Sobre la Conjetura Impar de Goldbach

Eratóstenes Flores Torres

Otoño 2002

A mis hermanos Arte y Juan.

AGRADECIMIENTOS

Quiero aprovechar este pequeño espacio para agradecer a todas las personas que me brindaron su apoyo durante la realización de este trabajo.

A la Dra. Magali Louise Marie Folch Gabayet por su asesoramiento durante todas las etapas por las que pasó este proyecto; a mis sinodales Dra. María de la Luz Jimena de Teresa de Oteyza, Dr. Salvador Pérez Esteva, Dr. Francisco Marcos López García y Dr. Carlos Hernández Garciadiego, gracias por sus comentarios y sugerencias que contribuyeron sustancialmente en la presentación de este trabajo.

Al Dr. Alejandro Illanes y a la Dra. Verónica Martínez de la Vega por el gran apoyo que me brindaron cuando más lo necesité.

Quiero agradecer también a mi madre Juana Torres Zaragoza, por su apoyo incondicional en todos mis proyectos; a mis hermanos Juan Flores Torres y Artemisa Flores Torres por enriquecer mi vida día con día; y por supuesto a la persona que me llevó de la mano en mis primeros despejes Mat. Juan Flores Fuentes, mi padre.

Debo agradecer también el apoyo que durante todo este peregrinar me ha brindado mi media naranja, gracias Mayte.

Y como no, a todos los cuates que acertadamente han elegido siempre, la primera opción: Judith, Jorge, Edna, Paul, Kathya, Tatiana, Cruz, Omar, Javier, Barbas, Ulises, Aarón, Agustín, Gris, Adriana, Sael, Elhoim, Pepe y Edgar.

Contenido

Casi siempre he ido a la escuela y puedo deletrear, leer y escribir un poco, y puedo decir las tablas de multiplicar hasta llegar a que seis por siete son treinta y cinco, y no creo que nunca necesite saber más que eso aunque llegue a vivir por siempre. Aunque es nada lo que sé de matemáticas.

Huckleberry Finn.

Capítulo 1

Introducción

En el año de 1770 se publicó un libro titulado *Meditaciones Algebraicas* en el cual el autor Edward Waring conjeturaba que todo entero positivo es o un cubo o la suma de $2, 3, 4, 5, 6, 7, 8$ ó 9 cubos; análogamente conjeturaba que todo entero positivo es o una cuarta potencia o la suma de $2, 3, \ldots,$ ó 19 cuartas potencias y así sucesivamente. Esta conjetura se convirtió en teorema en el año de 1909, cuando el matemático inglés David Hilbert demostró que para todo $k \in \mathbb{N}$, existe un número $G(k)$ de tal forma que cualquier natural se puede representar como la suma de a lo más $G(k)$ sumandos, cada uno de los cuales es una k-ésima potencia.

¿De cuántas formas?

Algunos años después de la demostración de Hilbert, los matemáticos ingleses Hardy y Littlewood obtuvieron una fórmula asintótica para el número de representaciones de un natural N como suma de s sumandos cada uno de los cuales es una k-ésima potencia. Hardy y Littlewood obtuvieron dicha fórmula perfeccionando un método que tuvo su génesis en uno de los trabajos conjuntos entre Hardy y Ramanujan sobre el número de representaciones de un natural como suma de cuadrados [1].

El método de Hardy-Littlewood

La idea general de este método versa más o menos así: Sea A un conjunto de enteros no negativos y $r_{A,s}(N)$ el número de representaciones de N como suma de s elementos de A, entonces

$$r_{A,s}(N) = \int_0^1 e^{-2\pi i N\theta}\Big(f_N(\theta)\Big)^s d\theta, \tag{1.1}$$

donde

$$f_N(\theta) = \sum_{\substack{a\in A\\ a\leq N}} e^{2\pi i a\theta}.$$

El método de Hardy-Littlewood asegura que para N suficientemente grande, la contribución principal a la integral 1.1, proviene de la unión de pequeños intervalos alrededor de fracciones $\frac{a}{q}$ con $(a,q)=1$ y q no muy grande, mientras que la integral sobre el complemento de la unión de estos intervalos es despreciable.

Teoría aditiva de números

Este tipo de problemas en el que se cuestiona la posibilidad de representar cualquier natural como una suma finita de elementos de un subconjunto de los naturales, es lo que dió origen a una rama de las matemáticas conocida hoy en día como *teoría aditiva de números.*

Definición 1.0.1. Dados dos conjuntos de enteros no negativos A y B, decimos que A es una base de orden s del conjunto B, si todo elemento de B se puede representar como la suma de s elementos del conjunto A, no necesariamente distintos.

Los cuadrados de Lagrange

Tal vez el resultado más conocido de naturaleza aditiva es el teorema de Lagrange que se suele probar en los cursos básicos de teoría de números;

todo entero no negativo es la suma de cuatro cuadrados. En términos de la definición 1.0.1, el teorema de Lagrange afirma que los cuadrados son una base de orden 4 del conjunto de los enteros no negativos, sin embargo, dado que el número 7 no se puede representar como la suma de 3 cuadrados, se sigue que los cuadrados no son una base de orden 3 del conjunto de los enteros no negativos.

En este trabajo veremos que el método de Hardy-Littlewood, puede ser utilizado con éxito para abordar un viejo problema de teoría aditiva de números.

La conjetura de Goldbach

En el año de 1742, el matemático prusiano Christian Goldbach envió una carta a su colega suizo Leonard Euler en la cual hizo una conjetura que en términos de la definición 1.0.1 dice lo siguiente:

Conjetura 1.0.2 (Goldbach). *El conjunto de los números primos es una base de orden* 2 *para el conjunto de los números pares mayores que* 2*; similarmente el conjunto de los números primos es una base de orden* 3 *para el conjunto de los números impares mayores que* 5*.*

Utilizando el método de Hardy-Littlewood, en el año de 1937 el matemático ruso Ivan M. Vinogradov, obtuvo una fórmula asintótica para el número de representaciones de un natural como suma de tres primos.

Teorema 1.0.3 (Vinogradov). *Sea $r(N)$ el número de representaciones de un natural N como suma de tres primos. Entonces, existe una constante positiva C y un entero positivo N_0, tal que para todo número impar $N > N_0$*

$$r(N) \geq C\frac{N^2}{log^3(N)}.$$

Corolario 1.0.4. Existe un entero positivo N_0 tal que para todo número impar $N > N_0$ existen tres primos p_1, p_2 y p_3 que satisfacen la ecuación

$$N = p_1 + p_2 + p_3. \tag{1.2}$$

El teorema de Vinogradov es el resultado más fuerte, que se tiene en dirección a la demostración de la conjetura de Goldbach para el caso impar y es precisamente la demostración de este teorema, lo que presentaremos en este trabajo.

Buenos Deseos

Denotemos con $r_m(N)$ a la cantidad de números primos que hay en la sucesión $\{N - p_1 - p_2 - \cdots - p_{m-1}\}$ donde los p_i recorren el conjunto de los números primos menores o iguales que N, para $i = 1, 2, \ldots, m-1$.
Si en particular queremos estimar $r_2(N)$, podemos proceder como sigue: Del teorema de los números primos[1] la sucesión $\{N - p\}_{p\leq N}$ tiene aproximadamente $\frac{N}{logN}$ elementos, de tal forma que si los números primos están distribuidos uniformemente en la sucesión $\{N - p\}_p$ podríamos esperar que

$$r_2(N) = O\left(\frac{\frac{N}{log(N)}}{log\left(\frac{N}{log(N)}\right)}\right) = O\left(\frac{\frac{N}{log(N)}}{log(N) - log(log(N))}\right) = O\left(\frac{N}{log^2(N)}\right),$$

donde O es el símbolo de Landau[2]. ¿Qué podemos decir de $r_3(N)$?.

La sucesión $\{N-p_3\}_{p_3}$ donde p_3 recorre el conjunto de los números primos menores o iguales que N, tiene aproximadamente $\frac{N}{log(N)}$ términos y cada uno de ellos se puede representar como la suma de dos primos $N - p_3 = p_1 + p_2$ un número de veces del orden de $\frac{N}{log^2(N)}$. Por lo anterior podemos esperar que

$$r_3(N) = O\left(\frac{N^2}{log^3(N)}\right).$$

[1]Este teorema afirma, que la cantidad de primos menores o iguales que N es aproximadamente $\frac{N}{logN}$. Ver capítulo 2 sección 2.7 teorema 2.7.1.

[2]Ver definición 2.4.2

No obstante, el problema central sería demostrar que $r_3(N) > 0$; más aún, nos gustaría probar que existe una constante positiva C, de tal forma que para N suficientemente grande

$$r_3(N) \geq C \frac{N^2}{log^3(N)}.$$

Estructura del Texto

En el capítulo dos, presentamos algunos resultados que serán utilizados de manera crucial en capítulos posteriores. En el capítulo tres, escribiremos $r_3(N)$ en términos de una integral oscilatoria y descompondremos el dominio de integración según el método de Hardy-Littlewood-Ramanujan en dos subconjuntos disjuntos, llamados por razones históricas arcos mayores y arcos menores respectivamente. En el capítulo cuatro, estimaremos la integral sobre los arcos mayores utilizando principalmente el teorema de Siegel sobre la distribución de los números primos en una progresión aritmética. Posteriormente en el capítulo cinco, estimaremos la integral sobre los arcos menores utilizando el criterio de Dirichlet y algunos resultados de Vinogradov sobre sumas exponenciales. La última parte del trabajo corresponde a un apéndice que contiene algunos resultados bien conocidos, que se suelen probar en un curso básico de teoría analítica de números y que serán utilizados constantemente.

Capítulo 2

Preliminares

En este capítulo presentaremos algunos resultados que se utilizarán en el desarrollo posterior de este trabajo. Cada uno de estos resultados se presenta con la demostración correspondiente, exceptuando los teoremas 2.7.1, 2.7.2, 2.7.3 y 2.7.4 cuya demostración sobrepasa las espectativas de este trabajo. De cualquier modo referimos al lector interesado en ver dichas demostraciones, a la bibliografía correspondiente.

2.1 Funciones Aritméticas

Definición 2.1.1. Una función $f : \mathbb{N} \to \mathbb{C}$, es llamada *función aritmética.*

Algunos ejemplos clásicos en teoría de números que son de nuestro interés, son los siguientes:

- *La función de Moebius.* Dado un número natural n se define $\mu(n)$ como sigue:
  - $\mu(1) = 1$.
  - $\mu(n) = 0$, si n tiene un factor cuadrado.
  - $\mu(p_1 p_2 \cdots p_r) = (-1)^r$, si todos los primos $p_1, p_2, \ldots, p_r$ son diferentes.

- *La función divisor.* Dado un número natural n se define $d(n)$ como la cantidad de enteros positivos m tales que $m|n$.
- *La función de Euler.* Dado un número natural n se define $\phi(n)$, como la cantidad de enteros m que satisfacen $1 \leq m \leq n \quad y \quad (n,m) = 1$.

Definición 2.1.2. Decimos que una función aritmética $f(n)$ es *multiplicativa* si dados $(n,n') = 1$, entonces $f(nn') = f(n)f(n')$. En caso de que $f(nn') = f(n)f(n')$ para cualesquiera n y n', decimos que f es *totalmente multiplicativa.*

Lema 2.1.3. *La función de Moebius es multiplicativa.*

Demostración. Sean n y n' enteros tales que $(n,n') = 1$. Podemos escribir $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$ y $n' = q_1^{\beta_1}q_2^{\beta_2}\cdots q_s^{\beta_s}$ donde $p_i \neq q_j$ para $i = 1,2,\ldots,r$ y $j = 1,2,\ldots,s$. Si $\mu(nn') = 0$ entonces $\alpha_i > 1$ ó $\beta_j > 1$ para alguna i o alguna j y por consiguiente $\mu(n) = 0$ ó $\mu(n') = 0$ de tal forma que $\mu(n)\mu(n') = 0$. Si por el contrario $\mu(nn') \neq 0$, entonces $\alpha_i = 1$ y $\beta_j = 1$ para todo i, j y en consecuencia $\mu(n) = (-1)^r$ y $\mu(n') = (-1)^s$. Así $\mu(n)\mu(n') = (-1)^r(-1)^s = (-1)^{r+s} = \mu(nn')$. □

Lema 2.1.4. *La función divisor es multiplicativa.*

Demostración. Sean $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$ y $n' = q_1^{\alpha'_1}q_2^{\alpha'_2}\cdots q_s^{\alpha'_s}$ las factorizaciones en primos de n y n' respectivamente. Cada divisor d de n y d' de n' puede ser escrito de manera única como,

$$d = p_1^{\beta_1}p_2^{\beta_2}\cdots p_r^{\beta_r},$$

$$d' = q_1^{\beta'_1}q_2^{\beta'_2}\cdots q_s^{\beta'_s}$$

donde $0 \leq \beta_i \leq \alpha_i$ para $i = 1,2,\ldots,r$ y $0 \leq \beta'_j \leq \alpha'_j$ para $j = 1,2,\ldots,s$. Si $(n,n') = 1$ tenemos que $p_i \neq q_j$ para cualesquiera $i = 1,2,\ldots,r$ y $j = 1,2,\ldots,s$. Por lo tanto, dado que hay $\alpha_i + 1$ elecciones de β_i, tenemos que

$$d(n) = \prod_{i=1}^{r}(\alpha_i + 1),$$

y en consecuencia

$$d(nn') = \prod_{h=1}^{r+s}(\gamma_h + 1) = \prod_{i=1}^{r}(\alpha_i + 1)\prod_{j=1}^{s}(\beta_j + 1) = d(n)d(n'),$$

donde γ_h es algún α_i o algún β_j. □

Lema 2.1.5. *La función de Euler es multiplicativa.*

Demostración. Un sistema completo de residuos primos a nn' contiene exactamente $\phi(nn')$ enteros[1]. Por el lema A.1.2 si $(n, n') = 1$, entonces los $\phi(n)\phi(n')$ números $m'n + mn'$ recorren un sistema completo de residuos primos a nn' cuando m y m' recorren un sistema completo de residuos primos a n y n' respectivamente. Por lo tanto $\phi(nn') = \phi(n)\phi(n')$. □

2.2 Sumas de Ramanujan

Las sumas de Ramanujan juegan un papel importante en la demostración del teorema de Vinogradov 1.0.3. En esta sección probaremos que las sumas de Ramanujan son funciones multiplicativas y en el lema 2.2.5 veremos como se relacionan estas sumas y la función de Moebius.

Definición 2.2.1. Sean a y q números enteros con $q \geq 1$. La suma exponencial

$$c_q(a) = \sum_{\substack{m=1 \\ (m,q)=1}}^{q} e^{2\pi i a \frac{m}{q}}$$

es llamada *Suma de Ramanujan.*

Lema 2.2.2. *La suma $c_q(a)$ es una función multiplicativa de q.*

Demostración. Por el lema A.1.2 cada representante de un sistema completo de residuos primos a qq' puede escribirse de manera única como $mq' + m'q$

[1]Ver definición A.1.1.

donde $1 \leq m \leq q$, $1 \leq m' \leq q'$ y $(m,q) = (m',q') = 1$ si $(q,q') = 1$. Entonces

$$\begin{aligned} c_q(a)c_{q'}(a) &= \sum_{\substack{m=1 \\ (m,q)=1}}^{q} e^{2\pi i a \frac{m}{q}} \sum_{\substack{m'=1 \\ (m',q')=1}}^{q'} e^{2\pi i a \frac{m'}{q'}} = \sum_{\substack{m=1 \\ (m,q)=1}}^{q} \sum_{\substack{m'=1 \\ (m',q')=1}}^{q'} e^{2\pi i a \frac{mq'+m'q}{qq'}} \\ &= \sum_{\substack{m''=1 \\ (m'',qq')=1}}^{qq'} e^{2\pi i a \frac{m''}{qq'}} = c_{qq'}(a). \end{aligned}$$

□

La suma $c_q(a)$ se relaciona bellamente con la función de Moebius como veremos en el lema 2.2.5. Sin embargo el motivo por el cual presentamos esta relación es por que nos será de gran ayuda en el capítulo 4. Los lemas 2.2.3 y 2.2.4 nos facilitarán la demostración del lema 2.2.5 mencionado anteriormente además de ser resultados clave en el capítulo 5.

Lema 2.2.3. *Dado un entero positivo n*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}$$

Demostración. El resultado es obviamente cierto para $n = 1$. Supongamos entonces que $n > 1$ y escribamos $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$. En la suma $\sum_{d|n} \mu(d)$ los únicos términos que son distintos de cero vienen de $d = 1$ y de los divisores de n que son productos de primos distintos. Así

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \mu(p_1) + \cdots + \mu(p_k) + \mu(p_1p_2) + \cdots \\ &\quad + \mu(p_{k-1}p_k) + \cdots + \mu(p_1p_2\cdots p_k) \\ &= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k \\ &= (1-1)^k = 0. \end{aligned}$$

□

Lema 2.2.4. *Sea P un entero positivo. Si z recorre un conjunto finito de enteros positivos A y $f(z)$ es una función arbitraria de z, entonces*

$$\sum_{\substack{z\in A\\(z,P)=1}} f(z) = \sum_{d|P}\mu(d) \sum_{\substack{z\in A\\ z\equiv 0(mod\ d)}} f(z).$$

Demostración. Del lema 2.2.3 tenemos que

$$\begin{aligned}\sum_{\substack{z\in A\\(z,P)=1}} f(z) &= \sum_{z\in A} f(z) \sum_{d|(z,P)} \mu(d) = \sum_{z\in A} f(z) \sum_{d|z,d|P} \mu(d)\\ &= \sum_{d|P}\mu(d) \sum_{\substack{z\in A\\ d|z}} f(z) = \sum_{d|P}\mu(d) \sum_{\substack{z\in A\\ z\equiv 0(\text{mod } d)}} f(z).\end{aligned}$$

□

Lema 2.2.5. *Si $(a,q)=1$, la suma de Ramanujan satisface*

$$c_q(a) = \mu(q).$$

Demostración. Por el lema 2.2.4, tenemos

$$\begin{aligned}\sum_{\substack{m=1\\(m,q)=1}}^{q} e^{2\pi i a\frac{m}{q}} &= \sum_{d|q}\mu(d) \sum_{\substack{m=1\\ m\equiv 0(\text{mod } d)}}^{q} e^{2\pi i a\frac{m}{q}} = \sum_{d|q}\mu(d) \sum_{\substack{m=1\\ m=kd}}^{q} e^{2\pi i a\frac{m}{q}}\\ &= \sum_{d|q}\mu(d) \sum_{\substack{m=kd\\ 1\le k\le \frac{q}{d}}}^{q} e^{2\pi i a\frac{m}{q}} = \sum_{d|q}\mu(d) \sum_{k=1}^{\frac{q}{d}} e^{2\pi i a\frac{kd}{q}}.\end{aligned}$$

Si $d=q$ tenemos $\mu(q)e^{2\pi i a\frac{kd}{q}} = \mu(q)e^{2\pi i ak} = \mu(q)$ ya que $e^{2\pi i ak}=1$, mientras que si $d<q$ tenemos

$$\sum_{k=1}^{\frac{q}{d}} e^{2\pi i a\frac{kd}{q}} = \frac{e^{2\pi i a\frac{(\frac{q}{d}+1)d}{q}} - e^{2\pi i a\frac{d}{q}}}{e^{2\pi i a\frac{d}{q}} - 1},$$

donde $e^{2\pi i a \frac{d}{q}} - 1 \neq 0$, pues $(a,q) = 1$ y $e^{2\pi i a \frac{(\frac{q}{d}+1)d}{q}} - e^{2\pi i a \frac{d}{q}} = 0$. Por lo tanto

$$\sum_{\substack{m=1 \\ (m,q)=1}}^{q} e^{2\pi i a \frac{m}{q}} = \mu(q).$$

□

2.3 Más Sobre la Función de Euler

En esta sección presentamos una estimación por abajo de la función de Euler que será utilizada en el capítulo 4. Probaremos que $\phi(n) > n^{1-\epsilon}$ para cualquier $\epsilon > 0$, siempre y cuando n sea suficientemente grande.

Lema 2.3.1. *Sea $f(n)$ una función aritmética multiplicativa. Si*

$$lim_{p^k \to \infty} f(p^k) = 0,$$

donde p^k recorre la sucesión de todas las potencias de primos, entonces

$$lim_{n \to \infty} f(n) = 0.$$

Demostración. Dado que $lim_{p^k \to \infty} f(p^k) = 0$, existe únicamente una cantidad finita de potencias de primos tales que $|f(p^k)| \geq 1$. Sea

$$A = \prod_{|f(p^k)| \geq 1} |f(p^k)|.$$

Tomemos $0 < \epsilon < A$. Nuevamente sólo existe una cantidad finita de potencias de primos p^k tales que $|f(p^k)| \geq \frac{\epsilon}{A}$. De tal forma que sólo una cantidad finita de enteros n son tales que

$$|f(p^k)| \geq \frac{\epsilon}{A}$$

para cada potencia p^k que divide a n. Por lo tanto si n es suficientemente grande existe al menos una potencia p^k que cumple $|f(p^k)| \leq \frac{\epsilon}{A}$ y por lo tanto n puede ser factorizado de la siguiente manera:

$$n = \prod_{i=1}^{r} p_i^{k_i} \prod_{i=r+1}^{r+s} p_i^{k_i} \prod_{i=r+s+1}^{r+s+t} p_i^{k_i},$$

donde

$$\begin{aligned} |f(p_i^{k_i})| &\geq 1 \qquad \text{Para } i=1,2,\ldots,r \\ 1 > |f(p_i^{k_i})| &\geq \frac{\epsilon}{A} \quad \text{Para } i=r+1,r+2,\ldots,r+s \\ |f(p_i^{k_i})| &\leq \frac{\epsilon}{A} \quad \text{Para } i=r+s+1,r+s+2,\ldots,r+s+t \text{ y } t\geq 1\ . \end{aligned}$$

Por lo tanto

$$|f(n)| = \prod_{i=1}^{r} |f(p_i^{k_i})| \prod_{i=r+1}^{r+s} |f(p_i^{k_i})| \prod_{i=r+s+1}^{r+s+t} |f(p_i^{k_i})| < A\left(\frac{\epsilon}{A}\right)^t \leq \epsilon.$$

Con lo cual el lema queda demostrado. □

Como consecuencia directa del lema 2.3.1 tenemos el siguiente:

Corolario 2.3.2. Sea $\epsilon > 0$. Entonces, para toda n suficientemente grande tenemos

$$n^{1-\epsilon} < \phi(n) < n.$$

Demostración. De la definición de la función de Euler es claro que $\phi(n) < n$. Además tenemos que $\phi(p^m) = p^m - p^{m-1}$ puesto que sólo hay p^{m-1} enteros menores que p^m que no son primos relativos con p^m; a saber $p, 2p, \ldots, p^{m-1}p$. Por lo tanto

$$\begin{aligned} \frac{p^{m(1-\epsilon)}}{\phi(p^m)} &= \frac{p^{m(1-\epsilon)}}{p^m - p^{m-1}} = \frac{p^{m(1-\epsilon)}}{p^{m-1}(p-1)} \\ &= \frac{pp^{m(1-\epsilon)}}{p^m(p-1)} = \frac{p}{p-1}\frac{p^{m(1-\epsilon)}}{p^m}. \end{aligned}$$

Por otro lado, cada número primo p satisface $\frac{p}{p-1} \leq 2$ y en consecuencia

$$\frac{p^{m(1-\epsilon)}}{\phi(p^m)} \leq \frac{2}{p^{m\epsilon}}.$$

Considerando ahora el límite cuando $p^m \to \infty$ tenemos que $\frac{p^{m(1-\epsilon)}}{\phi(p^m)} \to 0$ y dado que la función $\frac{n^{1-\epsilon}}{\phi(n)}$ es multiplicativa, el resultado se sigue del lema 2.3.1. □

2.4 Más Sobre la Función Divisor

Los resultados que presentamos en esta sección, son estimaciones de sumas que involucran a la función divisor, dichas estimaciones nos facilitarán el trabajo notablemente en el capítulo 5. Las siguientes definiciones son pertinentes.

Definición 2.4.1. Para cualquier $x \in \mathbb{R}$, denotamos con $[x]$ a la parte entera de x; es decir $[x]$ es el mayor entero menor o igual que x.

Definición 2.4.2. Dadas dos funciones $f : \mathbb{R} \to \mathbb{C}$ y $g : \mathbb{R} \to \mathbb{C}$, decimos que $f(x) = O(g(x))$ cuando $x \to \infty$, si existe una constante $C > 0$ que no depende de x de tal forma que $|f(x)| \leq C|g(x)|$, cuando $x \to \infty$.

Lema 2.4.3. *Sea d la función divisor. Entonces*

1. $\sum_{n \leq x} d(n) = xlog(x) + O(x)$, *para* $x \geq 1$.
2. $\sum_{n \leq x} \frac{d(n)}{n} = \frac{1}{2} log^2(x) + O(log(x))$.
3. $\sum_{n \leq x} d^2(n) = O(xlog^3(x))$.

Demostración. 1. Ya que $d(n) = \sum_{d|n} 1$ tenemos

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

Haciendo $n = qd$, la suma $\sum_{d|n} 1$ se puede interpretar como $\sum_{n=qd} 1$ donde esta última suma se extiende sobre todos los pares de enteros positivos q, d tales que $1 \leq d \leq x$ y $1 \leq q \leq \frac{x}{d}$. Entonces

$$\sum_{n \leq x} d(n) = \sum_{\substack{q,d \\ qd \leq x}} 1.$$

Podemos interpretar también esta suma, como una suma extendida a ciertos puntos reticulares[2] del plano qd. Los puntos reticulares con $qd = n$ pertenecen

[2]Un punto reticular es un punto con coordenadas enteras.

a la hipérbola $d = \frac{n}{q}$, de tal modo que la suma en la que estamos interesados cuenta el número de puntos reticulares que se hayan sobre las hipérbolas que corresponden a $n = 1, 2, \ldots, [x]$. Para cada $d \leq x$ fijo podemos contar los puntos reticulares que se encuentran en el segmento de recta $1 \leq q \leq \frac{x}{d}$ y después sumar para todos los $d \leq x$. De esta manera tenemos

$$\sum_{n\leq x} d(n) = \sum_{d\leq x}\sum_{q\leq \frac{x}{d}} 1,$$

donde

$$\sum_{q\leq \frac{x}{d}} 1 = \frac{x}{d} + O(1).$$

Utilizando este resultado junto con la primera parte del lema A.2.7 obtenemos

$$\begin{aligned}
\sum_{d|n} d(n) &= \sum_{d\leq x}\left\{\frac{x}{d} + O(1)\right\} = \sum_{d\leq x}\frac{x}{d} + \sum_{d\leq x} O(1) \\
&= x\left\{log(x) + C + O\left(\frac{1}{x}\right)\right\} + O(x) \\
&= xlog(x) + O(x).
\end{aligned}$$

2. Utilizando la fórmula para sumar de Abel (lema A.2.4) con $u(n) = d(n)$, $U(x) = \sum_{n\leq x} d(n)$ y $f(t) = \frac{1}{x}$ se tiene que:

$$\begin{aligned}
\sum_{n\leq x}\frac{d(n)}{n} &= \frac{1}{x}\sum_{n\leq x} d(n) + \int_1^x \frac{tlog(t) + O(t)}{t^2}dt \\
&= log(x) + O(1) + \int_1^x \frac{log(t)}{t}dt + O\left(\int_1^x \frac{dt}{t}\right) \\
&= \frac{1}{2}log^2(x) + O(log(x)).
\end{aligned}$$

3. En el lema 2.1.3 probamos que la función divisor es multiplicativa, sin embargo si $(a, b) \neq 1$ tenemos que existe al menos un divisor común de a y b, lo cual nos lleva a la desigualdad $d(ab) \leq d(a)d(b)$ para cualesquiera dos

enteros positivos a y b. De lo anterior tenemos

$$\begin{aligned}
\sum_{n\leq x} d^2(n) &= \sum_{n\leq x} d(n) \sum_{n=ab} 1 = \sum_{ab\leq x} d(ab) \leq \sum_{ab\leq x} d(a)d(b) \\
&= \sum_{a\leq x} d(a) \sum_{b\leq \frac{x}{a}} d(b) = \sum_{a\leq x} d(a)\left(\frac{x}{a}log\left(\frac{x}{a}\right) + O\left(\frac{x}{a}\right)\right) \\
&= \underbrace{\sum_{a\leq x} d(a)\left(\frac{x}{a}log\left(\frac{x}{a}\right)\right)}_{S_1} + \underbrace{\sum_{a\leq x} d(a)O\left(\frac{x}{a}\right)}_{S_2}.
\end{aligned}$$

Para S_1 tenemos

$$\begin{aligned}
S_1 &\leq xlog(x)\sum_{a\leq x}\frac{d(a)}{a} = xlog(x)\left\{\frac{1}{2}log^2(x) + O\Big(log(x)\Big)\right\} \\
&= \frac{1}{2}xlog^3(x) + O\Big(xlog^2(x)\Big) = O\Big(xlog^3(x)\Big).
\end{aligned}$$

Para S_2 se tiene

$$\begin{aligned}
S_2 &= O\left(x\sum_{a\leq x}\frac{d(a)}{a}\right) = O\left(x\left(\frac{1}{2}log^2(x) + O\Big(log(x)\Big)\right)\right) \\
&= O\left(xlog^2(x) + O\Big(log(x)\Big)\right) = O\Big(xlog^2(x)\Big).
\end{aligned}$$

□

2.5 Partes Fraccionarias

El resultado principal de esta sección es el lema 2.5.4. Este lema es de fundamental importancia pues está íntimamente relacionado, con la aplicación que haremos del método de Hardy-Littlewood-Ramanujan a la conjetura impar de Goldbach.

Definición 2.5.1. Para cualquier $\alpha \in \mathbb{R}$, definimos $||\alpha||$ como la distancia de α al entero más cercano, es decir $||\alpha|| = \min_{z\in\mathbb{Z}}\{|z-\alpha|\}$.

Lema 2.5.2. *Para cualquier número real α,*

$$|sen(\pi\alpha)| = sen(\pi||\alpha||).$$

Demostración. Tenemos que $\alpha = n \pm ||\alpha||$ para algún entero n, entonces

$$\begin{aligned}
|sen(\pi\alpha)| &= |sen(\pi(n \pm ||\alpha||))| \\
&= |sen(\pi n \pm \pi||\alpha||)| \\
&= |sen(\pi n)cos(\pi||\alpha||) \pm cos(\pi n)sen(\pi||\alpha||)| \\
&= |sen(\pi||\alpha||)|.
\end{aligned}$$

Y ya que $||\alpha|| \in [0, \frac{1}{2}]$ obtenemos el resultado deseado. □

Lema 2.5.3. *Si $0 < \alpha < \frac{1}{2}$, entonces $2\alpha < sen(\pi\alpha) < \pi\alpha$.*

Demostración. Sea $f(\alpha) = sen(\pi\alpha) - 2\alpha$. Entonces $f(0) = f(\frac{1}{2}) = 0$. Si $f(\alpha) = 0$ para algún $\alpha \in (0, \frac{1}{2})$, entonces $\frac{df}{d\alpha} = \pi cos(\pi\alpha) - 2$ tendría al menos dos ceros en $(0, \frac{1}{2})$, lo cual no puede ser pues $\frac{df}{d\alpha}$ decrece monótonamente de $\pi - 2$ a -2 en este intervalo. Ya que $f(\frac{1}{4}) = \frac{\sqrt{2}-1}{2} > 0$, tenemos que $f(\alpha) > 0$ para todo $\alpha \in (0, \frac{\pi}{2})$, de donde $2\alpha < sen(\pi\alpha)$. Análogamente se prueba que $sen(\pi\alpha) < \pi\alpha$.

□

Lema 2.5.4. *Sea β un número real tal que $|\beta| \leq \frac{1}{2}$, entonces*

$$\sum_{m=1}^{N} e^{2\pi i m\beta} = O(|\beta|^{-1}).$$

Demostración.

$$\begin{aligned}
\Big|\sum_{m=1}^{N} e^{2\pi i m\beta}\Big| &= \Big|\sum_{m=1}^{N} e^{(2\pi i\beta)^m}\Big| = \Big|\frac{1 - e^{(2\pi i\beta)^N}}{1 - e^{2\pi i\beta}}\Big| \leq \frac{2}{|1 - e^{2\pi i\beta}|} \\
&= \frac{2}{|e^{\pi i\beta} - e^{-\pi i\beta}|} = \frac{2}{|2isen(\pi\beta)|} = \frac{1}{|sen(\pi\beta)|} \\
&= \frac{1}{sen(\pi||\beta||)}.
\end{aligned}$$

Haciendo uso del lema 2.5.3

$$\frac{1}{sen(\pi||\beta||)} \leq \frac{1}{2||\beta||} = \frac{1}{2|\beta|}.$$

□

2.6 Aproximación por Racionales

El propósito de esta sección es presentar el llamado principio de Dirichlet. Este principio nos permite aproximarnos a un número real mediante fracciones con denominador "pequeño". En el capítulo 5, este resultado será la clave para obtener una fórmula asintótica para el número de representaciones de un natural como suma de tres primos.

Definición 2.6.1. Para cualquier número real α definimos $\{\alpha\}$ la parte fraccionaria de α como: $\alpha - [\alpha]$.

Lema 2.6.2 (Principio de Dirichlet). *Sean α y Q números reales, $Q \geq 1$. Existen dos números enteros a y q tales que*

$$1 \leq q \leq Q, \quad (a, q) = 1 \quad y \quad \left|\alpha - \frac{a}{q}\right| < \frac{1}{qQ}.$$

Demostración. Sea $N = [Q]$ y consideremos $\{q\alpha\}$ para $q = 1, 2, \ldots, N$. Tenemos tres casos:

1. $\{q\alpha\} \in [0, \frac{1}{N+1})$ para algún entero positivo $q \leq N$.
2. $\{q\alpha\} \in [\frac{N}{N+1}, 1)$ para algún entero positivo $q \leq N$.
3. $\{q\alpha\} \in [\frac{1}{N+1}, \frac{N}{N+1})$ para todo $q = 1, 2 \ldots, N$ y en consecuencia cada uno de los N números $\{q\alpha\}$ está en alguno de los $N - 1$ intervalos

$$\left[\frac{i}{N+1}, \frac{i+1}{N+1}\right) \quad i = 1, 2, \ldots, N-1.$$

- Caso 1. Si $a = [q\alpha]$, entonces
$$0 \le \{q\alpha\} = q\alpha - [q\alpha] = q\alpha - a < \frac{1}{N+1}$$
y por lo tanto
$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{q(N+1)} < \frac{1}{qQ}.$$

- Caso 2. Si $a = [q\alpha] + 1$, entonces
$$\frac{N}{N+1} \le \{q\alpha\} = q\alpha - a + 1 < 1 = \frac{N+1}{N+1}$$
implica que
$$|q\alpha - a| \le \frac{1}{N+1}$$
y por lo tanto
$$\left|\alpha - \frac{a}{q}\right| \le \frac{1}{q(N+1)} < \frac{1}{qQ}.$$

- Caso 3. Si $\{q\alpha\} \in [\frac{1}{N+1}, \frac{N}{N+1})$ para todo $q = 1, 2 \ldots, N$, entonces cada uno de los N números reales $\{q\alpha\}$ está en uno de los $N-1$ intervalos
$$\left[\frac{i}{N+1}, \frac{i+1}{N+1}\right) \quad i = 1, 2, \ldots, N-1.$$
Por lo tanto, dado que tenemos que repartir N números reales en $N-1$ intervalos, entonces existen enteros $i \in [1, N-1]$ y q_1, $q_2 \in [1, N]$ tales que
$$1 \le q_1 < q_2 \le N \quad \text{y} \quad \{q_1\alpha\}, \{q_2\alpha\} \in \left[\frac{i}{N+1}, \frac{i+1}{N+1}\right).$$
Sea $q = q_2 - q_1 \in [1, N-1]$ y $a = [q_2\alpha] - [q_1\alpha]$ entonces
$$\begin{aligned} |q\alpha - a| &= |(q_2\alpha - [q_2\alpha]) - (q_1\alpha - [q_1\alpha])| \\ &= |\{q_2\alpha\} - \{q_1\alpha\}| < \frac{1}{N+1} < \frac{1}{Q}. \end{aligned}$$
Por lo tanto
$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{qQ}.$$

En los tres casos el número $\frac{a}{q}$ se puede reducir de tal modo que $(a, q) = 1$.

□

2.7 Resultados Adicionales

Terminamos este capítulo de preliminares con algunos teoremas remarcables de teoría analítica de números. La demostración de estos teoremas no es en absoluto trivial, pues se requieren técnicas sofisticadas de variable compleja que van más allá del objetivo de este trabajo. No obstante, damos referencias al lector interesado en ver la demostración a la bibliografía correspondiente.

El primero de estos resultados es conocido como el teorema de los números primos y fue probado independientemente por el matemático francés J. Hadamar y su homólogo belga C. de la Vallée Poussin en 1896.

Teorema 2.7.1. *Sea $\pi(n)$ la cantidad de números primos menores o iguales a n, entonces*

$$\pi(n)\frac{ln(x)}{x} = O(1).$$

Una demostración muy elegante del teorema anterior se puede ver en [4], sin embargo existe un resultado más fuerte que el anterior que enunciamos a continuación:

Teorema 2.7.2 (de la Vallée Poussin). *Existe una constante positiva $c > 0$ tal que*

$$\pi(n) = \int_2^n \frac{d\gamma}{log(\gamma)} + O\Big(ne^{-c\sqrt{log(n)}}\Big).$$

Referimos al lector interesado en la demostración a [3].

El siguiente teorema debido al matemático alemán Carl Ludwig Siegel, nos da una estimación de la cantidad de números primos en una progresión aritmética.

Teorema 2.7.3 (Siegel). *Sea $u > 1$ y $1 \leq q \leq log^u(N)$, entonces existe una constante $c_1 = c_1(u) > 0$ tal que*

$$\Pi(N; q, m) = \frac{1}{\phi(q)} \int_2^N \frac{d\gamma}{log(\gamma)} + O\Big(Ne^{-c_1\sqrt{log(N)}}\Big), \tag{2.1}$$

donde $\Pi(N; q, m)$ *es el número de primos menores o iguales que* N *que son congruentes con* m *módulo* q

La demostración de este teorema se puede encontrar en [3].

El siguiente teorema, debido al matemático escocés Robert A. Rankin será utilizado en el capítulo 5 de manera crucial.

Teorema 2.7.4 (Rankin). *Sea* $R(x, y)$ *el número de enteros positivos menores o iguales que* x *cuyos factores primos son menores o iguales que* y*, entonces*

$$\begin{aligned} R(x,y) = x\ exp\Big\{ -log(x)\frac{log(log(log(y)))}{log(y)} &+ log(log(y)) \\ &+ O\Big(\frac{log(log(y))}{log(log(log(y)))}\Big)\Big\}. \end{aligned}$$

El lector interesado en los detalles técnicos, puede encontrar la demostración de este teorema en [5].

Capítulo 3

Sumas de Tres Primos

En este capítulo escribiremos $r_3(N)$ (el número de representaciones de un natural como suma de tres primos) en términos de una integral oscilatoria y descompondremos el dominio de integración según el método de Hardy-Littlewood-Ramanujan en arcos mayores y menores. De aquí en adelante, omitiremos el subíndice 3 y escribiremos simplemente $r(N)$.

A partir de este momento, nuestro objetivo será obtener una fórmula asintótica de $r(N)$; es decir, una fórmula con un margen de error despreciable para N suficientemente grande, que estime cuantas soluciones tiene la ecuación (3.1) donde p_i es primo para $i = 1, 2, 3$.

$$N = p_1 + p_2 + p_3. \tag{3.1}$$

3.1 Forma Integral para *r(N)*

El lema 3.1.1 nos dará un equivalente de $r(N)$ que será la pauta para lo que resta de este trabajo.

Lema 3.1.1. *Consideremos la suma trigonométrica*

$$S_N(\theta) = \sum_{p \leq N} e^{2\pi i p\theta}, \tag{3.2}$$

donde p es un número primo y θ es un número real, entonces

$$r(N) = \int_0^1 e^{-2\pi i N\theta} S_N^3(\theta) d\theta. \tag{3.3}$$

Demostración.

$$\begin{aligned}\int_0^1 e^{-2\pi i N\theta} S_N^3(\theta) d\theta &= \int_0^1 e^{-2\pi i N\theta} \sum_{p_1,p_2,p_3 \leq N} e^{2\pi i\theta(p_1+p_2+p_3)} d\theta \\ &= \sum_{p_1,p_2,p_3 \leq N} \int_0^1 e^{2\pi i\theta(p_1+p_2+p_3-N)} d\theta\end{aligned}$$

donde

$$\int_0^1 e^{2\pi i p\theta(p_1+p_2+p_3-N)} d\theta = 0$$

a menos que $N = p_1 + p_2 + p_3$ en cuyo caso vale 1. □

Observación 3.1.2. El corolario 1.0.4 se reduce a probar, que la integral 3.3 es mayor que cero para cualquier N impar, suficientemente grande.

Como mencionamos anteriormente, nuestro objetivo es encontrar una fórmula asintótica para $r(N)$. Específicamente, lo que queremos probar en este trabajo es el teorema de Vinogradov en el cual se asegura que $r(N) \geq C\frac{N^2}{log^3(N)}$ con C una constante positiva[1]. Dicha prueba está íntimamente relacionada con la obtención de una buena estimación de la integral 3.3 y en particular de una buena estimación de la suma trigonométrica 3.2. Para obtener dichas estimaciones utilizaremos el método de Hardy-Littlewood, junto con un método para estimar ciertas sumas exponenciales desarrollado por el mismo Vinogradov.

3.2 Descomposición de Hardy-Littlewood

El método de Hardy-Littlewood, asegura que la contribución principal a una integral como en la que estamos interesados, proviene de la unión $\mathfrak{M}$

[1] Ver teorema 1.0.3

de "pequeños" intervalos $\mathfrak{M}(a,q)$ alrededor de fracciones $\frac{a}{q}$, con q "no muy grande" y $(a,q)=1$, llamados por razones históricas *arcos mayores*[2]. De tal modo que la integral sobre $\mathfrak{M}^c = \mathfrak{m}$ o *arcos menores* es despreciable cuando N es suficientemente grande. Lo anterior sugiere la siguiente descomposición:

$$r(N) = \underbrace{\int_{\mathfrak{M}} e^{-2\pi i N\theta} S_N^3(\theta)d\theta}_{M(N)} + \underbrace{\int_{\mathfrak{m}} e^{-2\pi i N\theta} S_N^3(\theta)d\theta}_{E(N)}, \tag{3.4}$$

donde $M(N)$ es la parte principal y $E(N)$ puede interpretarse como el error.

En la siguiente sección definiremos de manera precisa los arcos mayores y los arcos menores para el problema ternario de Goldbach, como también se le llama a la conjetura de Goldbach para el caso impar.

3.2.1 Construcción de los Arcos Mayores $\mathfrak{M}$

Dado un número natural N y u un número real positivo (por ser determinado posteriormente), para $1 \leq q \leq log^u(N)$ y $0 < a \leq q-1$ con $(a,q)=1$, definimos:

$$\begin{aligned} \mathfrak{M}(a,q) &= \Big\{\theta \in [0,1] : \big|\theta - \frac{a}{q}\big| \leq \frac{log^u(N)}{N}\Big\} \\ \mathfrak{M} &= \bigcup_{q=1}^{log^u(N)} \bigcup_{\substack{a=1 \\ (a,q)=1}}^{q-1} \mathfrak{M}(a,q). \end{aligned}$$

En la brevísima descripción que dimos sobre el método de Hardy-Littlewood, se les dió el adjetivo de "pequeños" a los arcos mayores. En nuestro problema esto significa que los intervalos $\mathfrak{M}(a,q)$ constan de los números reales $\theta \in [0,1]$ que distan en menos de $\frac{log^u(N)}{N}$ de fracciones $\frac{a}{q}$ con q "no muy grande" donde esto último quiere decir que $q \leq log^u(N)$. Cabe mencionar que estos valores $\left(log^u(N) \text{ y } \frac{log^u(N)}{N}\right)$ han sido elegidos por necesidad, pues más adelante haremos uso del Teorema 2.7.3.

[2]Aquí el significado preciso de "pequeños" y "no muy grande" depende de las aplicaciones, no obstante para nuestro caso particular se establecerá de manera precisa este significado en la sección 3.2.1 de este capítulo.

Dado que estamos interesados en el comportamiento asintótico de la integral $r(N)$, es conveniente determinar el comportamiento de los arcos mayores en términos de N.

Lema 3.2.2. *Si N es suficientemente grande, los intervalos $\mathfrak{M}(a, q)$ son disjuntos.*

Demostración. Si existe un número real $\theta \in \mathfrak{M}(a_1, q_1) \cap \mathfrak{M}(a_2, q_2)$ donde $\frac{a_1}{q_1} \neq \frac{a_2}{q_2}$, entonces
$|a_1 q_2 - a_2 q_1| \geq 1$ y por lo tanto

$$\begin{aligned} \frac{1}{log^{2u}(N)} &\leq \frac{1}{q_1 q_2} \leq \left|\frac{a_1 q_2 - q_1 a_2}{q_1 q_2}\right| = \left|\frac{a_1}{q_1} - \frac{a_2}{q_2}\right| \\ &\leq \left|\frac{a_1}{q_1} - \theta\right| + \left|\frac{a_2}{q_2} - \theta\right| \leq 2\frac{log^u(N)}{N} \end{aligned}$$

de donde $N \leq 2log^{3u}(N)$ lo cual es imposible si N es suficientemente grande. $\square$

3.2.3 Construcción de los Arcos Menores $\mathfrak{m}$

Teniendo en consideración el conjunto $\mathfrak{M}$, definimos

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

El conjunto $\mathfrak{m}$ es una unión finita de intervalos abiertos y sus elementos son todos los números reales $\theta \in [0, 1]$ que distan en más de $\frac{log^u(N)}{N}$ de las fracciones $\frac{a}{q}$ involucradas en $\mathfrak{M}(a, q)$.

Una vez construidos los arcos mayores y menores, el siguiente paso es estimar $M(N)$ y $E(N)$ por separado. Una buena referencia para el lector interesado en ahondar en los detalles técnicos del método de Hardy-Littlewood es [2].

Capítulo 4

La Integral Sobre los Arcos Mayores

En vista del lema 3.2.2 basta estimar la integral 4.1 y después considerar la integral sobre la unión de los intervalos $\mathfrak{M}(a,q)$.

$$\int_{\mathfrak{M}(a,q)} e^{-2\pi i N\theta} S_N^3(\theta) d\theta. \tag{4.1}$$

Ya que el punto clave en todo esto es obtener una buena estimación de la suma trigonométrica $S_N(\theta)$, le recordamos al lector que:

$$S_N(\theta) = \sum_{p \leq N} e^{2\pi i p\theta}. \tag{4.2}$$

4.1 Estimación de $S_N(\theta)$ en los Arcos Mayores

Cada número real $\theta \in \mathfrak{M}$ está contenido en algún intervalo $\mathfrak{M}(a,q)$, en consecuencia, podemos escribir $\theta = \frac{a}{q} + \beta$ con $|\beta| \leq \frac{log^u(N)}{N}$ y tenemos la siguiente relación:

$$M(N) = \sum_{q=1}^{log^u(N)} \sum_{a=1}^{q-1} e^{-2\pi i N\frac{a}{q}} \int_{-\frac{\log^u(N)}{N}}^{\frac{\log^u(N)}{N}} e^{-2\pi i N\beta} S_N^3(\frac{a}{q} + \beta) d\beta. \tag{4.3}$$

Esta igualdad nos sugiere de alguna manera que es conveniente saber cómo se comporta $S_N(\theta)$ en $\mathfrak{M}(a,q)$. Como primer paso en esta dirección estimaremos $S_N(\theta)$ en $\theta = \frac{a}{q}$ donde $(a,q) = 1$, $1 \leq a \leq q-1$ y $1 \leq q \leq log^u(N)$.

Lema 4.1.1. *Sean $(a,q) = 1$ con $0 < a \leq q-1$ y $1 \leq q \leq log^u(N)$, entonces*

$$S_N\left(\frac{a}{q}\right) = \sum_{\substack{m=1 \\ (m,q)=1}}^{q} \Pi(N,q,m) e^{2\pi i m \frac{a}{q}} + \sum_{\substack{p \leq N \\ p|q}} e^{2\pi i p \frac{a}{q}},$$

donde $\Pi(N,q,m)$ es el número de primos menores o iguales que N que son congruentes con m módulo q.

Demostración. La suma $S_N(\frac{a}{q})$ se puede descomponer de la siguiente manera

$$S_N\left(\frac{a}{q}\right) = \underbrace{\sum_{\substack{p \leq N \\ (p,q)=1}} e^{2\pi i p \frac{a}{q}}}_{S_1} + \underbrace{\sum_{\substack{p \leq N \\ (p,q)\neq 1}} e^{2\pi i p \frac{a}{q}}}_{S_2}.$$

En el caso de S_1 tenemos que $e^{2\pi i p \frac{a}{q}} = e^{2\pi i m \frac{a}{q}}$ si $m \equiv p (mod\, q)$, por lo tanto,

$$S_1 = \sum_{\substack{m=1 \\ (m,q)=1}}^{q} \Pi(N,q,m) e^{2\pi i m \frac{a}{q}}$$

Por otro lado, ya que en S_2 tenemos $(p,q) \neq 1$, entonces existe $d \geq 2$ tal que $d|p$ lo cual implica que $d = p$ pero como además $d|q$ tenemos entonces que $p|q$ y por consiguiente

$$S_2 = \sum_{\substack{p \leq N \\ p|q}} e^{2\pi i p \frac{a}{q}},$$

con lo cual el lema queda demostrado. □

Observación 4.1.2. En el capítulo 2 sección 2.7 enunciamos el teorema 2.7.3 sobre la cantidad de primos en una progresión aritmética. Este teorema que será utilizado en el lema 4.1.3, está íntimamente relacionado con la construcción de los arcos mayores en la sección 3.2.1 del capítulo 3, de hecho la necesidad de tomar $1 \leq q \leq log^u(N)$ en dicha construcción queda justificada por este teorema. Por lo anterior, la primer restricción que le pondremos a u, es que sea estrictamente mayor que uno.

Lema 4.1.3. *Sean $(a, q) = 1$ con $0 < a \leq q - 1$, $1 \leq q \leq log^u(N)$ y $u > 1$ un número real. Entonces, existe $c_1 = c_1(u) > 0$ tal que*

$$S_N\left(\frac{a}{q}\right) = \frac{\mu(q)}{\phi(q)} \int_2^N \frac{d\gamma}{log(\gamma)} + O\left(qNe^{-c_1\sqrt{log(N)}}\right) + O(log(q)),$$

donde μ y ϕ son las funciones de Moebius y Euler respectivamente.

Demostración. Del lema 4.1.1 tenemos

$$S_N\left(\frac{a}{q}\right) = \sum_{\substack{m=1 \\ (m,q)=1}}^{q} \Pi(N, q, m)e^{2\pi i m\frac{a}{q}} + \sum_{\substack{p \leq N \\ p|q}} e^{2\pi i p\frac{a}{q}}.$$

Sea $q = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ la descomposición en factores primos de q. Utilizando las propiedades de la función logaritmo tenemos

$$log(q) = \sum_{i=1}^{r} \alpha_i log(p_i) \geq \sum_{i=1}^{r} log(2) = rlog(2),$$

de donde $r \leq \frac{log(q)}{log(2)} = log_2(q)$[1] y por consiguiente

$$\left| \sum_{\substack{p \leq N \\ p|q}} e^{2\pi i p\frac{a}{q}} \right| \leq \sum_{\substack{p \leq N \\ p|q}} 1 \leq r = log_2(q) = O(log(q)).$$

[1]Basta aplicar la función logaritmo en ambos lados de la ecuación $2^{log_2(q)} = q$

Por otro lado, del teorema 2.7.3 tenemos

$$\begin{aligned}
&\sum_{\substack{m=1\\(m,q)=1}}^{q} \Pi(N,q,m)e^{2\pi i m\frac{a}{q}} = \\
&= \sum_{\substack{m=1\\(m,q)=1}}^{q} \left(\frac{1}{\phi(q)}\int_2^N \frac{d\gamma}{log(\gamma)} + O(Ne^{-c_1\sqrt{log(N)}})\right)e^{2\pi i m\frac{a}{q}} \\
&= \sum_{\substack{m=1\\(m,q)=1}}^{q} \frac{1}{\phi(q)}\int_2^N \frac{d\gamma}{log(\gamma)}e^{2\pi i m\frac{a}{q}} + \sum_{\substack{m=1\\(m,q)=1}}^{q} O\big(Ne^{-c_1\sqrt{log(N)}}\big)e^{2\pi i m\frac{a}{q}} \\
&= \sum_{\substack{m=1\\(m,q)=1}}^{q} \frac{1}{\phi(q)}\int_2^N \frac{d\gamma}{log(\gamma)}e^{2\pi i m\frac{a}{q}} + O\big(qNe^{-c_1\sqrt{log(N)}}\big) \\
&= \frac{1}{\phi(q)}\int_2^N \frac{d\gamma}{log(\gamma)} \sum_{\substack{m=1\\(m,q)=1}}^{q} e^{2\pi i m\frac{a}{q}} + O\big(qNe^{-c_1\sqrt{log(N)}}\big),
\end{aligned}$$

donde la suma involucrada en esta última igualdad, es la suma de Ramanujan $c_q(a)$ de la sección 2.2 del capítulo 2 y el resultado se sigue del lema 2.2.5. $\square$

Hasta el momento tenemos que $S_N(\frac{a}{q}) = \frac{\mu(q)}{\phi(q)}\int_2^N \frac{d\gamma}{log(\gamma)}$ salvo términos $O\Big(qNe^{-c_1\sqrt{log(N)}}\Big)$ y $O(log(q))$. En el lema 4.1.6 veremos que estos términos pueden ser reemplazados, por términos $O(Ne^{-c_2\sqrt{log(N)}})$ para alguna constante positiva $c_2 = c_2(u)$ estrictamente menor que c_1. Tenemos el siguiente resultado previo.

Lema 4.1.4. *Sea $u > 1$ y c'' una constante positiva que puede depender de u. Entonces*

$$O\Big(log^u(N)e^{-c''\sqrt{log(N)}}\Big) = O\Big(e^{-c'\sqrt{log(N)}}\Big),$$

donde $0 < c' < c''$.

Demostración. Sabemos que $e^x \geq \frac{x^m}{m!}$ para todo $n \in \mathbb{N}$, por lo tanto para $x > 1$ y δ un número real positivo, tenemos las siguientes desigualdades

$$\frac{x^\delta}{([\delta]+1)!} \leq \frac{x^{[\delta]+1}}{([\delta]+1)!} \leq e^x.$$

Por lo anterior, si tomamos $0 < c' < c''$ y hacemos $x = (c'' - c')\sqrt{log(N)}$ con N suficientemente grande y $\delta = 2u$, tenemos

$$log^u(N) \leq C(u)e^{(c''-c')\sqrt{log(N)}}.$$

El resultado se sigue trivialmente. $\square$

Observación 4.1.5. En lo sucesivo estaremos utilizando constantemente el resultado anterior para realizar algunas estimaciones. De aquí en adelante cada que este lema vaya a ser utilizado, sólo haremos alusión al hecho de que estamos tomando una constante positiva $c' < c''$ según sea el caso.

Lema 4.1.6. *Sean $(a, q) = 1$ con $0 < a \leq q - 1$, $1 \leq q \leq log^u(N)$ y $u > 1$. Sea c_1 como en el lema 4.1.3, entonces*

$$S_N\Big(\frac{a}{q}\Big) = \frac{\mu(q)}{\phi(q)}\int_2^N \frac{d\gamma}{log(\gamma)} + O(Ne^{-c_2\sqrt{log(N)}}),$$

donde $0 < c_2 < c_1$.

Demostración. Basta probar que $qNe^{-c_1\sqrt{log(N)}}$ y $log(q)$ son $O(Ne^{-c_2\sqrt{log(N)}})$ con $0 < c_2 < c_1$.
El hecho de que $qNe^{-c_1\sqrt{log(N)}} = O(Ne^{-c_2\sqrt{log(N)}})$ se sigue del lema 4.1.4 y de observar que $q \leq log^u(N)$.
Por otro lado, para x suficientemente grande tenemos

$$e^{\frac{x}{2}} \geq log(x) \quad \text{y} \quad e^{\frac{x}{2}} \geq Ce^{c_2\sqrt{x}},$$

por lo tanto $log(x) \leq Ce^{x-c_2\sqrt{x}}$. Haciendo $x = log(N)$ obtenemos

$$log\Big(log(N)\Big) \leq CNe^{-c_2\sqrt{log(N)}},$$

entonces

$$\begin{aligned} log(q) &\leq log(log^u(N)) = ulog(log(N)) \\ &\leq CuNe^{-c_2\sqrt{log(N)}} = C'Ne^{-c_2\sqrt{log(N)}}, \end{aligned}$$

donde C' depende de u. $\square$

El lema 4.1.6 nos proporciona una estimación de la suma trigonométrica $S_N(\theta)$ en fracciones $\theta = \frac{a}{q}$ con $(a, q) = 1$, $1 \leq a \leq q - 1$ y $1 \leq q \leq log^u(N)$. Sin embargo, como el título de esta sección lo dice, estamos interesados en estimar $S_N(\theta)$ en los arcos mayores $\mathfrak{M}$; es decir en $\theta = \frac{a}{q} + \beta$ con $|\beta| \leq \frac{log^u(N)}{N}$. Esto no significa que el trabajo anterior haya sido en vano como veremos en el siguiente:

Lema 4.1.7. *Sean $(a, q) = 1$ con $0 < a \leq q - 1$ y $1 \leq q \leq log^u(N)$. Sea β un número real tal que $|\beta| \leq \frac{log^u(N)}{N}$ y c_2 como en el lema 4.1.6, entonces*

$$S_N\Big(\frac{a}{q} + \beta\Big) = \frac{\mu(q)}{\phi(q)} \sum_{3 \leq n \leq N} \frac{e^{2\pi i n\beta}}{log(n)} + O(Ne^{-c_3\sqrt{log(N)}}),$$

donde $0 < c_3 < c_2$.

Demostración. Si n no es primo, entonces $S_n(\frac{a}{q}) = S_{n-1}(\frac{a}{q})$ y por lo tanto

$$S_N\Big(\frac{a}{q} + \beta\Big) = \sum_{2 \leq n \leq N} \bigg(S_n\Big(\frac{a}{q}\Big) - S_{n-1}\Big(\frac{a}{q}\Big)\bigg)e^{2\pi i n\beta}.$$

Utilizando el método para sumar de Abel (lema A.2.4) tenemos

$$S_N\Big(\frac{a}{q} + \beta\Big) = S_N\Big(\frac{a}{q}\Big)e^{2\pi i N\beta} + \sum_{2 \leq n \leq N-1} S_n\Big(\frac{a}{q}\Big)\Big[e^{2\pi i n\beta} - e^{2\pi i(n+1)\beta}\Big].$$

Es precisamente en este punto en el que queda justificado nuestro trabajo previo al estimar la suma $S_N(\theta)$ en $\theta = \frac{a}{q}$. Sin embargo, antes de utilizar el lema 4.1.6 para estimar la suma anterior, debemos verificar que $q \leq log^u(n)$, pues en la hipótesis de dicho lema teníamos $q \leq log^u(N)$.

Si n es tal que $\sqrt{N} < n \leq N$, podemos obtener fácilmente la desigualdad $log^u(N) < 2^u log^u(n) < 2^u log^u(N)$ y como por hipótesis $q \leq log^u(N)$, se sigue que $q < 2^u log^u(n)$. En consecuencia si N es suficientemente grande y $u' > u$ se tiene

$$2^u \leq log^{u'-u}(n) = \frac{log^{u'}(n)}{log^u(n)},$$

para toda n que satisface $\sqrt{N} < n \leq N$; Así $q \leq log^{u'}(n)$ y por el lema 4.1.6 tenemos

$$S_n\Big(\frac{a}{q}\Big) = \frac{\mu(q)}{\phi(q)} \int_2^n \frac{d\gamma}{log(\gamma)} + O(ne^{-c_2\sqrt{log(n)}}).$$

Esta misma relación se cumple para $2 \leq n \leq \sqrt{N}$ de manera trivial pues $|S_{\sqrt{N}}(\frac{a}{q})| \leq \sqrt{N} = O\Big(Ne^{-c_2\sqrt{log(N)}}\Big)$. Por lo tanto,

$$S_N\Big(\frac{a}{q} + \beta\Big) = S_1 + S_2$$

donde

$$\begin{aligned} S_1 &= \frac{\mu(q)}{\phi(q)}\Bigg(\sum_{2\leq n\leq N-1} \int_2^n \frac{\big[e^{2\pi in\beta} - e^{2\pi i(n+1)\beta}\big]d\gamma}{log(\gamma)} + \int_2^N \frac{e^{2\pi iN\beta}d\gamma}{log(\gamma)}\Bigg) \quad \text{y} \\ S_2 &= \sum_{2\leq n\leq N-1} O(ne^{-c_2\sqrt{log(n)}})\big[e^{2\pi in\beta} - e^{2\pi i(n+1)\beta}\big] \\ &+ O(Ne^{-c_2\sqrt{log(N)}})e^{2\pi iN\beta}. \end{aligned}$$

S_1 puede reescribirse como $S_1 = \frac{\mu(q)}{\phi(q)}\Big(A + B + C\Big)$, donde

$$\begin{aligned} A &= \sum_{2\leq n\leq N-1} \int_2^n \frac{e^{2\pi in\beta}d\gamma}{log(\gamma)}. \\ B &= -\sum_{2\leq n\leq N-1} \int_2^n \frac{e^{2\pi i(n+1)\beta}d\gamma}{log(\gamma)}. \\ C &= \int_2^N \frac{e^{2\pi iN\beta}d\gamma}{log(\gamma)}. \end{aligned}$$

Haciendo $m = n + 1$ en B tenemos

$$S_1 = \frac{\mu(q)}{\phi(q)} \sum_{3\leq n\leq N} \int_{n-1}^n \frac{e^{2\pi in\beta}d\gamma}{log(\gamma)}.$$

Del teorema del valor medio para $f(\gamma) = \frac{1}{log(\gamma)}$, tenemos

$$\Big|\frac{1}{log(\gamma)} - \frac{1}{log(n)}\Big| = \Big| - \frac{(\gamma - n)}{\xi log^2(\xi)}\Big| = \frac{|(\gamma - n)|}{\xi log^2(\xi)} \leq \frac{1}{\xi log^2(\xi)},$$

donde $n-1 \leq \gamma \leq \xi \leq n$, entonces

$$\int_{n-1}^{n} \frac{d\gamma}{log(\gamma)} \leq \frac{1}{log(n)} + \frac{1}{(n-1)log^2(n-1)} = \frac{1}{log(n)} + O\Big(\frac{1}{nlog^2(n)}\Big).$$

Por lo tanto

$$S_1 = \frac{\mu(q)}{\phi(q)} \sum_{3\leq n\leq N} \frac{e^{2\pi in\beta}}{log(n)} + \underbrace{\sum_{3\leq n\leq N} e^{2\pi in\beta} O\Big(\frac{1}{nlog^2(n)}\Big)}_{E}$$

donde $|E| \leq C\sum_{n=3}^{N} \frac{1}{nlog^2(n)}$ y por el lema A.2.2 tenemos que $E = O(1)$.

En el caso de S_2 como $n \leq N$ tenemos $ne^{-c_2\sqrt{log(n)}} \leq CNe^{-c_2\sqrt{log(N)}}$, por lo tanto

$$\begin{aligned}
S_2 &= O(Ne^{-c_2\sqrt{log(N)}})\Bigg(\sum_{2\leq n\leq N-1}\Big[e^{2\pi in\beta} - e^{2\pi i(n+1)\beta}\Big] + e^{2\pi iN\beta}\Bigg)\\
&= O\Bigg(Ne^{-c_2\sqrt{log(N)}}\Bigg(\sum_{2\leq n\leq N-1}\Big|e^{2\pi in\beta} - e^{2\pi i(n+1)\beta}\Big| + 1\Bigg)\Bigg)\\
&= O\Bigg(Ne^{-c_2\sqrt{log(N)}}\Bigg(\sum_{2\leq n\leq N-1}\Big|1 - e^{2\pi i\beta}\Big| + 1\Bigg)\Bigg)\\
&= O\Bigg(Ne^{-c_2\sqrt{log(N)}}\Bigg(\sum_{2\leq n\leq N-1} 2sen(\pi|\beta|) + 1\Bigg)\Bigg) \text{ ver lemas 2.5.3 y 2.5.4.}\\
&= O\Big(Ne^{-c_2\sqrt{log(N)}}(N|\beta| + 1)\Big)\\
&= O\Big(Ne^{-c_2\sqrt{log(N)}}(log^u(N) + 1)\Big)\\
&= O\Big(Ne^{-c_3\sqrt{log(N)}}\Big),
\end{aligned}$$

donde $0 < c_3 < c_2$.[2] Por último combinando ambos casos obtenemos

$$S_N(\frac{a}{q} + \beta) = \frac{\mu(q)}{\phi(q)} \sum_{3\leq n\leq N} \frac{e^{2\pi in\beta}}{log(n)} + O(Ne^{-c_3\sqrt{log(N)}}).$$

□

[2] Ver lema 4.1.4.

Lema 4.1.8. *Si $\theta \in \mathfrak{M}$, entonces*

$$S_N^3(\theta) = \Bigg(\frac{\mu(q)}{\phi(q)}\sum_{n=3}^{N}\frac{e^{2\pi i n\beta}}{log(n)}\Bigg)^3 + O\Big(N^3 e^{-c_3\sqrt{log(N)}}\Big),$$

donde $|\beta| \leq \frac{log^u(N)}{N}$ y c_3 es una constante positiva.

Demostración. Dado que $\theta \in \mathfrak{M}$ podemos escribir $\theta = \frac{a}{q}+\beta$ donde $(a,q)=1$, $0 \leq a \leq q-1$, $q \leq log^u(N)$ y β es un número real tal que $|\beta| \leq \frac{log^u(N)}{N}$, entonces del lema 4.1.7 tenemos

$$S_N^3(\theta) = \Bigg(\frac{\mu(q)}{\phi(q)}\sum_{n=3}^{N}\frac{e^{2\pi i n\beta}}{log(n)} + O\Big(N e^{-c_3\sqrt{log(N)}}\Big)\Bigg)^3.$$

Desarrollando el binomio obtenemos

$$S_N^3(\theta) = \Bigg(\frac{\mu(q)}{\phi(q)}\sum_{n=3}^{N}\frac{e^{2\pi i n\beta}}{log(n)}\Bigg)^3 + O\Big(N^3 e^{-c_3\sqrt{log(N)}}\Big) + S_1 + S_2,$$

donde

$$\begin{aligned} S_1 &= \frac{3\mu^2(q)}{\phi^2(q)}\Big(\sum_{n=3}^{N}\frac{e^{2\pi i n\beta}}{log(n)}\Big)^2 O(N e^{-c_3\sqrt{log(N)}}) = O\Big(N^3 e^{-c_3\sqrt{log(N)}}\Big). \\ S_2 &= \frac{3\mu(q)}{\phi(q)}\Big(\sum_{n=3}^{N}\frac{e^{2\pi i n\beta}}{log(n)}\Big) O(N^2 e^{-c_3\sqrt{log(N)}}) = O\Big(N^3 e^{-c_3\sqrt{log(N)}}\Big). \end{aligned}$$

pues $\Big|\sum_{n=3}^{N}\frac{e^{2\pi i n\beta}}{log(n)}\Big| \leq CN$ y $\frac{\mu(q)}{\phi(q)} \leq C$. Por lo tanto,

$$S_N^3(\theta) = \Big(\frac{\mu(q)}{\phi(q)}\sum_{n=3}^{N}\frac{e^{2\pi i n\beta}}{log(n)}\Big)^3 + O(N^3 e^{-c_3\sqrt{log(N)}}).$$

□

Lema 4.1.9. *Sea β un número real tal que $|\beta| \leq \frac{1}{2}$, entonces*

$$\sum_{n=3}^{N}\frac{e^{2\pi i n\beta}}{log(n)} = O(|\beta|^{-1}).$$

Demostración. Del método para sumar de Abel (lema A.2.4) y el lema 2.5.4, tenemos

$$\begin{aligned}
\sum_{n=3}^{N}\frac{e^{2\pi in\beta}}{log(n)} &= \left(\sum_{n=1}^{N}e^{2\pi in\beta}\right)\frac{1}{log(N)} - \int_{2}^{N}\left(\sum_{n\leq t}e^{2\pi in\beta}\right)dlog^{-1}(t).\\
&= O(|\beta|^{-1})\frac{1}{log(N)} + O\left(\int_{2}^{N}|\beta|^{-1}dlog^{-1}(t)\right)\\
&= O(|\beta|^{-1}).
\end{aligned}$$

□

4.2 La Integral Sobre $\mathfrak{M}(a,q)$

Como mencionamos al comienzo de la sección anterior, cada número real $\theta \in \mathfrak{M}$ está contenido en algún intervalo $\mathfrak{M}(a,q)$, donde $\theta = \frac{a}{q} + \beta$ y $|\beta| \leq \frac{log^u(N)}{N}$, de tal forma que

$$\begin{aligned}
I &= \int_{\mathfrak{M}(a,q)} e^{-2\pi iN\theta}S_N^3(\theta)d\theta && (4.4)\\
&= e^{-2\pi iN\frac{a}{q}}\int_{-\frac{\log^u(N)}{N}}^{\frac{\log^u(N)}{N}} e^{-2\pi iN\beta}S_N^3(\frac{a}{q}+\beta)d\beta. && (4.5)
\end{aligned}$$

Lema 4.2.1. *Sea β un número real tal que $|\beta| \leq \frac{log^u(N)}{N}$. Sea c_3 como en el lema 4.1.8 y*

$$J = \int_{-\frac{\log^u(N)}{N}}^{\frac{\log^u(N)}{N}} e^{-2\pi iN\beta}S_N^3(\frac{a}{q}+\beta)d\beta,$$

entonces

$$J = \frac{\mu^3(q)}{\phi^3(q)}T(N) + O\left(q^{-3(1-\epsilon)}\frac{N^2}{log^{2u}(N)} + N^2e^{-c_4\sqrt{log(N)}}\right),$$

donde $0 < c_4 < c_3$ y

$$T(N) = \sum_{\substack{n_1+n_2+n_3=N\\ 2\leq n_1,n_2,n_3\leq N}}\frac{1}{log(n_1)log(n_2)log(n_3)}.$$

Demostración. Del lema 4.1.8 tenemos que

$$J = \int_{-\frac{\log^u(N)}{N}}^{\frac{\log^u(N)}{N}} e^{-2\pi i N\beta} \left[\left(\frac{\mu(q)}{\phi(q)} \sum_{n=2}^{N} \frac{e^{2\pi i n\beta}}{log(n)} \right)^3 + O\Big(N^3 e^{-c_3\sqrt{log(N)}}\Big) \right] d\beta.$$

Sea

$$J_1 = \int_{-\frac{\log^u(N)}{N}}^{\frac{\log^u(N)}{N}} e^{-2\pi i N\beta} \left(\frac{\mu(q)}{\phi(q)} \sum_{n=2}^{N} \frac{e^{2\pi i n\beta}}{log(n)} \right)^3 d\beta.$$

Dado que $log^u(N) = O(N)$ entonces $\frac{log^u(N)}{N} \leq \frac{1}{2}$ para N suficientemente grande; así haciendo uso del lema 4.1.9 tenemos

$$J_1 = \int_{-\frac{1}{2}}^{\frac{1}{2}} e^{-2\pi i N\beta} \left(\frac{\mu(q)}{\phi(q)} \sum_{n=2}^{N} \frac{e^{2\pi i n\beta}}{log(n)} \right)^3 d\beta + O\bigg(\phi^{-3}(q)\Big(\int_{\frac{log^u(N)}{N}}^{\frac{1}{2}} |\beta|^{-3} d\beta\Big)\bigg).$$

Por lo tanto del corolario 2.3.2 y del hecho de que

$$\int_{\frac{log^u(N)}{N}}^{\frac{1}{2}} |\beta|^{-3} d\beta = O\Big(\frac{N^2}{log^{2u}(N)}\Big)$$

obtenemos

$$J_1 = \int_{-\frac{1}{2}}^{\frac{1}{2}} e^{-2\pi i N\beta} \left(\frac{\mu(q)}{\phi(q)} \sum_{n=2}^{N} \frac{e^{2\pi i n\beta}}{log(n)} \right)^3 d\beta + O\Big(q^{-3(1-\epsilon)} \frac{N^2}{log^{2u}(N)}\Big).$$

Por otro lado si

$$H = \int_{-\frac{1}{2}}^{\frac{1}{2}} e^{-2\pi i N\beta} \left(\frac{\mu(q)}{\phi(q)} \sum_{n=2}^{N} \frac{e^{2\pi i n\beta}}{log(n)} \right)^3 d\beta$$

tenemos

$$\begin{aligned}
H &= \frac{\mu^3(q)}{\phi^3(q)} \int_{-\frac{1}{2}}^{\frac{1}{2}} e^{-2\pi i N\beta} \Big(\sum_{n=2}^{N} \frac{e^{2\pi i n\beta}}{log(n)} \Big)^3 d\beta \\
&= \frac{\mu^3(q)}{\phi^3(q)} \int_{-\frac{1}{2}}^{\frac{1}{2}} e^{-2\pi i N\beta} \sum_{n_1=2}^{N} \sum_{n_2=2}^{N} \sum_{n_3=2}^{N} \frac{e^{2\pi i(n_1+n_2+n_3)\beta}}{log(n_1)log(n_2)log(n_3)} d\beta \\
&= \frac{\mu^3(q)}{\phi^3(q)} \int_{-\frac{1}{2}}^{\frac{1}{2}} \sum_{n_1,n_2,n_3=1}^{N} \frac{e^{2\pi i\beta(n_1+n_2+n_3-N)}}{log(n_1)log(n_2)log(n_3)} d\beta \\
&= \frac{\mu^3(q)}{\phi^3(q)} \sum_{n_1,n_2,n_3=1}^{N} \frac{1}{log(n_1)log(n_2)log(n_3)} \int_{-\frac{1}{2}}^{\frac{1}{2}} e^{2\pi i\beta(n_1+n_2+n_3-N)} d\beta \\
&= \frac{\mu^3(q)}{\phi^3(q)} \sum_{n_1+n_2+n_3=N} \frac{1}{log(n_1)log(n_2)log(n_3)} \\
&= \frac{\mu^3(q)}{\phi^3(q)} T(N).
\end{aligned}$$

Por lo tanto

$$J_1 = \frac{\mu^3(q)}{\phi^3(q)} T(N) + O\Big(q^{-3(1-\epsilon)} \frac{N^2}{log^{2u}(N)} \Big).$$

Si

$$J_2 = \int_{-\frac{\log^u(N)}{N}}^{\frac{\log^u(N)}{N}} e^{-2\pi i N\beta} O\Big(N^3 e^{-c_3\sqrt{log(N)}} \Big) d\beta,$$

entonces

$$\begin{aligned}
J_2 &= O\Big(\frac{log^u(N)}{N} N^3 e^{-c_3\sqrt{log(N)}} \Big) \\
&= O\Big(N^2 e^{-c_3\sqrt{log(N)}} log^u(N) \Big) \\
&= O\Big(N^2 e^{-c_4\sqrt{log(N)}} \Big),
\end{aligned}$$

donde $0 < c_4 < c_3$. Por lo tanto $J = J_1 + J_2$, esto es

$$\begin{aligned}
J &= \frac{\mu^3(q)}{\phi^3(q)} T(N) + O\Big(q^{-3(1-\epsilon)} \frac{N^2}{log^{2u}(N)} \Big) + O\Big(N^2 e^{-c_4\sqrt{log(N)}} \Big) \\
&= \frac{\mu^3(q)}{\phi^3(q)} T(N) + O\Big(q^{-3(1-\epsilon)} \frac{N^2}{log^{2u}(N)} + N^2 e^{-c_4\sqrt{log(N)}} \Big)
\end{aligned}$$

como queríamos probar. $\square$

4.3 La parte principal $M(N)$

Vale la pena detenernos en este punto y hacer una breve reseña de lo que hemos logrado hasta este momento. En el capítulo 3 obtuvimos la siguiente equivalencia para el número de representaciones de un natural como suma de tres primos:

$$r(N) = \int_0^1 e^{-2\pi i N\theta} S_N^3(\theta) d\theta.$$

Posteriormente en ese mismo capítulo descompusimos el intervalo $[0,1]$ según el método de Hardy-Littlewood como sigue:

$$r(N) = \underbrace{\int_{\mathfrak{M}} e^{-2\pi i N\theta} S_N^3(\theta) d\theta}_{M(N)} + \underbrace{\int_{\mathfrak{m}} e^{-2\pi i N\theta} S_N^3(\theta) d\theta}_{E(N)}.$$

En vista del lema 3.2.2 y con el objetivo de estimar la integral $M(N)$, en este capítulo abordamos el problema de estimar la integral

$$I = \int_{\mathfrak{M}(a,q)} e^{-2\pi i N\theta} S_N^3(\theta) d\theta,$$

para después considerar la integral sobre la unión de los intervalos $\mathfrak{M}(a,q)$. Del lema 4.2.1 tenemos la siguiente relación para la integral sobre $\mathfrak{M}(a,q)$.

$$I = e^{-2\pi i N\frac{a}{q}} \left(\frac{\mu^3(q)}{\phi^3(q)} T(N) + O\Big(q^{-\frac{5}{2}} \frac{N^2}{log^{2u}(N)} + N^2 e^{-c_4\sqrt{log(N)}} \Big) \right)$$

de tal modo que la integral sobre la unión de los intervalos $\mathfrak{M}(a,q)$; es decir $M(N)$, se puede escribir como $M(N) = M_1(N) + M_2(N)$, donde

$$\begin{aligned} M_1(N) &= \sum_{q=1}^{log^u(N)} \sum_{\substack{a=1\\(a,q)=1}}^{q-1} e^{-2\pi i N\frac{a}{q}} \left(\frac{\mu^3(q)}{\phi^3(q)} T(N) \right) \\ M_2(N) &= \sum_{q=1}^{log^u(N)} \sum_{\substack{a=1\\(a,q)=1}}^{q-1} e^{-2\pi i N\frac{a}{q}} O\Big(q^{-3(1-\epsilon)} \frac{N^2}{log^{2u}(N)} + N^2 e^{-c_4\sqrt{log(N)}} \Big). \end{aligned}$$

4.4 Estimación de $M(N)$

En esta sección abordaremos el problema de estimar las sumas $M_1(N)$ y $M_2(N)$. Esto nos conducirá de manera natural a obtener una buena estimación de la integral 4.3 en la que estamos interesados.

4.4.1 Estimación de $M_2(N)$

La estimación de la suma $M_2(N)$ se sigue de un cálculo directo. El lema A.2.3, el corolario 2.3.2 y los siguientes hechos son pertinentes:

$$\Big|\sum_{\substack{a=1\\(a,q)=1}}^{q-1} e^{-2\pi i N\frac{a}{q}}\Big| \leq \phi(q) \leq q \leq log^u(N).$$

Lema 4.4.2. *Sea $M_2(N)$ como en la sección 4.3. Entonces*

$$M_2(N) = O\bigg(\frac{N^2}{log^{2u}(N)}\bigg).$$

Demostración. Existen $0 < c_5 < c_4$ tales que

$$\begin{aligned}
M_2(N) &= O\bigg(\sum_{q=1}^{log^u(N)} \phi(q)q^{-\frac{5}{2}}\frac{N^2}{log^{2u}(N)} + \phi(q)N^2e^{-c_4\sqrt{log(N)}}\bigg)\\
&= O\bigg(\sum_{q=1}^{log^u(N)} q^{-\frac{3}{2}}\frac{N^2}{log^{2u}(N)} + log^u(N)N^2e^{-c_4\sqrt{log(N)}}\bigg)\\
&= O\bigg(\sum_{q=1}^{\infty} q^{-\frac{3}{2}}\frac{N^2}{log^{2u}(N)} + N^2e^{-c_5\sqrt{log(N)}}\bigg)\\
&= O\bigg(\frac{N^2}{log^{2u}(N)} + N^2e^{-c_5\sqrt{log(N)}}\bigg)\\
&= O\bigg(\frac{N^2}{log^{2u}(N)}\bigg).
\end{aligned}$$

□

4.4.3 Estimación de $M_1(N)$

La suma $M_1(N)$ puede reescribirse como:

$$M_1(N) = A(N)T(N), \quad \text{con} \quad A(N) = \sum_{q=1}^{log^u(N)} \left(c_q(N) \frac{\mu^3(q)}{\phi^3(q)} \right), \qquad (4.6)$$

donde $c_q(N)$ es la suma de Ramanujan definida en la sección 2.2 del capítulo 3. En los lemas 4.4.4 y 4.4.5 estimaremos $T(N)$ y $A(N)$ respectivamente.

Lema 4.4.4. *Sea $T(N)$ como se definió en el lema 4.2.1, entonces existen dos constantes positivas A y B tales que*

$$\frac{AN^2}{log^3(N)} \leq T(N) \leq \frac{BN^2}{log^3(N)}.$$

Demostración. Tenemos la siguiente relación

$$T(N) = \sum_{\substack{\sqrt{N} \leq n_1, n_2, n_3 \leq N \\ N = n_1 + n_2 + n_3}} \frac{1}{log(n_1)log(n_2)log(n_3)} \; + \; O\Big(T'(N)\Big),$$

donde

$$T'(N) = \sum_{\substack{n_1 \leq \sqrt{N},\, 2 \leq n_2, n_3 \leq N \\ N = n_1 + n_2 + n_3}} \frac{1}{log(n_1)log(n_2)log(n_3)}.$$

$T'(N)$ se puede estimar como sigue:

$$\begin{aligned} T'(N) \;&\leq\; C \sum_{\substack{n_1 \leq \sqrt{N},\, 2 \leq n_2, n_3 \leq N \\ N = n_1 + n_2 + n_3}} 1 \leq \sum_{n_1=1}^{\sqrt{N}} \sum_{n_2=1}^{N-n_1} 1 \\ &\leq\; \sum_{n_1=1}^{\sqrt{N}} \Big(N - n_1\Big) \leq \sum_{n_1=1}^{\sqrt{N}} N = O(N^{\frac{3}{2}}). \end{aligned}$$

Por otro lado, si $\sqrt{N} \leq n_j \leq N$, para $j = 1, 2, 3$, entonces $log^{-1}(n_j) \leq$

$log^{-1}(\sqrt{N})$ y en consecuencia

$$\begin{aligned} \sum_{\substack{\sqrt{N}\leq n_1,n_2,n_3\leq N \\ N=n_1+n_2+n_3}} \frac{1}{log(n_1)log(n_2)log(n_3)} &\leq log^{-3}(\sqrt{N}) \sum_{\substack{\sqrt{N}\leq n_1,n_2,n_3\leq N \\ N=n_1+n_2+n_3}} 1 \\ &\leq log^{-3}(\sqrt{N}) \sum_{n_1+n_2+n_3=N} 1, \end{aligned}$$

donde

$$\sum_{n_1+n_2+n_3=N} 1 = \sum_{n_1=1}^{N} \sum_{n_2=1}^{N-n_1} 1 = \sum_{n_1=1}^{N} \Big(N - n_1\Big) = \frac{N^2}{2} + O(N) = O(N^2). \quad (4.7)$$

Por lo tanto

$$T(N) = O\Big(N^2 log^{-3}(\sqrt{N}) + N^{\frac{3}{2}}\Big)$$

Como $log^3(\sqrt{N}) \leq \sqrt{N}$ para N suficientemente grande, tenemos

$$N^{\frac{3}{2}} \leq \frac{N^2}{log^3(\sqrt{N})} = O\Big(\frac{N^2}{log^3(N)}\Big)$$

con lo cual

$$T(N) \leq \frac{BN^2}{log^3(N)}.$$

Por otro lado, ya que

$$T(N) = \sum_{\substack{2\leq n_1,n_2,n_3\leq N \\ n_1+n_2+n_3=N}} \frac{1}{log(n_1)log(n_2)log(n_3)},$$

tenemos de manera trivial que

$$T(N) \geq \frac{1}{log^3(N)} \overbrace{\sum_{\substack{2\leq n_1,n_2,n_3\leq N \\ n_1+n_2+n_3=N}} 1}^{T''(N)}, \quad (4.8)$$

pero

$$T''(N) = \sum_{n_1=2}^{N} \sum_{n_2=2}^{N-n_1} 1 = \sum_{n_1=2}^{N} \Big(N - n_1 - 1\Big) = \frac{N^2 - 5N}{2}.$$

Por lo anterior se tiene que

$$\lim_{N\to\infty} \frac{T''(N)}{N^2} = \frac{1}{2},$$

de tal modo, que para todo $\epsilon > 0$ existe M tal que para cualquier $N > M$ tenemos

$$\Big|\frac{T''(N)}{N^2} - \frac{1}{2}\Big| < \epsilon.$$

Por lo tanto

$$-\epsilon < \frac{T''(N)}{N^2} - \frac{1}{2} < \epsilon,$$

y en consecuencia

$$\Big(\frac{1}{2} - \epsilon\Big)N^2 < T''(N) < \Big(\epsilon + \frac{1}{2}\Big)N^2.$$

Haciendo $\epsilon < \frac{1}{2}$, tenemos que existe una constante positiva A, tal que

$$T''(N) > AN^2.$$

Finalmente de la ecuación 4.8, obtenemos

$$T(N) \geq \frac{AN^2}{log^3(N)}.$$

□

Lema 4.4.5. *Sea $A(N)$ como en la ecuación 4.6, entonces*

$$A(N) = \mathfrak{G}(N) + O(log^{-u(1-\epsilon)}(N)),$$

donde

$$\mathfrak{G}(N) = \prod_{p\nmid N}\Big(1 + \frac{1}{(p-1)^3}\Big)\prod_{p|N}\Big(1 - \frac{1}{(p-1)^2}\Big).$$

Demostración. Definimos $\mathfrak{G}(N)$, la serie singular del problema ternario de Goldbach como sigue:

$$\mathfrak{G}(N) = \sum_{q=1}^{\infty} c_q(N)\frac{\mu(q)}{\phi^3(q)}.$$

Entonces, del corolario 2.3.2 y del hecho de que $|c_q(N)| \leq \phi(q)$, tenemos

$$\Big|A(N) - \mathfrak{S}(N)\Big| \leq \sum_{q > log^u(N)} \frac{1}{\phi^2(q)} \leq \sum_{q > log^u(N)} \frac{1}{q^{2-\epsilon}} = O\Big(log^{-u(1-\epsilon)}(N)\Big).$$

Por lo tanto

$$A(N) = \mathfrak{S}(N) + O(log^{-u(1-\epsilon)}(N)).$$

Por otro lado, como μ, ϕ y la suma de Ramanujan c_q, son funciones multiplicativas de q, se tiene que la función aritmética $G(q) = \frac{\mu(q)c_q(N)}{\phi^3(q)}$ es multiplicativa. $\mathfrak{S}$ converge absolutamente puesto que

$$\Big|\frac{\mu(q)c_q(N)}{\phi^3(q)}\Big| \leq \frac{1}{\phi^2(q)} \leq \frac{1}{q^{2-\epsilon}}.$$

En consecuencia del lema A.3.7 $\mathfrak{S}$ tiene una representación como producto de Euler como sigue:

$$\begin{aligned} \mathfrak{S}(N) &= \prod_p \Big(1 + \sum_{i=1}^{\infty} \frac{\mu(p^i)c_{p^i}(N)}{\phi^3(p^i)}\Big) \\ &= \prod_p \Big(1 - \frac{c_p(N)}{\phi^3(p)}\Big). \end{aligned}$$

Esta última igualdad se cumple puesto que $\mu(p^i) = 0$ para $i \geq 2$.
Para finalizar, observemos que

$$c_p(N) = \begin{cases} p-1 & \text{Si } p \mid N \\ -1 & \text{Si } p \nmid N \end{cases}$$

de tal forma que

$$\mathfrak{S}(N) = \prod_{p \nmid N} \Big(1 + \frac{1}{(p-1)^3}\Big) \prod_{p \mid N} \Big(1 - \frac{1}{(p-1)^2}\Big).$$

□

Lema 4.4.6. *Sea $\mathfrak{G}$ como en el lema anterior, entonces*

1. *Si N es par $\mathfrak{G}(N) = 0$.*

2. *Si N es impar $\mathfrak{G}(N) > 1$.*

Demostración. Si N es par, entonces 2 está en la descomposición en factores primos de N y $1 - \frac{1}{(2-1)^2} = 0$, por lo tanto $\mathfrak{G}(N) = 0$. Si por el contrario N es impar, entonces $2 \nmid N$ y en consecuencia

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

Por otro lado, ya que $0 < 1 - \frac{1}{(p-1)^2} < 1$ para cualquier primo $p > 2$, tenemos

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

y como $p_n \leq p_{n+1} - 1$ donde p_n es el enésimo primo, tenemos

$$\prod_{2<p<\infty} \left(1 - \frac{1}{(p-1)^2}\right) \geq \prod_{2\leq p<\infty} \left(1 - \frac{1}{(p)^2}\right) > \prod_{n=2}^{\infty} \left(1 - \frac{1}{(n)^2}\right).$$

donde

$$\prod_{n=2}^{\infty} \left(1 - \frac{1}{(n)^2}\right) = \lim_{N\to\infty} \prod_{n=2}^{N} \left(1 - \frac{1}{(n)^2}\right) = \lim_{N\to\infty} \left(1 - \frac{N+1}{2N}\right) = \frac{1}{2}.$$

por lo tanto si N es impar

$$\mathfrak{G}(N) > 1.$$

□

Finalmente como consecuencia inmediata de los lemas 4.4.2, 4.4.4, 4.4.5 y 4.4.6 podemos estimar $M(N)$.

Teorema 4.4.7. *Sea*

$$M(N) = \int_{\mathfrak{M}} e^{-2\pi i N\theta} S_N^3(\theta) d\theta.$$

Entonces existe una constante positiva C y un natural N_0 tal que si N es impar y $N > N_0$ se cumple

$$|M(N)| \geq C \frac{N^2}{log^3(N)}.$$

Demostración. En la sección 4.3 vimos que

$$M(N) = M_1(N) + M_2(N). \tag{4.9}$$

Posteriormente en la sección 4.4 vimos que $M_2(N) = O\Big(\frac{N^2}{log^{2u}(N)}\Big)$ y que $M_1(N) = T(N)A(N)$, donde

$$\begin{aligned} T(N) &= \sum_{\substack{2 \leq n_1, n_2, n_3 \leq N \\ n_1+n_2+n_3=N}} \frac{1}{log(n_1)log(n_2)log(n_3)} \quad \text{y} \\ A(N) &= \mathfrak{G}(N) + O\Big(log^{-u(1-\epsilon)}(N)\Big), \quad \text{con } \mathfrak{G}(N) > 1. \end{aligned}$$

De este modo

$$M(N) = T(N)A(N) + O\Big(\frac{N^2}{log^{2u}(N)}\Big).$$

Por un lado tenemos $|A(N) - \mathfrak{G}(N)| \leq Clog^{-u(1-\epsilon)}(N)$, de tal manera que $|\mathfrak{G}(N)| - |A(N)| \leq Clog^{-u(1-\epsilon)}(N)$ y por lo tanto

$$1 < |\mathfrak{G}(N)| \leq Clog^{-u(1-\epsilon)}(N) + |A(N)|.$$

En consecuencia, para N suficientemente grande tenemos que

$$Clog^{-u(1-\epsilon)}(N) \leq \frac{1}{2},$$

de tal modo que $|A(N)| > \frac{1}{2}$. Por lo anterior y el lema 4.4.4 tenemos

$$|T(N)A(N)| \geq C_1 \frac{N^2}{log^3(N)}.$$

Ahora, por otro lado tenemos $|M(N) - T(N)A(N)| \leq C_2 \frac{N^2}{log^{2u}(N)}$ y en consecuencia $|T(N)A(N)| - |M(N)| \leq C_2 \frac{N^2}{log^{2u}(N)}$ de tal manera que

$$C_1 \frac{N^2}{log^3(N)} - C_2 \frac{N^2}{log^{2u}(N)} \leq |M(N)|.$$

Por lo tanto, si $u > \frac{3}{2}$ y N es suficientemente grande tenemos

$$|M(N)| \geq C_3 \frac{N^2}{log^3(N)}.$$

$\square$

Capítulo 5

La Integral Sobre los Arcos Menores

El resultado principal de este capítulo tiene que ver esencialmente con el método de sumas exponenciales de I. M. Vinogradov [6]. La integral

$$E(N) = \int_{\mathfrak{m}} e^{-2\pi i N\theta} S_N^3(\theta) d\theta$$

puede ser acotada trivialmente como sigue:

$$\begin{aligned}
|E(N)| &\leq \sup_{\theta\in\mathfrak{m}} |S_N(\theta)| \int_0^1 |S_N(\theta)|^2 d\theta \\
&= \sup_{\theta\in\mathfrak{m}} |S_N(\theta)| \sum_{p_1,p_2\leq N} \int_0^1 e^{2\pi i(p_1-p_2)\theta} d\theta \\
&= \sup_{\theta\in\mathfrak{m}} |S_N(\theta)| \Big\{ \sum_{p_1=p_2\leq N} \int_0^1 e^{2\pi i(p_1-p_2)\theta} d\theta + \sum_{p_1\neq p_2\leq N} \int_0^1 e^{2\pi i(p_1-p_2)\theta} d\theta \Big\} \\
&= \sup_{\theta\in\mathfrak{m}} |S_N(\theta)| \Big\{ \pi(N) + 0 \Big\}.
\end{aligned}$$

Por lo tanto, del teorema 2.7.1 tenemos

$$E(N) = O\Big(\sup_{\theta\in\mathfrak{m}} |S_N(\theta)| \frac{N}{\log(N)} \Big).$$

Si logramos probar que $\sup_{\theta\in\mathfrak{m}}|S_N(\theta)| = O\left(\frac{N}{log^3(N)}\right)$ tendríamos que

$$|r(N) - M(N)| \leq C\frac{N^2}{log^4(N)},$$

por lo tanto $|M(N)| - |r(N)| \leq C\frac{N^2}{log^4(N)}$ y en consecuencia del teorema 4.4.7, tendríamos que

$$r(N) \geq C'\frac{N^2}{log^3(N)}$$

con lo cual quedaría demostrado el teorema de Vinogradov 1.0.3 junto con el respectivo corolario 1.0.4.

5.1 Estimación de $S_N(\theta)$ en los Arcos Menores

Para estimar $S_N(\theta)$ en $\mathfrak{m}$ utilizaremos el lema 2.6.2 haciendo $Q = \frac{N}{log^u(N)}$. De este modo para $\theta \in \mathfrak{m}$ existen dos enteros positivos a y q tales que $(a, q) = 1$, $log^u(N) \leq q \leq Q = \frac{N}{log^u(N)}$ y

$$\left|\theta - \frac{a}{q}\right| \leq \frac{log^u(N)}{qN},$$

donde esta última desigualdad puede ser reemplazada por

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

ya que $q \leq \frac{N}{log^u(N)}$. En consecuencia cualquier $\theta \in \mathfrak{m}$ se puede escribir como sigue:

$$\theta = \frac{a}{q} + \frac{\epsilon}{q^2} \qquad \text{donde} \qquad |\epsilon| \leq 1. \tag{5.1}$$

Los lemas 5.1.1, 5.1.2 y 5.1.3 que presentamos a continuación serán utilizados de manera crucial en lo que resta del capítulo.

Lema 5.1.1. *Sea*

$$\Phi(z) = \frac{az + \psi(z)}{q},$$

con $(a, q) = 1$. *Sean* g *y* q' *enteros con* $0 < q' \leq q$. *Si* z *toma los valores* g, $g+1, \ldots g+q'-1$ *y si para estos valores de* z *la función* $\psi(z)$ *toma valores reales, de tal forma que*

$$\lambda = \max_{g \leq z < g+q'} \psi(z) - \min_{g \leq z < g+q'} \psi(z) > 0, \tag{5.2}$$

entonces para $U \geq 1$

$$\sum_{z=g}^{g+q'} min\left(U, \frac{1}{2||\Phi(z)||}\right) \leq (\lambda+3)U + qlog(q).$$

Demostración. Haciendo $z = g + z'$ donde $z' = 0, 1, \ldots, q'-1$, tenemos

$$||\Phi(z)|| = \left|\left|\frac{az' + \psi_1(z')}{q}\right|\right|$$

con $\psi_1(z') = ag + \psi(g+z')$. En vista de 5.2 podemos encontrar un número real B tal que

$$B \leq \psi_1(z') \leq B + \lambda, \tag{5.3}$$

para $z' = 0, 1, \ldots, q'-1$. Si $B_1 = B - [B]$ y denotamos con $z'' = z''(z)$ al mínimo residuo no negativo de $az + [B]$ módulo q tenemos,

$$az' + \psi_1(z') = az' + [B] + (B - [B]) + \psi_1(z') - B = z'' + b(z')q + \psi_2(z'')$$

donde $b(z')$ es un entero y $\psi_2(z'') = B_1 + (\psi_1(z') - B)$ de tal modo que restando $[B]$ de la ecuación (5.3) tenemos

$$B_1 \leq \psi_2(z'') \leq B_1 + \lambda. \tag{5.4}$$

En consecuencia

$$||\Phi(z)|| = \left|\left|\frac{z'' + \psi_2(z'')}{q}\right|\right|.$$

Si $q \leq \lambda + 3$ el resultado se sigue trivialmente puesto que

$$\sum_{z=g}^{g+q'} min\left(U, \frac{1}{2||\Phi(z)||}\right) \leq qU.$$

Por lo tanto podemos suponer que $\lambda < q-3$. Los valores de z'' son algunos o todos los números $0, 1, \ldots, q-1$. Sea $q_0 = [B_1 + \lambda + 1]$. Ya que $q > \lambda + 3$ tenemos que $0 < q_0 < q$ y además de la ecuación 5.4

$$0 \leq \psi_2(z'') < q_0, \tag{5.5}$$

para cada valor de z''. Para los valores de z para los cuales

$$z'' = 0,\ q - q_0, \ldots, q-1,$$

tomamos el término U involucrado en la suma y como tenemos a lo más q_0+1 valores de estos y $q_0 + 1 \leq \lambda + 3$ obtenemos.

$$\sum_{z''(z)=0,\, q-q_0, \ldots,\, q-1} min\left(U, \frac{1}{2||\Phi(z)||}\right) \leq (\lambda+3)U.$$

Para $1 \leq z'' = z''(z) < q - q_0$ tenemos

$$1 \leq z'' + \psi_2(z'') < (q-q_0) + q_0 = q.$$

Entonces

$$||\Phi(z)|| = \left|\left|\frac{z'' + \psi_2(z'')}{q}\right|\right| \geq \frac{z_1(z)}{q},$$

donde (ver ecuación 5.5)

$$z_1(z) = \begin{cases} z'' & z'' + \psi_2(z'') < \frac{q}{2}, \\ q - q_0 - z'' & z'' + \psi_2(z'') \geq \frac{q}{2}, \end{cases}$$

y cada valor de $z_1(z)$ se repite a lo más para dos valores de z''. Finalmente tomamos

$$\sum_{1 \leq z''(z) \leq q-q_0} min\Big(U, \frac{1}{2||\Phi(z)||}\Big) \leq 2 \sum_{1 \leq z_1 \leq \frac{q}{2}} \frac{q}{2z_1} \leq 2q \int_1^{\frac{q}{2}} \frac{dt}{2t} = O\Big(qlog(q)\Big)$$

y el resultado se sigue inmediatamente. $\square$

Lema 5.1.2. *Sean* $2 \leq q \leq W$, $1 < W_0 \leq W$ *y*

$$\theta = \frac{a}{q} + \frac{\epsilon}{q^2} \qquad \textit{donde} \qquad (a,q) = 1 \quad y \quad |\epsilon| \leq 1.$$

Si

$$S = \sum_{1 < z \leq W_0} min\Big(\frac{W}{z}, \frac{1}{2||z\theta||}\Big),$$

entonces

$$S = O\bigg(log(W)\Big(W_0 + q + \frac{W}{q}\Big)\bigg).$$

Demostración. Dividimos la suma S como sigue:

$$S = \sum_{1 \leq z \leq \frac{q}{2}} + \sum_{\frac{q}{2} < z \leq \frac{3q}{2}} + \cdots + \sum_{(j_0 - \frac{1}{2})q < z \leq W_0},$$

donde $(j_0 - \frac{1}{2})q < W_0 \leq (j_0 + \frac{1}{2})q$. Para los valores de z en el primer sumando, sea z'' el mínimo residuo no negativo de az módulo q. Ya que

$$z\theta = \frac{1}{q}\Big[az + \frac{z\epsilon}{q}\Big] \quad \text{y} \quad 0 < z \leq \frac{q}{2}$$

tenemos

$$z\theta = \frac{1}{q}\Big(az + \frac{z\epsilon}{q}\Big) = \frac{1}{q}\Big(z'' + bq + \frac{z\epsilon}{q}\Big) = b + \frac{1}{q}\Big(z'' + \frac{z\epsilon}{q}\Big),$$

entonces

$$||z\theta|| = \bigg|\bigg|\frac{1}{q}\Big[z'' + \frac{z\epsilon}{q}\Big]\bigg|\bigg| \geq \frac{1}{q}\Big(z_1 - \frac{1}{2}\Big),$$

donde

$$z_1(z) = \begin{cases} z'' & z'' \leq \frac{q}{2}, \\ q - z'' & z'' > \frac{q}{2}, \end{cases}$$

de tal modo que el primer sumando no excede

$$\frac{q}{2} \sum_{1 \leq z \leq \frac{q}{2}} \frac{1}{z_1 - \frac{1}{2}} \leq \frac{q}{2} \int_1^{\frac{q}{2}} \frac{dt}{t - \frac{1}{2}} = O(qlog(q)).$$

Por otro lado, los demás sumandos los podemos estimar haciendo uso del lema 5.1.1. Cada una de estas sumas es del tipo considerado ahí, con $\lambda = 1$, $\psi(z) = \frac{1}{q^2}(z\epsilon)$ y $U = \frac{W}{(j-\frac{1}{2})q}$, donde $j = 1, 2, \ldots, j_0$. Por lo tanto cada una de estas sumas no excede $qlog(q) + \frac{4W}{(j-\frac{1}{2})q}$. En consecuencia

$$\begin{aligned}
S &= O\Big(qlog(q) + \sum_{j=1}^{j_0}\Big(qlog(q) + \frac{4W}{(j-\frac{1}{2})q}\Big)\Big) \\
&= O\Big((q + j_0 q)log(q) + \frac{4W}{q}\Big(\sum_{j=1}^{j_0}\frac{1}{(j-\frac{1}{2})}\Big)\Big) \\
&= O\Big((q + j_0 q)log(q) + \frac{4W}{q}log(j_0)\Big) \\
&= O\Big(\Big(q + \Big(\frac{W_0}{q} + 1\Big)q\Big)log(q) + \frac{4W}{q}log\Big(\frac{W_0}{q} + 1\Big)\Big) \\
&= O\Big(\Big(q + W_0\Big)\Big)log(W) + \frac{4W}{q}log\Big(\frac{W_0}{q} + 1\Big)\Big) \\
&= O\Big(\Big(q + W_0 + \frac{W}{q}\Big)log(W)\Big).
\end{aligned}$$

□

Lema 5.1.3. *Sean U_1, U_2 y V tres sucesiones de números naturales. Sea*

$$1 < U < N \qquad U < U' = KU,$$

donde K es una constante mayor que 1. Sea $\theta \in \mathbb{R}$ tal que

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

Sea también la suma

$$S = \sum_{U<n<U'}\sum_{v\leq\frac{N}{n}} e^{2\pi i n v\theta}, \qquad \Big(N \geq 2\Big)$$

donde $v \in V$, las n son de la forma $n = u_1u_2$ con $u_1 \in U_1$ y $u_2 \in U_2$ y cada n se cuenta dependiendo del número de veces que $n = u_1u_2$. Entonces

$$S = O\Big(Nlog^2(N)\Big(\frac{1}{q} + \frac{q}{N} + \frac{1}{U} + \frac{U}{N}\Big)^{\frac{1}{2}}\Big).$$

Demostración. De la desigualdad de Cauchy-Schwarz tenemos

$$S^2 = O\Big(\sum_{U<n\leq U'} d_1^2(n) \sum_{U<n\leq U'} \Big|\sum_{v\leq \frac{N}{n}} e^{2\pi i n v\theta}\Big|^2\Big),$$

donde

$$d_1(n) = \sum_{n=u_1u_2} 1.$$

Es claro que $0 \leq d_1(n) \leq d(n)$, así que de la parte 3 del lema 2.4.3 tenemos

$$\begin{aligned} S^2 &= O\Big(Ulog^3(U) \sum_{U<n\leq U'} \sum_{v\leq \frac{N}{n}} \sum_{v'\leq \frac{N}{n}} e^{2\pi i n(v-v')\theta}\Big) \\ &= O\Big(Ulog^3(U) \sum_{U<n\leq U'} \sum_{v\leq \frac{N}{U}} \sum_{v'\leq \frac{N}{U}} e^{2\pi i n(v-v')\theta}\Big) \\ &= O\Big(Ulog^3(U) \sum_{v\leq \frac{N}{U}} \sum_{v'\leq \frac{N}{U}} \sum_{U<n\leq U'} e^{2\pi i n(v-v')\theta}\Big). \end{aligned}$$

Del lema 2.5.4 tenemos

$$\sum_{U<n\leq U'} e^{2\pi i n(v-v')\theta} = O\Big(min\Big(U, \frac{1}{||(v-v')\theta||}\Big)\Big).$$

Por lo tanto

$$S^2 = O\Big(Ulog^3(U) \sum_{v\leq \frac{N}{U}} \sum_{v'\leq \frac{N}{U}} min\Big(U, \frac{1}{||(v-v')\theta||}\Big)\Big).$$

Fijemos ahora v y sumemos sobre v', para esto dividimos el intervalo $[1, \frac{N}{U}]$ en bloques de longitud q. De esta forma obtendremos a lo más $\frac{N}{qU}+1$ bloques y la suma sobre cada uno de estos bloques es del tipo que consideramos en el lema 5.1.1, por lo tanto

$$\begin{aligned} S^2 &= O\Big(Ulog^3(U)\sum_{v\leq \frac{N}{U}}\Big(\frac{N}{qU}+1\Big)\Big(U+qlog(q)\Big)\Big) \\ &= O\Big(Nlog^3(N)\Big(\frac{N}{qU}+1\Big)\Big(U+qlog(q)\Big)\Big) \\ &= O\Big(Nlog^3(N)\Big(U+qlog(q)+\frac{N}{q}+\frac{Nlog(q)}{U}\Big)\Big) \\ &= O\Big(N^2log^4(N)\Big(\frac{U}{N}+\frac{q}{N}+\frac{1}{q}+\frac{1}{U}\Big)\Big) \end{aligned}$$

□

Los lemas que hemos presentado anteriormente han dejado listo el camino para abordar el problema principal de este capítulo: probar que para $\theta \in \mathfrak{m}$, $S_N(\theta) = O\Big(\frac{N}{log^3(N)}\Big)$. Recordemos que $S_N(\theta) = \sum_{p\leq N} e^{2\pi i p\theta}$.

Lema 5.1.4. *Sea* $P_{\sqrt{N}} = \prod_{p\leq\sqrt{N}} p$, *entonces*

$$S_N(\theta) = O(\sqrt{N}) + \sum_{\substack{n=1 \\ (n,P_{\sqrt{N}})=1}}^{N} e^{2\pi i p\theta}.$$

Demostración. Tenemos

$$S_N(\theta) = \underbrace{\sum_{2\leq p\leq\sqrt{N}} e^{2\pi i p\theta}}_{S_1} + \underbrace{\sum_{\sqrt{N}<p\leq N} e^{2\pi i p\theta}}_{S_2}.$$

Claramente tenemos que $S_1 = O(\sqrt{N})$, mientras que

$$S_2 = \sum_{\substack{n=\sqrt{N}+1 \\ (n,P_{\sqrt{N}})=1}}^{N} e^{2\pi i p\theta} = O(\sqrt{N}) + \sum_{\substack{n=1 \\ (n,P_{\sqrt{N}})=1}}^{N} e^{2\pi i p\theta},$$

y esta misma relación se cumple para $S_N(\theta)$ de manera trivial. □

Como consecuencia directa de este resultado y del lema 2.2.4 podemos reescribir $S_N(\theta)$ como sigue:

Sea $n = md$, entonces

$$S_N(\theta) = O(\sqrt{N}) + \sum_{d|P_N} \mu(d) \sum_{m=1}^{\frac{N}{d}} e^{2\pi imd\theta},$$

donde la suma en el lado derecho de la igualdad anterior, puede ser estimada dividiendo el intervalo $0 \leq m \leq N$ en $O(log(N))$ bloques de la forma:

$$M < m \leq M', \qquad \text{donde} \qquad M < M' \leq 2M.$$

Así obtenemos $O(log(N))$ sumas del tipo:

$$S(M) = \sum_{d|P_N} \mu(d) \sum_{\substack{M<m\leq M' \\ 1\leq m\leq \frac{N}{d}}} e^{2\pi imd\theta}.$$

Necesitamos estimar entonces $S(M)$ y para esto consideraremos los siguientes dos casos:

1. Cuando $M \geq e^{\frac{1}{2}\sqrt{log(N)}}$
2. Cuando $M < e^{\frac{1}{2}\sqrt{log(N)}}$

5.1.5 Caso 1

Como veremos a continuación, este caso quedará resuelto utilizando el lema 5.1.6 y aplicando los resultados del lema 5.1.2, con $W = N$ y $W_0 = \frac{N}{e^{\sqrt{log(N)}}}$.

Lema 5.1.6. *Sea*

$$S(M) = \sum_{d|P_N} \mu(d) \sum_{\substack{M<m\leq M' \\ 1\leq m\leq \frac{N}{d}}} e^{2\pi imd\theta},$$

entonces

$$S(M) = O\Bigg(\sum_{d=1}^{\frac{N}{M}} min\Big\{\frac{N}{d}, \frac{1}{2||d\theta||}\Big\}\Bigg).$$

Demostración. Ya que $d \leq \frac{N}{M}$ tenemos,

$$|S(M)| \leq \sum_{d=1}^{\frac{N}{M}} \Big| \sum_{m=1}^{\frac{N}{d}} e^{2\pi i m d\theta} \Big|.$$

Si $\theta \in \mathbb{Z}$, podemos estimar la suma dentro de las barras de manera trivial haciendo uso de que $|e^{2\pi i m d\theta}| = 1$ obteniendo

$$\Big| \sum_{m=1}^{\frac{N}{d}} e^{2\pi i m d\theta} \Big| \leq \frac{N}{d}.$$

Sin embargo si $\theta \notin \mathbb{Z}$ podemos estimarla como en el lema 2.5.4 obteniendo así,

$$\Big| \sum_{m=1}^{\frac{N}{d}} e^{2\pi i m d\theta} \Big| \leq \frac{1}{2||d\theta||}$$

Con lo cual el lema queda demostrado. □

Teorema 5.1.7. *Sea $\theta \in \mathfrak{m}$, $M \geq e^{\frac{1}{2}\sqrt{log(N)}}$ y $u \geq 5$, entonces*

$$S_N(\theta) = O\Big(\frac{N}{log^3(N)}\Big).$$

Demostración. Teníamos que

$$S_N(\theta) = O(\sqrt{N}) + \sum_{d|P_N} \mu(d) \sum_{m=1}^{\frac{N}{d}} e^{2\pi i m d\theta}.$$

Del lema 5.1.6 podemos reescribir $S_N(\theta)$ como sigue:

$$S_N(\theta) = O(\sqrt{N}) + O\Big(log(N) \sum_{d=1}^{\frac{N}{M}} min\Big\{\frac{N}{d}, \frac{1}{||d\theta||}\Big\}\Big).$$

Haciendo $W = N$ y $W_0 = \frac{N}{M}$ $\Big(\frac{N}{M} \leq \frac{N}{e^{\frac{1}{2}\sqrt{log(N)}}}\Big)$ en el lema 5.1.2, obtenemos

$$S_N(\theta) = O(\sqrt{N}) + O\Big(log^2(N)\Big(\frac{N}{e^{\frac{1}{2}\sqrt{log(N)}}} + q + \frac{N}{q}\Big)\Big).$$

Como $log^u(N) \leq q \leq \frac{N}{log^u(N)}$, tenemos

$$\begin{aligned}
S_N(\theta) &= O(\sqrt{N}) + O\Bigg(log^2(N)\Bigg(\frac{N}{e^{\frac{1}{2}\sqrt{log(N)}}} + \frac{N}{log^u(N)} + \frac{N}{q}\Bigg)\Bigg) \\
&= O(\sqrt{N}) + O\Bigg(Nlog^2(N)\Bigg(\frac{1}{e^{\frac{1}{2}\sqrt{log(N)}}} + \frac{1}{log^u(N)} + \frac{1}{log^u(N)}\Bigg)\Bigg) \\
&= O(\sqrt{N}) + O\Bigg(Nlog^2(N)\Bigg(\frac{1}{e^{\frac{1}{2}\sqrt{log(N)}}} + \frac{1}{log^u(N)}\Bigg)\Bigg) \\
&= O(\sqrt{N}) + O\Bigg(\frac{Nlog^2(N)}{log^u(N)}\Bigg).
\end{aligned}$$

Por lo tanto si $u \geq 5$, tenemos

$$\begin{aligned}
S_N(\theta) &= O(\sqrt{N}) + O\Bigg(\frac{N}{log^3(N)}\Bigg) \\
&= O\Bigg(\frac{N}{log^3(N)}\Bigg).
\end{aligned}$$

□

5.1.8 Caso 2

Si $M < e^{\frac{1}{2}\sqrt{log(N)}}$ consideraremos nuevamente dos casos. El primero de ellos es considerar los divisores d tales que todos sus factores primos son menores o iguales que $e^{\sqrt{log(N)}}$; de aquí en adelante les llamaremos *divisores malos*. El segundo caso será considerar los divisores d tales que al menos uno de sus factores primos es estrictamente mayor que $e^{\sqrt{log(N)}}$. Estos serán llamados *divisores buenos*.

Divisores malos

Haciendo uso del teorema 2.7.4 a continuación veremos que en realidad no tenemos demasiados divisores malos.

Lema 5.1.9. *Sea*

$$S_1(M) = \sum_{\substack{d \leq \frac{N}{M} \\ d|P}} \mu(d) \sum_{\substack{M < m \leq M' \\ 1 \leq m \leq \frac{N}{d}}} e^{2\pi i m d\theta},$$

donde el subíndice 1 *indica que la suma se extiende sobre los divisores malos. Entonces*

$$\sum_{M<e^{\sqrt{log(N)}}} S_1(M) = O(Ne^{-c\sqrt{log(N)}}), \quad con \quad c>0.$$

Demostración. Haciendo $H = e^{\frac{1}{2}\sqrt{log(N)}}$, $x = \frac{N}{M}$ y $y = H^2$ en el teorema 2.7.4 tenemos que

$$R\Big(\frac{N}{M}, H^2\Big) = \frac{N}{M} e^{\left\{-log\left(\frac{N}{M}\right)\frac{log(log(\sqrt{log(N)}))}{\sqrt{log(N)}} + log(\sqrt{log(N)}) + O\left(\frac{log(\sqrt{log(N)})}{log(log(\sqrt{log(N)}))}\right)\right\}}.$$

Ahora

$$\begin{aligned} log\Big(\frac{N}{M}\Big) &= log(N) - log(M) \\ &\geq log(N) - log(e^{\sqrt{log(N)}}) \\ &= log(N) - \sqrt{log(N)}. \end{aligned}$$

Pero para N suficientemente grande tenemos $2\sqrt{log(N)} \leq log(N)$, entonces $log(N) - \sqrt{log(N)} \geq \frac{1}{2}log(N)$. Por lo tanto

$$log\Big(\frac{N}{M}\Big) \geq \frac{1}{2}log(N) \qquad \text{y} \qquad \frac{log\left(\frac{N}{M}\right)}{\sqrt{log(N)}} \geq \frac{\sqrt{log(N)}}{2}.$$

En consecuencia, dada C_1 una constante positiva cualquiera, existe N suficientemente grande tal que

$$\begin{aligned} \frac{log\left(\frac{N}{M}\right)}{\sqrt{log(N)}} log(log(\sqrt{log(N)})) &\geq \frac{\sqrt{log(N)}}{2} log(log(\sqrt{log(N)})) \\ &\geq C_1\sqrt{log(N)}. \end{aligned}$$

Por lo tanto

$$-\frac{log\left(\frac{N}{M}\right)}{\sqrt{log(N)}} log(log(\sqrt{log(N)})) < -C_1\sqrt{log(N)}.$$

Por otro lado, sea

$$F_N = log(\sqrt{log(N)}) + O\Big(\frac{log(\sqrt{log(N)})}{log(log(\sqrt{log(N)}))}\Big).$$

Para N suficientemente grande tenemos

$$\begin{aligned} F_N &\leq log(\sqrt{log(N)}) + C_2\frac{log(\sqrt{log(N)})}{log(log(\sqrt{log(N)}))} \\ &\leq log(\sqrt{log(N)}) + C_2 log(\sqrt{log(N)}) \\ &\leq C_3 log\Big(\sqrt{log(N)}\Big), \end{aligned}$$

donde C_2 y C_3 son constantes positivas. Tomando $C_1 > C_3$ tenemos

$$\begin{aligned} R\Big(\frac{N}{M}, H^2\Big) &= O\Big(\frac{N}{M}e^{-C_1\sqrt{log(N)}+C_3 log(\sqrt{log(N)})}\Big) \\ &= O\Big(\frac{N}{M}e^{-C_4\sqrt{log(N)}}\Big), \end{aligned}$$

donde $C_4 = C_3 - C_1$. Como $M' = O(M)$ tenemos que

$$S_1(M) = O\Big(M\frac{N}{M}e^{-C_4\sqrt{log(N)}}\Big) = O(Ne^{-C_4\sqrt{log(N)}})$$

y como teníamos $O(log(N))$ intervalos de la forma $M < m \leq M'$ tenemos que la contribución de los divisores malos a la suma $S(M)$ es:

$$\begin{aligned} \sum_{M<e^{\frac{1}{2}\sqrt{log(N)}}} S_1(M) &= O(log(N)Ne^{-C_4\sqrt{log(N)}}) \\ &= O(Ne^{-C_5\sqrt{log(N)}}). \qquad (C_5 > C_4) \end{aligned}$$

$\square$

Divisores buenos

Sólo nos resta considerar la suma

$$S(M) - S_1(M) = \sum_{M<m\leq M'}\sum_{d\leq\frac{N}{m}} \mu(d)e^{2\pi i m d\theta}, \qquad (5.6)$$

cuando $M < e^{\frac{1}{2}\sqrt{log(N)}}$ y d se extiende sobre los divisores de P que tienen al menos un factor primo estrictamente mayor que $e^{\sqrt{log(N)}}$. Podemos reescribir esta suma como sigue:

$$\sum_k S'_k(M) - \sum_k S''_k(M), \qquad \text{donde}$$

$$S'_k(M) = \sum_{M<m\leq M'} \sum_{d\leq \frac{N}{m}} e^{2\pi i dm\theta}.$$

En $S'_k(M)$ d es un divisor de P que tiene exactamente k factores primos estrictamente mayores que $e^{\sqrt{log(N)}}$ y además $\mu(d) = 1$. $S''_k(M)$ se define análogamente para cuando $\mu(d) = -1$. El índice k recorre los naturales $1, 2, 3, \ldots$ hasta alcanzar un valor $O(log(N))$, pues cualquier número que no exceda a N tiene a lo más $O(log(N))$ factores primos. Dado que $S'_k(M)$ y $S''_k(M)$ se pueden estimar de la misma manera, sólo consideraremos $S'_k(M)$. Sea

$$T_k(M) = \sum_{M<m\leq M'} \sum_{pt\leq \frac{N}{m}} \sum e^{2\pi i ptm\theta},$$

donde p recorre los números primos tales que $e^{\sqrt{log(N)}} < p \leq \sqrt{N}$ y t recorre los divisores de P tales que $\mu(t) = -1$ y que tienen exactamente $k-1$ factores primos estrictamente mayores que $e^{\sqrt{log(N)}}$. Los valores pt para los que $(p,t) = 1$ son los valores de d que puede tomar la suma $S'_k(M)$ y cada uno de estos valores aparecen k veces en la suma T_k (considere cada uno de los k factores primos de d que son mayores que $e^{\sqrt{log(N)}}$). Entonces el número de términos en T_k para los cuales $(p,t) > 1$ es trivialmente

$$O\Big(M \sum_{p>e^{\sqrt{log(N)}}} \sum_{p^2u\leq \frac{N}{M}} 1\Big) = O\Big(M \sum_{p>e^{\sqrt{log(N)}}} \frac{N}{Mp^2}\Big) = O\Big(\frac{N}{e^{\sqrt{log(N)}}}\Big).$$

En consecuencia

$$S'_k(M) = \frac{1}{k} T_k(M) + O(Ne^{-\sqrt{log(N)}}). \tag{5.7}$$

Para estimar $T_k(M)$ dividiremos el intervalo $e^{\sqrt{log(N)}} < p \leq \sqrt{N}$ en $O(log(N))$ bloques de la forma $Q < p \leq Q'$, donde $Q < Q' = O(Q)$. Sea $T_k(M,Q)$ la parte de la suma $T_k(M)$ correspondiente a tal intervalo de primos. Tenemos el siguiente:

Lema 5.1.10. *Sea*

$$T_k(M,Q) = \sum_{M<m\leq M'} \sum_{Q<p\leq Q'} \sum_{mpt\leq N} e^{2\pi impt\theta}.$$

Entonces

$$T_k(M,Q) = O\left(Nlog^2(N)\left(\left(\frac{1}{q} + \frac{q}{N}\right)^{\frac{1}{2}} + e^{-\frac{1}{2}\sqrt{log(N)}}\right)\right)$$

Demostración. El resultado se sigue si aplicamos el lema 5.1.3 con $n = mp$ y $v = t$ donde t está restringido a los divisores de P tales que $\mu(t) = -1$ y tienen exactamente $k-1$ factores primos estrictamente mayores que $e^{\sqrt{log(N)}}$. La U en el lema 5.1.3 corresponde aquí a MQ; tenemos

$$T_k(M,Q) = O\left(Nlog^2(N)\left(\frac{1}{q} + \frac{q}{N} + \frac{1}{MQ} + \frac{MQ}{N}\right)^{\frac{1}{2}}\right),$$

pero $e^{\sqrt{log(N)}} \leq Q \leq \sqrt{N}$, entonces

$$\frac{1}{MQ} < e^{-\sqrt{log(N)}} \qquad \text{y} \qquad \frac{MQ}{N} < \frac{e^{\frac{1}{2}\sqrt{log(N)}}}{\sqrt{N}} < e^{-\sqrt{log(N)}}.$$

El resultado se sigue trivialmente. □

Del lema anterior, si sumamos ahora sobre los $O(log(N))$ valores de Q tenemos que

$$T_k(M) = O\left(Nlog^3(N)\left(\left(\frac{1}{q} + \frac{q}{N}\right)^{\frac{1}{2}} + e^{-\frac{1}{2}\sqrt{log(N)}}\right)\right).$$

Esta misma relación salvo un factor de $\frac{1}{k}$ se cumple para $s'_k(M)$ $(s''_k(M))$ utilizando la ecuación 5.7. Por lo tanto, sumando sobre los $O(log(N))$ valores posibles de k y notando que

$$\sum_{k=1}^{O(log(N))} \frac{1}{k} = O\Big(log\Big(log(N)\Big)\Big) = O(\sqrt{log(N)}),$$

tenemos que

$$S(M)-S_1(M)=O\left(Nlog^{\frac{7}{2}}(N)\left(\left(\frac{1}{q}+\frac{q}{N}\right)^{\frac{1}{2}}+e^{-\frac{1}{2}\sqrt{log(N)}}\right)\right),$$

donde $S(M)-S_1(M)$ es como en la ecuación 5.6. Para finalizar, si sumamos ahora sobre los $O(log(N))$ valores de M obtenemos

$$S(M)-S_1(M)=O\left(Nlog^{\frac{9}{2}}(N)\left(\left(\frac{1}{q}+\frac{q}{N}\right)^{\frac{1}{2}}+e^{-\frac{1}{2}\sqrt{log(N)}}\right)\right). \tag{5.8}$$

Teorema 5.1.11. *Sea* $\theta\in\mathfrak{m}$, *entonces*

$$S_N(\theta)=\sum_{p\leq N}e^{2\pi ip\theta}=O\Big(\frac{N}{log^3(N)}\Big).$$

Demostración. De los lemas 5.1.7, 5.1.9 y la ecuación 5.8 tenemos que

$$S_N(\theta) \;=\; O\Big(\frac{N}{log^3(N)}\Big)+O\Big(Ne^{-c_5\sqrt{log(N)}}\Big)+R,$$

donde

$$R=O\left(Nlog^{\frac{9}{2}}(N)\left(\left(\frac{1}{q}+\frac{q}{N}\right)^{\frac{1}{2}}+e^{-\frac{1}{2}\sqrt{log(N)}}\right)\right).$$

Es claro que

$$O\Big(\frac{N}{log^3(N)}\Big)+O\Big(Ne^{-c_5\sqrt{log(N)}}\Big)=O\Big(\frac{N}{log^3(N)}\Big).$$

Por otro lado $log^u(N)\leq q\leq\frac{N}{log^u(N)}$, entonces

$$\Big(\frac{1}{q}+\frac{q}{N}\Big)^{\frac{1}{2}}=O\Big(log^{\frac{-u}{2}}(N)\Big),$$

de tal modo que

$$R=O\left(log^{\frac{9-u}{2}}(N)\right)$$

En consecuencia si $u>15$ tenemos que

$$S_N(\theta)=O\Big(\frac{N}{log^3(N)}\Big).$$

□

Apéndice A

Miscelánea

A.1 Congruencias

Si m y n son dos enteros positivos que satisfacen, $(m, n) = 1$ y x es tal que $x \equiv m (mod\, n)$, entonces $(x, n) = 1$ y por lo tanto hay $\phi(n)$ clases de equivalencia módulo n tales que cada representante y n son primos relativos.

Definición A.1.1. Cualquier conjunto formado por $\phi(n)$ residuos módulo n que son primos relativos a n, cada uno de distinta clase, es llamado *sistema completo de residuos primos* a n.

Lema A.1.2. *Suponga que $m_1, m_2, \ldots, m_{\phi(n)}$ es un sistema completo de residuos primos a n y que $m'_1, m'_2, \ldots, m_{\phi(n')}$ es un sistema completo de residuos primos a n' donde $(n, n') = 1$. Entonces $m'_i n + m_j n'$ con $i = 1, 2, \ldots, \phi(n')$ y $j = 1, 2, \ldots, \phi(n)$ es un sistema completo de residuos primos a nn'.*

Demostración. Trivialmente podemos observar que hay $\phi(n)\phi(n')$ números de la forma $m'_i n + m_j n'$. Por otro lado, si

$$\begin{aligned} m'_i n + m_j n' &\equiv m'_k n + m_l n' (mod\, nn') \\ \Rightarrow \quad m'_i n + m_j n' &\equiv m'_k n + m_l n' (mod\, n) \\ \Rightarrow \quad m_j n' &\equiv m_l n' (mod\, n) \end{aligned}$$

$$\begin{aligned} \Rightarrow \qquad\qquad m_j &\equiv m_l (mod\, n) \\ \text{y análogamente} & \\ m'_i &\equiv m'_k (mod\, n'). \end{aligned}$$

Ahora, si $(m'_i n + m_j n', n'n) > 1$ para alguna i y j, entonces existe un primo p de tal forma que $p|n'n$ y $p|(m'_i n + m_j n')$. Como $(n', n) = 1$, entonces p divide únicamente a n' ó a n. Si $p|n'$ se tiene que $p|m'_i n$ y por lo tanto $p|m'_i$ lo cual no puede ser pues $(m'_i, n') = 1$. De manera análoga si suponemos que $p|n$ llegamos a una contradicción. Por lo tanto los $\phi(n)\phi(n')$ números forman un sistema completo de residuos primos a nn'. □

A.2 Series, Sumas e Integrales

Lema A.2.1. *Sea* $0 \leq a < 1$, *entonces*

$$\sum_{k=0}^{\infty} a^k = \frac{1}{1-a}.$$

Demostración. Tenemos la siguientes relaciones:

$$\begin{aligned} 1 - a^n &= (1-a)(1 + a + a^2 + \cdots + a^{n-1}) \\ \frac{1-a^n}{1-a} &= (1 + a + a^2 + \cdots + a^{n-1}) \\ \frac{1-a^n}{1-a} &= \sum_{k=1}^{n-1} a^k. \end{aligned}$$

El resultado se sigue tomando el límite cuando $n \to \infty$. □

Lema A.2.2 (Criterio de Condensación de Cauchy). *Sea* $\{a_n\}_{n \in N}$ *una sucesión monótona decreciente de números reales positivos, entonces*

$$\sum_{n=1}^{\infty} a_n \quad \textit{converge si y sólo si} \quad \sum_{n=1}^{\infty} 2^n a_{2^n} \quad \textit{converge.}$$

Demostración. Del hecho de que una serie de números reales positivos converge, si y sólo si sus sumas parciales forman una sucesión acotada, será suficiente considerar las sucesiones de sumas parciales correspondientes.

Sean $s_n = a_1 + a_2 + \cdots + a_n$ y $t_k = a_1 + 2a_2 + \cdots + 2^k a_{2^k}$.
Para $n < 2^k$,

$$\begin{aligned} s_n &\leq a_1 + (a_2 + a_3) + \cdots + (a_{2^k} + \cdots + a_{2^{k+1}-1}) \\ &\leq a_1 + 2a_2 + \cdots + 2^k a_{2^k} = t_k. \end{aligned}$$

Por lo tanto, $s_n \leq t_k$.

Por otro lado si $n > 2^k$,

$$\begin{aligned} s_n &\geq a_1 + a_2 + (a_3 + a_4) + \cdots + (a_{2^{k-1}+1} + \cdots + a_{2^k}) \\ &\geq \frac{1}{2}a_1 + a_2 + 2a_4 \cdots + 2^{k-1}a_{2^k} = \frac{1}{2}t_k, \end{aligned}$$

de tal modo que $2s_n \geq t_k$ y se cumple la relación $s_n \leq t_k \leq 2s_n$ que implica que las sucesiones $\{s_n\}$ y $\{t_k\}$ son simultáneamente convergentes o divergentes. □

Lema A.2.3. *Sea $\{\frac{1}{n}\}_{n\in N}$ la sucesión armónica y $r > 1$, entonces la serie $\sum_{n=1}^{\infty} \frac{1}{n^r}$ converge.*

Demostración. Del lema A.2.2 tenemos que la serie $\sum_{n=1}^{\infty} \frac{1}{n^r}$ converge si y sólo si la serie $\sum_{n=0}^{\infty} 2^n \frac{1}{2^{nr}} = \sum_{n=0}^{\infty} 2^{(1-r)n}$ converge. Del lema A.2.1 tenemos que esto pasa si $2^{1-r} < 1$, esto es si y sólo si $1 - r < 0$. El resultado se sigue trivialmente. □

Lema A.2.4 (Fórmula para sumar de Abel). *Sean u y f funciones aritméticas. Sea $U(t) = \sum_{n\leq t} u(n)$. Entonces*

1. *Si a y b son enteros no negativos tales que $a < b$, entonces*

$$\sum_{n=a+1}^{b} u(n)f(n) = U(b)f(b) - U(a)f(a+1) - \sum_{n=a+1}^{b-1} U(n)(f(n+1) - f(n)).$$

2. *Si x y y son números reales no negativos tales que $0 \leq y < x$ y g es una función de clase $C^1(y,x)$, entonces*

$$\sum_{y<n\leq x} u(n)g(n) = U(x)g(x) - U(y)g(y) - \int_y^x U(t)g'(t)dt.$$

Demostración. 1. En este caso tenemos

$$\begin{aligned}\sum_{n=a+1}^{b} u(n)f(n) &= \sum_{n=a+1}^{b}\Big(U(n)-U(n-1)\Big)f(n) \\ &= \sum_{n=a+1}^{b} U(n)f(n) - \sum_{n=a}^{b-1} U(n)f(n+1) \\ &= U(b)f(b) - U(a)f(a+1) - \sum_{n=a+1}^{b-1} U(n)(f(n+1)-f(n)).\end{aligned}$$

2. Si g es de clase $C^1(y,x)$, tenemos

$$g(n+1)-g(n) = \int_n^{n+1} g'(t)dt.$$

Por lo tanto, como $U(t)=U(n)$ si $n \leq t < n+1$ tenemos

$$U(n)(g(n+1)-g(n)) = \int_n^{n+1} U(t)g'(t)dt.$$

Sean $a=[y]$ y $b=[x]$. Entonces

$$\begin{aligned}\sum_{y<n\leq x} u(n)g(n) &= \sum_{n=a+1}^{b} u(n)g(n)dt \\ &= U(b)g(b) - U(a)g(a+1) - \sum_{n=a+1}^{b-1} U(n)(g(n+1)-g(n)) \\ &= U(x)g(b) - U(y)g(a+1) - \sum_{n=a+1}^{b-1}\int_n^{n+1} U(t)g'(t)dt\end{aligned}$$

$$\begin{aligned}
&= U(x)g(x) - U(y)g(y) - U(x)(g(x) - g(b)) \\
&\quad -U(y)(g(a+1) - g(y)) - \int_{a+1}^{b} U(t)g'(t)dt \\
&= U(x)g(x) - U(y)g(y) - \int_{y}^{x} U(t)g'(t)dt.
\end{aligned}$$

□

Observación A.2.5. Nótese que si g es de clase $C^1[1,x]$, tenemos

$$\begin{aligned}
\sum_{n\le x} u(n)g(n) &= u(1)g(1) + \sum_{1<n\le x} u(n)g(n) \\
&= u(1)g(1) + U(x)g(x) - U(1)g(1) - \int_1^x U(t)g'(t)dt \\
&= U(x)g(x) - \int_1^x U(t)g'(t)dt.
\end{aligned}$$

Lema A.2.6 (Fórmula para sumar de Euler). *Si f tiene derivada continua f' en el intervalo $[y,x]$, en donde $0<y<x$, entonces*

$$\sum_{y<n\le x} f(n) = \int_y^x f(t)dt + \int_y^x (t-[t])f'(t)dt + f(x)([x]-x) - f(y)([y]-y).$$

Demostración. Sea $m=[y]$, $k=[x]$. Para enteros n y $n-1$ de $[y,x]$ tenemos

$$\begin{aligned}
\int_{n-1}^{n} [t]f'(t)dt &= \int_{n-1}^{n} (n-1)f'(t)dt = (n-1)(f(n)-f(n-1)) \\
&= \Big(nf(n) - (n-1)f(n-1)\Big) - f(n).
\end{aligned}$$

Sumando de $n=m+1$ hasta $n=k$ tenemos

$$\begin{aligned}
\int_m^k [t]f'(t)dt &= \sum_{n=m+1}^{k} \Big(nf(n) - (n-1)f(n-1)\Big) - \sum_{y<n\le x} f(n) \\
&= kf(k) - mf(m) - \sum_{y<n\le x} f(n).
\end{aligned}$$

Por lo tanto

$$\sum_{y<n\leq x} f(n) = -\int_m^k [t]f'(t)dt + kf(k) - mf(m) \tag{A.1}$$

$$= -\int_y^x [t]f'(t)dt + kf(x) - mf(y). \tag{A.2}$$

Por otro lado, podemos integrar por partes $\int_y^x tf'(t)dt$ y obtenemos

$$\int_y^x f(t)dt = xf(x) - yf(y) - \int_y^x tf'(t)dt. \tag{A.3}$$

Por último, combinando la ecuación (A.3) con la ecuación (A.1) obtenemos el resultado deseado. □

Lema A.2.7. *Si $x \geq 1$ tenemos:*

1. $\sum_{n\leq x} \frac{1}{n} = log(x) + C + O\Big(\frac{1}{x}\Big)$.
2. *Si* $\alpha > 0$, $\sum_{n\leq x} n^{\alpha} = \frac{x^{\alpha+1}}{\alpha+1} + O(x^{\alpha})$

Demostración. 1. Utilizamos la fórmula para sumar de Euler con $f(t) = \frac{1}{t}$ y obtenemos

$$\begin{aligned}\sum_{n\leq x}\frac{1}{n} &= \int_1^x \frac{dt}{t} - \int_1^x \frac{t-[t]}{t^2}dt + 1 - \frac{x-[x]}{x} \\ &= log(x) - \int_1^x \frac{t-[t]}{t^2}dt + 1 + O\Big(\frac{1}{x}\Big) \\ &= log(x) + 1 - \int_1^\infty \frac{t-[t]}{t^2}dt + \int_x^\infty \frac{t-[t]}{t^2}dt + O\Big(\frac{1}{x}\Big).\end{aligned}$$

Ahora la integral impropia $\int_1^\infty \frac{t-[t]}{t^2}dt$ existe pues está dominada por $\int_1^\infty \frac{1}{t^2}dt$. Además

$$0 \leq \int_x^\infty \frac{t-[t]}{t^2}dt \leq \int_x^\infty \frac{1}{t^2}dt = \frac{1}{x}.$$

De esta manera tenemos

$$\sum_{n\leq x}\frac{1}{n} = log(x) + 1 - \int_1^{\infty}\frac{t-[t]}{t^2}dt + O\Big(\frac{1}{x}\Big).$$

Esto prueba el resultado con

$$C = 1 - \int_1^{\infty}\frac{t-[t]}{t^2}dt.$$

2. Utilizamos una vez más la fórmula para sumar de Euler con $f(t) = t^{\alpha}$ para obtener

$$\begin{aligned}\sum_{n\leq x} n^{\alpha} &= \int_1^x t^{\alpha}dt + \alpha\int_1^x t^{\alpha-1}(t-[t])dt + 1 - (x-[x])x^{\alpha}\\ &= \frac{x^{\alpha+1}}{\alpha+1} - \frac{1}{\alpha+1} + O\left(\alpha\int_1^x t^{\alpha-1}dt\right) + O(x^{\alpha})\\ &= \frac{x^{\alpha+1}}{\alpha+1} + O(x^{\alpha}).\end{aligned}$$

□

A.3 Productos Infinitos

Definición A.3.1. Sea $\{a_n\}_{n\in\mathbb{N}}$ una sucesión de números complejos. El enésimo producto parcial de esta sucesión es el número

$$p_n = a_1a_2\cdots a_n = \prod_{k=1}^{n} a_k.$$

Si la sucesión de productos parciales converge a algún límite $a \neq 0$ cuando $n \to \infty$ decimos que el producto infinito $\prod_{k=1}^{\infty} a_k$ converge y

$$\prod_{k=1}^{\infty} a_k = \lim_{n\to\infty} p_n = \lim_{n\to\infty}\prod_{k=1}^{n} a_k.$$

Diremos que el producto infinito diverge si el límite de la sucesión de productos parciales no existe o es cero. En este último caso diremos que el producto infinito diverge a cero.

Lema A.3.2. *Sea* $\{a_n\}_{n\in\mathbb{N}}$ *una sucesión de números complejos y* $\alpha_n = 1+a_n$. *Si el producto infinito* $\prod_{k=1}^{\infty}(1+a_k)$ *converge, entonces* $\lim\limits_{n\to\infty} a_n = 0$.

Demostración. Como el producto infinito converge entonces $a_n \neq -1$ para todo $n \in \mathbb{N}$. Además $\lim\limits_{n\to\infty}(1+a_n) = \lim\limits_{n\to\infty}\frac{p_n}{p_{n-1}} = 1$. Por lo tanto $\lim\limits_{n\to\infty} a_n = 0$. □

Lema A.3.3. *Sea* $a_k \geq 0$ *para toda* $k \in \mathbb{N}$. *El producto infinito* $\prod_{k=1}^{\infty}(1+a_k)$ *converge si y sólo si la serie* $\sum_{k=1}^{\infty} a_k$ *converge.*

Demostración. Sean $s_n = \sum_{k=1}^{n} a_k$ y $p_n = \prod_{k=1}^{n}(1+a_k)$. Ya que $a_n \geq 0$, las sucesiones $\{s_n\}$ y $\{p_n\}$ son monótonas crecientes y $p_n \geq 1$ para toda n. Dado que

$$1 + x \leq e^x$$

para $x \in \mathbb{R}^+$, tenemos

$$0 \leq \sum_{k=1}^{n} a_k < \prod_{k=1}^{n}(1+a_k) \leq \prod_{k=1}^{n} e^{a_k} = e^{a_1+a_2+\cdots+a_n}$$

y por lo tanto

$$0 \leq s_n \leq p_n \leq e^{s_n}.$$

Lo cual comprueba que $\{p_n\}$ converge si y sólo si $\{s_n\}$ converge. □

Definición A.3.4. Decimos que el producto infinito $\prod_{n=1}^{\infty}(1+a_n)$ converge absolutamente si el producto infinito $\prod_{n=1}^{\infty}(1+|a_n|)$ converge.

Lema A.3.5. *Si el producto infinito* $\prod_{n=1}^{\infty}(1+a_n)$ *converge absolutamente, entonces converge.*

Demostración. Sean

$$p_n = \prod_{k=1}^{n}(1+a_k) \quad \text{y} \quad P_n = \prod_{k=1}^{n}(1+|a_k|).$$

Si el producto infinito converge absolutamente, entonces la sucesión de productos parciales $\{P_n\}$ converge y por lo tanto la serie $\sum_{n=2}^{\infty}(P_n - P_{n-1})$ converge, puesto que

$$\sum_{n=2}^{\infty}(P_n - P_{n-1}) = \sum_{n=2}^{\infty} P_{n-1}|a_n|,$$

donde $1 \leq P_{n-1} \leq \lim_{n\to\infty} P_{n-1} = P$ para toda $n \geq 2$.

Por lo tanto

$$\sum_{n=2}^{\infty}(P_n - P_{n-1}) \leq P \sum_{n=2}^{\infty} |a_n|$$

y por el lema A.3.3 la serie $\sum_{n=2}^{\infty} |a_n|$ converge. Dado que

$$\begin{aligned} 0 \ \leq \ & |p_n - p_{n-1}| = |a_n p_{n-1}| = \left| a_n \prod_{k=1}^{n-1}(1 + a_k) \right| \\ \leq \ & |a_n| \prod_{k=1}^{n-1}(1 + |a_k|) = |a_n| P_{n-1} = P_n - P_{n-1}, \end{aligned}$$

tenemos que la serie

$$\sum_{n=2}^{\infty} |p_n - p_{n-1}|$$

converge y por lo tanto

$$\sum_{n=2}^{\infty}(p_n - p_{n-1}) = \lim_{n\to\infty} \sum_{k=2}^{n}(p_k - p_{k-1}) = \lim_{n\to\infty}(p_n - p_1)$$

converge. De tal forma que la sucesión de productos parciales $\{p_n\}$ converge a un límite finito. Debemos probar ahora que este límite no es cero, pues de lo contrario la sucesión de productos parciales divergería a cero.[1] Ya que el producto infinito $\prod_{k=1}^{\infty}(1 + a_k)$ converge absolutamente, se sigue del lema

[1] Ver la definición C.0.22

A.3.3 que la serie $\sum_{k=1}^{\infty} |a_k|$ converge y por lo tanto los números a_k convergen a cero. Por consiguiente, para todo k suficientemente grande,

$$|1 + a_k| \geq \frac{1}{2} \quad \text{y} \quad \left|\frac{-a_k}{1 + a_k}\right| \leq 2|a_k|$$

Se sigue que

$$\sum_{k=1}^{\infty} \left|\frac{-a_k}{1 + a_k}\right|$$

converge y por lo tanto el producto

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

converge absolutamente. La primera parte de la demostración implica que la sucesión de productos parciales

$$\prod_{k=1}^{n} \left(1 - \frac{a_k}{1 + a_k}\right) = \prod_{k=1}^{n} \frac{1}{1 + a_k} = \frac{1}{\prod_{k=1}^{n}(1 + a_k)} = \frac{1}{p_n}$$

converge a un límite finito y entonces el límite de la sucesión $\{p_n\}$ es distinto de cero. Por lo tanto el producto infinito $\prod_{k=1}^{\infty}(1 + a_k)$ converge.

□

Definición A.3.6. Un *producto de Euler* es un producto infinito sobre números primos y se denota con $\prod_p$.

Lema A.3.7. *Sea $f(n)$ una función multiplicativa que no es idénticamente cero. Si la serie*

$$\sum_{n=1}^{\infty} f(n)$$

converge absolutamente, entonces

$$\sum_{n=1}^{\infty} f(n) = \prod_{p} (1 + f(p) + f(p^2) + \cdots).$$

Si $f(n)$ es completamente multiplicativa, entonces

$$\sum_{n=1}^{\infty} f(n) = \prod_{p} \Big(\frac{1}{1-f(p)}\Big).$$

Demostración. Si la serie $\sum_{n=1}^{\infty} f(n)$ converge absolutamente, entonces la serie

$$a_p = \sum_{k=1}^{\infty} f(p^k)$$

converge absolutamente para todo primo p. También la serie $\sum_p |a_p|$ converge puesto que

$$\sum_{p} |a_p| = \sum_{p} \Big|\sum_{k=1}^{\infty} f(p^k)\Big| \leq \sum_{p}\sum_{k=1}^{\infty} |f(p^k)| < \sum_{k=1}^{\infty} |f(n)|.$$

Además del lema A.3.3 el producto

$$\prod_{p}(1+a_p) = \prod_{p} \Big(1 + \sum_{k=1}^{\infty} f(p^k)\Big)$$

converge absolutamente y por el lema A.3.5, este producto infinito converge. Sea $\epsilon > 0$ y N_0 un entero tal que

$$\sum_{n>N_0} |f(n)| < \epsilon.$$

Para cada entero positivo n, sea $P(n)$ el factor primo más grande de n. Denotamos por

$$\sum_{P(n)\leq N} \qquad \text{y} \sum_{P(n)>N}$$

la suma sobre los enteros cuyos factores primos son todos menores o iguales que N y la suma sobre los enteros que tienen al menos un factor primo mayor que N. Sea $N \geq N_0$. Utilizando la factorización única como producto de primos para n, se sigue que

$$\prod_{p\leq N} \Big(1 + \sum_{k=1}^{\infty} f(p^k)\Big) = \sum_{P(n)\leq N} f(n)$$

y por lo tanto

$$\begin{aligned}
\Big|\sum_{n=1}^{\infty} f(n) - \prod_{p\leq N}\Big(1+\sum_{k=1}^{\infty} f(p^k)\Big)\Big| &= \Big|\sum_{n=1}^{\infty} f(n) - \sum_{P(n)\leq N} f(n)\Big| \\
&= \Big|\sum_{P(n)>N} f(n)\Big| \leq \sum_{P(n)>N} |f(n)| \\
&\leq \sum_{n>N} |f(n)| \leq \sum_{n>N_0} |f(n)| < \epsilon.
\end{aligned}$$

Lo cual implica que

$$\sum_{n=1}^{\infty} f(n) = \lim_{N\to\infty} \prod_{p\leq N}\Big(1+\sum_{k=1}^{\infty} f(p^k)\Big) = \prod_{p}\Big(1+\sum_{k=1}^{\infty} f(p^k)\Big)$$

y con esto probamos la primera parte del lema.

Por otro lado si $f(n)$ es completamente multiplicativa, entonces $f(p^k) = \Big(f(p)\Big)^k$ para todo primo p y cualquier entero no negativo k. Ya que $f(p^k) \to 0$ si $k \to \infty$ se sigue que $|f(p)| < 1$. Calculando la progresión geométrica obtenemos

$$1+\sum_{k=1}^{\infty} f(p^k) = 1+\sum_{k=1}^{\infty}\Big(f(p)\Big)^k = \frac{1}{1-f(p)}$$

y por lo tanto

$$\prod_{p}\Big(1+\sum_{k=1}^{\infty} f(p^k)\Big) = \prod_{p}\frac{1}{1-f(p)}.$$

□

Bibliografía.

[1] G. H. Hardy & S. Ramanujan: *Asymptotic formulae in combinatory analysis*, Proc. Lond. Math. Soc., (2), 17, (1918), 75-115. [1].

[2] R. C. Vaughan: *The Hardy-Littlewood Method*, Cambridge University Press Vol. 125 (1997)

[3] A. A. Karatsuba: *Basic analytic number theory*, Springer-Verlag (1993)

[4] W. Rudin: *Functional Analysis*, MacGraw-Hill Vol. (1973)

[5] R. A. Rankin: *The difference between consecutive prime numbers*, J. Lond. Math. Soc., No. 13 (1938), 242-247.

[6] I. M. Vinogradov: *The method of triginometrical sums in the theory of numbers*, Interscience Publishers LTD., London (1947).