_{p^m}(-N) = 0$ si $m > 1$, por lo que $\mathcal{F}_p = 1 - p^{-k/2}$.

- Si $p \mid N$ y $p \neq 2$, utilizando las propiedades de $c_q(-N)$ y operando llegamos a,

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

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

- Si $p \mid N$ y $p = 2$, operando de la misma manera y agrupando términos adecuadamente obtenemos,

$$\mathcal{F}_2 = 1 + 2^{(1-k/2)} + 2^{2(1-k/2)} + \ldots + 2^{l(1-k/2)} - 2 \cdot 2^{l(1-k/2)}.$$

Teniendo en cuenta lo anterior, $\prod_p \mathcal{F}_p = \mathcal{F}_2 \prod_{p\neq 2} \mathcal{F}_p$ y

$$\prod_{p\neq 2} \mathcal{F}_p = (\underbrace{\prod_p (1-p^{-k/2})}_{C}) \sum_{d|N} d^{1-k/2},$$

con lo que

$$\mathcal{F}_2 \prod_{p\neq 2} \mathcal{F}_p = C \cdot [\sum_{d|N} d^{1-k/2} - 2 \cdot 2^{l(1-k/2)} \sum_{d|N, 2\nmid d} d^{1-k/2}] =$$

$$= C \cdot [\sum_{d|N} d^{1-k/2} - 2 \cdot \sum_{d|N, 2\nmid d} (2^l d)^{1-k/2}],$$

donde $2^l d = D$ es, si existe, un divisor de N con la máxima potencia positiva de 2, lo que implica que $\prod_p \mathcal{F}_p = C(\sum_A (\quad) - 2\sum_B (\quad))$, donde $A \equiv$todos los divisores y $B \equiv$divisores con la máxima potencia de 2.

Podemos escribir $\prod_p \mathcal{F}_p$ como una suma en todos los divisores, los términos que sumamos serán positivos si los divisores no contienen la máxima potencia de 2, y negativos en caso contrario, para detectar el signo de los sumandos, es decir, para ver si un divisor de N contiene a la máxima potencia de 2, introduciremos $(-1)^{N+N/d}$ en nuestro sumatorio, (ya que $N + N/d$ es impar si N es par y d contiene a la máxima potencia de 2 y par en caso contrario). Así que finalmente queda

$$\prod_p \mathcal{F}_p = \sum_{d|N} (-1)^{N+N/d} d^{1-k/2}. \tag{75}$$

Llamemos $\widetilde{S}$ la suma doble de (74) que estamos simplificando,

$$\widetilde{S} = \sum_{q=1}^{\infty} c_q(-N)\alpha_{a/q}^k q^{-k/2} = \sum_{q=1}^{\infty} c_q(-N) 2^{-k/2} f(q),$$

aplicando, lo que hemos obtenido en (75),

$$\widetilde{S} = \sum_{d|N} (-1)^{N+N/d} d^{1-k/2} 2^{-k/2} \prod_{p\neq 2} (1-p^{k/2}),$$

multiplicando y dividiendo por $(2^{k/2}-1)$ y aplicando que

$$\zeta(\frac{k}{2}) = \sum_{n\geq 1} \frac{1}{n^{k/2}} = \prod_p (1 - \frac{1}{p^{k/2}})$$

llegamos a

$$\widetilde{S} = \frac{1}{(2^{k/2}-1)\zeta(k/2)} \sum_{d|N} (-1)^{N+N/d} d^{1-k/2},$$

finalmente sustituyendo la igualdad anterior en la expresión (74) el teorema queda probado.□

6. Otro problema relacionado con el método del círculo. El problema de Waring

En esta sección presentaremos el problema de Waring ya que es un problema aditivo muy importante y está también muy relacionado con el método del círculo.

En 1770 Waring afirmó en su libro, *Meditationes Algebraicae*, que todo número natural se puede escribir como suma de 9 cubos o 19 bicuadrados[9] y así sucesivamente, pero no lo probó. Debido a la afirmación anterior se piensa que Waring creía que para todo número natural $k \geq 2$ existe un número s tal que todo número natural es suma de como mucho s potencias k-ésimas de otros naturales. Los menores de estos s, llamémosle $g(k)$, son $g(3) = 9$ y $g(4) = 19$.

Probablemente Diofanto ya conocía, aunque en un modo distinto, que todo número natural es como mucho suma de 4 cuadrados. El teorema de los 4 cuadrados fue enunciado por Bachet en 1621 y Fermat afirmó que tenía la prueba pero murió antes de mostrarla, por lo que hubo que esperar hasta 1770 la tan ansiada prueba que fue dada por Lagrange, (véase capítulo 20 de [Ha-Wr]).

En el siglo XIX se demostró la existencia de $g(k)$ para muchos valores de k, pero los avances más grandes se han producido en el siglo XX. Hilbert en 1909 probó con un difícil argumento combinatorio basado en identidades algebraicas, (véase [Elli]), que $g(k)$ existe para todo k,pero su método da una cota muy pobre para $g(k)$.

El método del círculo ha hecho posible algunas evaluaciones para $g(k)$. A partir de un argumento teórico basado en el método se consigue un número C_k, que es suma de como mucho s_k potencias k-ésimas de números naturales con $s_k \leq g(k)$

Después de la Primera Guerra Mundial (1920, 1921), Hardy y Littlewood empezaron a trabajar en el problema de Waring aplicando el método del círculo, posteriormente Vinogradov (1928) introdujo algunos refinamientos y se vio como $g(k)$ quedaba condicionado por algunos números naturales no muy grandes. A partir aquí, se empezó a pensar en la estimación de $G(k)$, el mínimo s tal que todo número natural suficientemente grande se puede escribir como suma de s potencias k-ésimas de números naturales, para $k \geq 2$. Se deduce que $G(k)$ es mucho menor que $g(k)$ cuando k es grande y esto hace que su evaluación sea más difícil. De hecho sólo se conoce el valor de $G(k)$ cuando $k = 2$ ó $k = 4$, $G(2) = 4$ y $G(4) = 16$, (este último resultado fue dado por Davenport, 1939). Linnik en 1943 demostró que $G(3) \leq 7$ (Watson en 1951 dio una prueba

[9]Entendemos por bicuadrado un número elevado a la cuarta.

muy elegante de esto). En 1958 J.R. Chen probó que $G(k) \leq n(3\log n + 5{,}2)$ y en 1984 R.Balasubramanian y C.J. Mozzochi mejoraron esto para obtener

$$G(k) \leq \frac{\log 108 + 3\log k}{\log(k/(k-1))} - 4.$$

Otros matemáticos, sobre todo R.C. Vaughan en 1986, han conseguido mejorar esto para algunas k pequeñas. Los límites más conocidos son

k	4	5	6	7	8	9	10	11	12	13	15	15
$G(k)$	19	21	31	45	62	82	102	120	135	150	166	181

Cuando $k > 3$ las mejores estimaciones que se conocen han sido obtenidas con el método del círculo.

7. Apéndice

En este apéndice mencionaremos algunos resultados básicos del Análisis Real y de la Teoría de Números que hemos empleado en este trabajo.

Teorema 24 (Fórmula integral de Cauchy) . *Sea D un dominio simplemente conexo con frontera regular ∂D, para $a \in D$ y f holomorfa en un dominio que contiene a D entonces*

$$\frac{f^{(n)}(a)}{n!} = \frac{1}{2\pi i}\int_{\partial D} \frac{f(z)}{(z-a)^{n+1}} dz \qquad \text{con} \quad n = 0, 1, 2 \ldots$$

Lema 25 (Lema de Abel) . *Sea $(c_n)_{n=1}^{\infty}$ una sucesión arbitraria de números complejos y sea $C(t) = \sum_{n \leq t} c_n$. Dado $x \geq 1$, para cualquier $g : [1, \infty) \longrightarrow \mathbb{C}$, $g \in C^1$, se verifica*

$$\sum_{n \leq x} c_n g(n) = C(x)g(x) - \int_1^x C(t)g'(t)dt.$$

Lema 26 (Fórmula de sumación de Poisson) . *Sea f una función de decaimiento rápido, entonces*

$$\sum_{n=-\infty}^{\infty} f(n) = \sum_{n=-\infty}^{\infty} \hat{f}(n).$$

donde $\hat{f}$ es la transformada de Fourier $\hat{f}(\xi) = \int_{-\infty}^{\infty} f(t)e^{-2\pi i t\xi} dt$.

Teorema 27 (Desigualdad de Bessel) *Si los números* $a_n = \int_a^b f\phi_n dx$ *son los coeficientes de Fourier de* f *con respecto al sistema ortonormal* $\{\phi_n\}$*, entonces la serie* $\sum a_n^2$ *es convergente y satisface la desigualdad de Bessel,*

$$\sum_{n=1}^{\infty} a_n^2 \leq \int_a^b [f(x)]^2 dx.$$

Teorema 28 (Teorema de los residuos) *. Sea* $\Omega \subset \mathbb{C}$ *un abierto y* f *una función meromorfa en* Ω *con polos en ciertos* a_j *pertenecientes a un dominio* $D \subset \Omega$ *simplemente conexo cuya frontera es una curva cerrada regular* γ *entonces*

$$\int_\gamma f(z)dz = 2\pi i \sum_j Res(f, a_j) n(\gamma, a_j).$$

Referencias

[Dav] H. Davenport. *Multiplicative number theory,*2nd ed., revised by Hugh L. Montgomery. Graduate texts in mathematics 74. Springer-Verlag, 1980.

[Ell] W.J. Ellison, F. Ellison. *Prime Numbers.* Hermann, 1975.

[Elli] W.J. Ellison. Waring's problem and its generalization. *Am. Math. Mon., 78*, (1975), 10-36.

[Fol] G.B. Folland. *Fourier analysis and its applications.* Wadsworth & Brooks/Cole, 1992.

[Gro] E. Grosswald. *Representations of Integers as Sums of Squares.* Springer-Verlag, 1985.

[Har] G. H. Hardy, S. Ramanujan Asymptotic Formulæ in combinatory analysis. *Proc. London Math. Soc.* (2) **17** (1918), 75-115.

[Ha-Wr] G. H. Hardy, E. M. Wright. *An Introduction to the theory of numbers.* 5th ed. Oxford: Oxford University Press, 1979.

[Pes] D. Pestana, J.M. Rodríguez. y F. Marcellán. *Variable Compleja, un curso práctico.* Síntesis, 1999.

[Ste] I. Stewart. *Galois theory.* Chapman and Hall, 1984.

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