EL MÉTODO DEL CÍRCULO Y EL TEOREMA DE VINOGRADOV

JORGE JIMÉNEZ URROZ

Máster en Matemáticas Avanzadas.
Universidad Complutense de Madrid.

Fechas: Primera sesión: Lunes 28 de noviembre de 2023. De 17:00h. a 18:30h.

Segunda sesión: Martes 29 de noviembre de 2023. De 17:00h. a 18:30h.

Aula:. Seminario 238 de la Facultad de Matemáticas, UCM.

---

1. INTRODUCCIÓN

La Aritmética nace como el arte de clasificar, distribuir y, en definitiva, entender de la mayor forma posible una amplia variedad de subconjuntos pintorescos de los números enteros como son los números perfectos, amigables, repunidades, números de Fibonacci, de Lucas, soluciones de ecuaciones diofánticas, sumas de cuadrados, y problemas relacionados con ellos como son el último Teorema de Fermat, el problema de Waring, la conjetura de Goldbach, de los primos gemelos, primos representables como n^2+1, etc.

Todos estos problemas están relacionados de una u otra forma con la estructura que adquieren los enteros con las operaciones de suma y multiplicación. Sumar es más o menos fácil. Multiplicar ya no tanto y, de hecho, nuestra sociedad basa su seguridad en que nadie sabe dividir lo suficientemente bien, como para factorizar un número con solamente dos factores primos. Y ya lo que hace que un problema sea intratable es cuando se mezclan la suma y la multiplicación, como son los problemas que enunciamos al final del párrafo anterior.

Teoría analítica de números es el estudio de problemas de aritmética utilizando herramientas típicas de análisis. Es más fácil ver algo continuo que algo que está espaciado de forma que parece ser aleatoria. El primer ejemplo del puente entre las dos nos lo revela Euler gracias al teorema fundamental de la aritmética, con la identidad

$$\zeta(s)=\sum_{n\geq 1}\frac{1}{n^s}=\prod_{p}\left(1-p^{-s}\right)^{-1},$$

cierta para cualquier $s>1$, donde el producto recorre los números primos, y la suma los números enteros. El estudio de los números primos, de apariencia aleatoria, se reduce así a teoremas sobre la función $\zeta(s)$. Y, simplemente observando que la serie armónica es divergente, probamos que existe un número infinito de primos.

Resulta que dicha función se puede extender de forma analítica a todo el plano complejo, salvo en $s=1$ que tiene un polo simple, lo que permite a Riemann dar

una vía plausible de atacar el problema de la distribución de los números primos, a través de la variable compleja. La prueba completa del teorema de los números primos, por el que sabemos que si $\pi(x)$ es la función que cuenta los números primos hasta x cumple la fórmula asintótica

$$\pi(x) \sim \frac{x}{\log x},$$

se la debemos a Hadamard y de la Valle Poussin, y no es casualidad que el teorema de Hadamard, una especie de generalización del teorema fundamental del Álgebra, nos permita expresar la función $\zeta(s)$ como producto de sus ceros

$$\zeta(s) = \frac{e^{(\log(2\pi)-1-\gamma/2)s}}{2(s-1)\Gamma(1+s/2)} \prod_{\rho} \left(1-\frac{s}{\rho}\right) e^{s/\rho},$$

y así sacar información de los números primos a través de información de los ceros de la función zeta de Riemann.

Uno de los objetivos principales de la Teoría Analítica de Números, como hemos visto en el comportamiento de $\pi(x)$, es establecer fórmulas asintóticas para cantidades aritméticas que crecen con x y controlar el término de error en dichas fórmulas, a través de medidas que detecten algún tipo de cancelación. Es decir, de alguna forma hay que distinguir la parte principal de la cantidad que estamos intentando entender. Pues bien, quizás una de las grandes ideas que debemos tener en cuenta es que lo grande se ve mucho más que lo pequeño. Así por ejemplo mirando en $s=1$, donde la función zeta tiene un polo extraemos la información de la infinitud de los primos. Para estudiar los ceros de la función zeta, estudiamos los polos de la función $1/\zeta(s)$ que serán mucho mas visibles y, sin embargo, gracias a su fórmula como producto de Euler, tendrá propiedades similares. Concretamente

$$\frac{1}{\zeta(s)} = \prod_{p} \left(1-p^{-s}\right) = \sum_{n\geq 1} \frac{\mu(n)}{n^s},$$

donde

$$\mu(n) = \begin{cases} (-1)^k & \text{si } n = p_1 \cdots p_k, \\ 0 & \text{si } p^2 | n, \end{cases}$$

es la función de Möbius. Es interesante la fórmula de ortogonalidad

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \neq 1. \end{cases} \tag{1}$$

Otro truco que ahonda en esta misma idea es utilizar la función logaritmo que de nuevo transforma lo pequeño en grande, y que además convierte la difícil multiplicación en la más asequible suma. Así, un ejemplo muy simple y muy ilustrativo del uso de análisis elemental lo encontramos al considerar la derivada de la función $(\log \zeta(s))$, obteniendo

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n\geq 1} \frac{\Lambda(n)}{n^s},$$

donde

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

es la función de Von Mangoldt. No es por tanto casualidad que la función de Von Mangoldt sea el puente natural para estudiar problemas de aritmética con técnicas de análisis y, de hecho, es fácil ver que

$$\sum_{d|n} \Lambda(d) = \log n \tag{2}$$

convierte de forma sencilla toda la naturaleza aritmética del problema a la izquierda de la ecuación, en la analítica de la función logaritmo a la derecha de la misma.

Como vemos, para sacar el término principal de una estimación habitualmente debemos mirar a las singularidades de la función involucrada. No es de extrañar que siendo la función zeta la función generatriz de los números primos, permita estudiar una gran generalidad de funciones aritméticas multiplicativas. En general para cualquier serie de Dirichlet $F(s) = \sum_n \frac{a_n}{n^s}$, y $G(s) = \sum_n \frac{b_n}{n^s}$, se tiene

$$F(s)G(s) = \sum_{n\geq 1} \frac{a_n}{n^s} \sum_{m\geq 1} \frac{b_m}{m^s} = \sum_{k\geq 1} \sum_{nm=k} \frac{a_n b_m}{k^s} = \sum_{k\geq 1} \frac{c_k}{k^s} \tag{3}$$

donde

$$c_k = \sum_{d|k} a_d b_{k/d},$$

es la convolución de las sucesiones $\{a_n\}$ y $\{b_n\}$. Por ejemplo, si tomamos ambas funciones $F(s) = G(s) = \zeta(s)$, obtenemos

$$\zeta^2(s) = \sum_{k\geq 1} \frac{d(k)}{k^s},$$

donde $d(k)$ es la función que cuenta el número de divisores de k.

2. El método del círculo

Podemos resumir la idea de atacar un problema aritmético de forma analítica de la siguiente forma: codificamos el problema a través de una función de variable real o compleja que almacene dicha información, usamos las técnicas apropiadas del análisis, y recuperamos la aritmética al final del proceso. En el caso de la función $\pi(x)$ esto se hace a través de la función zeta de Riemann. Veremos que una técnica apropiada cuando el problema tiene naturaleza aditiva es el método el círculo.

El método del círculo se origina con un artículo de Hardy y Ramanujan en el que pretenden determinar el comportamiento asintótico de la función partición, que cuenta el número de veces que se puede representar un entero n como suma de enteros positivos, así que tomémoslo como ejemplo. En este caso, la función de variable compleja será su función generatriz

$$F(z) = \prod_{n\geq 1} \frac{1}{1-z^n} = \sum_{k\geq 1} p(k) z^k,$$

identidad que surge de expandir la serie geométrica de razón z^n, y multiplicar los factores. Para recuperar la función aritmética utilizamos la fórmula integral de Cauchy

$$p(k) = \frac{1}{2\pi i} \int_{|z|=r} \frac{F(z)}{z^{n+1}} dz.$$

Así pues, dar una buena estimación de la función particion pasa por estimar la integral de forma apropiada. Y como hemos mencionado en la sección anterior, la aportación más significativa viene de las singularidades de la función.

En este caso, la función tiene su frontera natural de convergencia en el círculo unidad, pero no todas las singularidades alli son del mismo tamaño. Concretamente en $z = 1$ todos los factores tienen un polo, mientras que en $z = -1$ solo la mitad de ellos. De la misma forma, solo una fracción de los factores tendrá polos en las raíces q-ésimas de la unidad y, dicha fracción, será menor según n crezca. Si denotamos por $e(\alpha) = e^{2\pi i\alpha}$ entonces es pues de esperar que las singularidades mayores vendrán de números $\alpha = \frac{a}{q}$ racionales con q pequeño.

Así pues, para estimar la integral, lo que haremos será considerar un r cercano a 1 y luego dividir el intervalo de integración en subintervalos de dos clases: los arcos mayores $\mathfrak{M}$, con subintervalos alrededor de números racionales de denominador pequeño, y $\mathfrak{m}$, los arcos menores, que será el complementario. El tamaño de cada uno de los subintervalos se debe tomar en función del problema.

El método se puede aplicar a cualquier tipo de problema del estilo siguiente: tomamos una sucesión de números enteros positivos $A = \{a_k\}$, y queremos calcular el número de representaciones de un entero cualquiera n, como suma de l elementos de A. Vamos a llamar a ese número $r_A(n)$. Y como en el caso anterior, consideramos la serie de potencias

$$F_A(z) = \sum_k z^{a_k},$$

con lo que

$$(F_A(z))^l = \sum_{n_i \dots n_l} z^{a_{n_1} \dots a_{n_l}} = \sum_{n \geq 1} r_A(n) z^n,$$

y de nuevo por la fórmula de Cauchy se tiene

$$r_A(n) = \frac{1}{2\pi i} \int_{|z|=r} \frac{(F_A(z))^l}{z^{n+1}} dz.$$

El método, original como hemos dicho de Hardy, Ramanujan y Littlewood, fué después notablemente mejorado por Vinogradov entre otras cosas con una simple observación. Y es que en la integral que aparece en el problema de las particiones no podemos tomar $r = 1$ pues la integral vale infinito, y tenemos una nueva variable a tener en cuenta. Vinogradov observó que para estimar $r_A(n)$, no hace falta considerar toda la sucesión A pues los enteros a_k son positivos, con lo que basta con considerar a_k con $k \leq n$, y considerar como función F la serie truncada

$$F(z) = \sum_{k \leq n} z^{a_k}.$$

De nuevo

$$r_A(n) = \frac{1}{2\pi i} \int_{|z|=r} \frac{(F(z))^l}{z^{n+1}} dz,$$

salvo que en esta ocasión, es una suma finita y podemos tomar $r = 1$ con lo que nos queda

$$r_A(n) = \int_0^{2\pi} (f(\alpha))^l e(-n\alpha) d\alpha,$$

con $f(\alpha) = F(e(\alpha))$.

3. El problema ternario de Goldbach.

El objetivo es demostrar que todo entero impar suficientemente grande se puede escribir como suma de tres primos. Este problema también se conoce como la conjetura débil de Goldbach. La conjetura fuerte afirma que cualquier entero par se puede escribir como suma de dos primos, y es inmediato ver que la fuerte implica la débil. (**Ejercicio 1**).

En este caso una primera opción sería tomar A como la sucesión de números primos. Sin embargo, teniendo en cuenta lo que mencionamos en la introducción, nos será mas conveniente tomar la función con pesos dados por la función de Von mangoldt

$$f(z) = \sum_{k \leq n} \Lambda(k) z^k.$$

Ciertamente el coeficiente n -ésimo de

$$f^3(z) = \sum_{k_1+k_2+k_3=n} \Lambda(k_1)\Lambda(k_2)\Lambda(k_3) z^n,$$

mide las formas de expresar n como suma de 3 potencias de primos. Teniendo en cuenta que hay muy pocas potencias de primos, esta cantidad será básicamente lo mismo que contar las representaciones de n como suma de tres primos. Concretamente se tiene lo siguiente: sea

$$\begin{aligned} r(N) &= \sum_{m_1+m_2+m_3=N} \Lambda(m_1)\Lambda(m_2)\Lambda(m_3), \\ R(N) &= \sum_{p_1+p_2+p_3=N} \log(p_1)\log(p_2)\log(p_3). \end{aligned}$$

Lema 1. $|r(N) - R(N)| \leq N^{3/2}(\log N)^3$

Prueba: Primero notamos que

$$0 \leq r(N) - R(N) = \sum_{m_1+m_2+m_3=N} \Lambda(m_1)\Lambda(m_2)\Lambda(m_3) \leq (\log N)^3 \sum_{m_1^k+m_2+m_3=N} 1$$

donde $k \geq 2$, y $0 \leq m_2, m_3 \leq N$. Así pues tenemos $N^{1/k} \leq N^{1/2}$ formas de escoger m_1, y N formas de escoger m_2, y una vez fijados m_1 y m_2, m_3 esta fijo. Con lo que la última suma esta acotada por $N^{3/2}$ de donde se sigue el resultado.

La aproximación anterior nos será de utilidad siempre y cuando el número de representaciones de un entero como suma de 3 primos sea asintóticamente mayor que $N^{3/2}$. Concretamente el teorema que vamos a demostrar es el siguiente resultado.

Teorema 2. *(Vinogradov) Cualquiera que sea $A > 0$, se tiene*

$$r(N) = \frac{1}{2}\mathfrak{S}(N)N^2 + O\left(\frac{N^2}{(\log N)^A}\right),$$

con

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

No tenemos más que cancelar los pesos para obtener

Corolario 3. *Sea $\mathfrak{r}(N)$ el número de representaciones de N como suma de tres primos. Entonces*

$$\mathfrak{r}(N) = \frac{1}{2}\frac{\mathfrak{S}(N)N^2}{(\log N)^3} + o\left(\frac{N^2}{(\log N)^3}\right)$$

cualquiera que sea $A > 0$.

Es importante observar que para N par $\mathfrak{S}(N) = 0$. Notese que cualquier entero par no se podrá expresar como suma de tres primos, salvo si alguno es $p = 2$, con lo que $\mathfrak{S}(N) \neq 0$ demostraría la conjetura fuerte de Goldbach para N suficientemente grande. Por otro lado, si N es impar efectivamente el primero es el término principal. Obsérvese que en ese caso teniendo en cuenta

$$\prod_{n\leq k}\left(1-\frac{1}{n^2}\right) = \prod_{n\leq k}\left(\frac{n^2-1}{n^2}\right) = \frac{1}{2}\frac{k+1}{k},$$

lo que se puede probar por inducción, obtenemos

$$1 > \prod_{p|N}\left(1-\frac{1}{(p-1)^2}\right) > \prod_{n\geq 2}\left(1-\frac{1}{n^2}\right) = \frac{1}{2},$$

mientras que

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

con lo que $\frac{1}{2} < \mathfrak{S}(N) < 2$ para cualquier N.

4. Prueba del teorema 2.

Como hemos mencionado, la prueba se basa en el Método del círculo, es decir, partimos de la fórmula de Cauchy

$$r(n) = \int_0^1 F(\alpha)e(-n\alpha)d\alpha,$$

donde $e(\alpha) = e^{2\pi i\alpha}$, y

$$F(\alpha) = f(e(\alpha)),$$

valida para cualquier $n \leq N$. Para obtener el comportamiento asintótico de la integral, lo primero que debemos hacer es definir los arcos mayores y los arcos menores.

Definición 4. *Sea $B > 0$.*

a) (Arcos Mayores) Sean $1 \leq a \leq q \leq (\log N)^B$, dos enteros tal que $(a, q) = 1$. Consideramos el conjunto $\mathfrak{M}(a,q) = \left\{\alpha : \left|\frac{a}{q} - \alpha\right| < \frac{(\log N)^B}{N}\right\}$. El conjunto de arcos mayores es

$$\mathfrak{M} = \cup_{(a,q)=1}\mathfrak{M}(a,q)$$

b) (Arcos Menores) El conjunto de arcos menores es $\mathfrak{m} = [0,1] \setminus \mathfrak{M}$.

Es quizas interesante observar que se llaman arcos mayores, pues de alli saldrá el término principal para nuestro teorema. Sin embargo, dados $1 \leq a_1 \leq q_1 \in \mathfrak{M}(a_1, q_1)$, $1 \leq a_2 \leq q_2 \in \mathfrak{M}(a_2, q_2)$, trivialmente se tiene

$$\left| \frac{a_1}{q_1} - \frac{a_2}{q_2} \right| \geq \frac{1}{q_1 q_2} > (\log N)^{-2B},$$

con lo que la mayor parte del circulo unidad corresponde a arcos menores. El resto de estas notas se dedica a la estimación por separado de la contribución a la integral por los arcos mayores y los arcos menores

4.1. Arcos Mayores. La aportación depende de la cancelación que aparece en el polinomio trigonométrico. Ahora bien, al haber considerado números muy cercanos a $\frac{a}{q}$, el comportamiento en cada $\mathfrak{M}(a, q)$ será muy parecido al valor de la función en el racional $\frac{a}{q}$. Así pues, la cancelación depende de entender los enteros en congruencias módulo q. La forma de distinguir congruencias módulo un entero dado es a través de los caracteres de Dirichlet. Estos caracteres son funciones completamente multiplicativas q periódicas $\chi_m : \mathbb{Z} \to \mu_q$, con $(0 \leq m < \varphi(q))$, con imagen en las raices q-ésimas de la unidad y que se definen para q primos como $\chi_m(k) = e(\frac{am}{q-1})$ para enteros $(k, q) = 1$, y $\chi_m(k) = 0$ si $(k, q) > 1$, donde $g^a \equiv k \pmod{q}$ y $< g >= (\mathbb{Z}/q\mathbb{Z})^*$. Las congruencias módulo q aparecen gracias a las fórmulas de ortogonalidad

$$\sum_{0 \leq m < \varphi(q)} \chi_m(k) = \begin{cases} \varphi(q) & \text{si } k \equiv 1 \pmod{q} \\ 0 & \text{si } k \not\equiv 1 \pmod{q}. \end{cases}$$

Dichas fórmulas permiten escribir (**Ejercicio 2**)

$$\frac{1}{\varphi(q)} \sum_{0 \leq m < \varphi(q)} \chi_m(k) \tau(\overline{\chi}_m) = \begin{cases} e(k/q) & \text{si } (k, q) = 1 \\ 0 & \text{si } (k, q) > 1, \end{cases} \tag{4}$$

donde

$$\tau(\chi) = \sum_{1 \leq k \leq q} \chi(k) e(k/q).$$

es la suma de Gauss asociada a χ. El objetivo es sustituir (4) en $F(\alpha)$. Para ello, primero notamos que

$$F(\alpha) = \sum_{k \leq N} \Lambda(k) e(\alpha k) = \sum_{\substack{k \leq N \\ (k,q)=1}} \Lambda(k) e\left(\left(\frac{a}{q} + \beta \right) k \right) + O\left((\log N)^2 \right),$$

pues la aportación de los términos con divisor común con q viene de un factor primo divisor de q y tiene como mucho $\log q \ll \log N$. (**Ejercicio 3.**)

Sustituyendo ahora $e(a/q)$ por su valor en (4) queda (**Ejercicio 4**.)

$$F(\alpha) = \frac{1}{\varphi(q)} \sum_{0 \leq m < \varphi(q)} \chi_m(a) \tau(\overline{\chi}_m) \sum_{\substack{k \leq N \\ (k,q)=1}} \chi_m(k) \Lambda(k) e(\beta k) + O\left((\log N)^2 \right). \tag{5}$$

La primera suma ya solo depende de a y q, mientras que en la segunda, tenemos una parte aritmética y una parte analítica con β pequeño, con lo que tendremos que estudiar ambos términos por separado. Para ello utilizamos integración por partes

Lema 5. *(Sumación por partes) Sea $S(n) = \sum_{k\leq n} a_k$. Entonces*

$$\sum_{n\leq x} f(n)a_n = f(x)S(x) - \int_{t=1}^{x} S(t)f'(t)dt.$$

Vamos a denotar

$$\psi(N,\chi) = \sum_{k\leq N} \chi(k)\Lambda(k). \tag{6}$$

Entonces, por el lema anterior

$$\sum_{\substack{k\leq N\\(k,q)=1}} \chi_m(k)\Lambda(k)e(\beta k) = \psi(N,\chi_m)e(\beta N) - 2\pi i\beta\int_1^N \psi(t,\chi_m)e(\beta t)dt \tag{7}$$

La función $\psi(N,\chi)$ no es más que la descripción analítica de la distribución de los números primos en congruencias. Concretamente, El Teorema de los números primos en progresiones aritméticas dice lo siguiente:

Teorema 6. *Sea $C > 0$, $q \leq (\log x)^C$ y χ un caracter modulo q. Entonces*

$$\psi(x,\chi) = \delta_\chi x + O\left(xe^{-C(\log x)^{1/2}}\right),$$

donde $\delta_\chi = 0$ si χ no es principal y 1 si $\chi = \chi_0$ es el caracter principal módulo q.

Asi pues, usanto el Teorema 6 en (7) queda para cualquier caracter no principal (**Ejercicio 5**).

$$\sum_{\substack{k\leq N\\(k,q)=1}} \chi_m(k)\Lambda(k)e(\beta k) = O\left((1+|\beta|N)Ne^{-C(\log N)^{1/2}}\right),$$

Por otro lado, la aportación que viene del caracter principal será,

$$\begin{aligned}\sum_{\substack{k\leq N\\(k,q)=1}} \chi_0(k)\Lambda(k)e(\beta k) &= Ne(\beta N) - 2\pi i\beta\int_1^N te(\beta t)dt + O\left(\frac{(1+|\beta|N)N}{e^{C(\log N)^{1/2}}}\right)\\ &= \sum_{k\leq N} e(k\beta) + O\left(\frac{(1+|\beta|N)N}{e^{C(\log N)^{1/2}}}\right),\end{aligned}$$

usando de nuevo sumación por partes. Agrupando ambos términos en (5) queda

$$\begin{aligned}F(\alpha) &= \frac{1}{\varphi(q)}\tau(\chi_0)\left(\sum_{k\leq N} e(k\beta) + O\left(\frac{(1+|\beta|N)N}{e^{C(\log N)^{1/2}}}\right)\right) +\\ &+ O\left(\frac{1}{\varphi(q)}\frac{(1+|\beta|N)N}{e^{C(\log N)^{1/2}}}\sum_{0<m<\varphi(q)}|\tau(\overline{\chi}_m)|\right)\end{aligned}$$

y teniendo en cuenta que $|\tau(\chi)| \leq q$, queda

$$F(\alpha) = \frac{1}{\varphi(q)}\tau(\chi_0)\sum_{k\leq N} e(k\beta) + O\left(q\frac{(1+|\beta|N)N}{e^{C(\log N)^{1/2}}}\right)$$

Observese que para β pequeño, esperamos que el primer sumando sea el término principal. Ademas, este término ya no contiene la aritmética de los números primos sino que es una suma sobre todos los enteros, con lo que será más fácil de controlar.

Pero antes, deberíamos probar que las sumas de Gauss no se anulan para el caracter principal. En realidad se tiene el siguiente lema valido para las sumas generales de Ramanujan

$$c_q(n) = \sum_{\substack{(a,q)=1\\ a\leq q}} e(an/q),$$

para cualquier $n \in \mathbb{N}$. Observese que $\tau(\chi_0) = c_q(1)$.

Lemma 1. *$c_q(n)$ cumple lo siguiente*

a) $c_q(n)$ es multiplicativa en q.

b)

$$c_p(n) = \begin{cases} p-1 & si\ p|n \\ -1 & si\ p \nmid n \end{cases}$$

c) $c_q(1) = \mu(q)$.

Demostración.

a) Por el Teorema Chino del Resto si $(q_1, q_2) = 1$ entonces para cada $(a, q_1q_2) = 1$ se tiene una y solo una pareja $(a_1, q_1) = 1, (a_2, q_2) = 1$, y $0 \leq a_1 \leq q_1$, $0 \leq a_2 \leq q_2$, tal que $a = a_1q_2 + a_2q_1$ con lo que

$$\begin{aligned} c_{q_1q_2}(n) &= \sum_{\substack{(a,q_1q_2)=1\\ a\leq q_1q_2}} e(an/(q_1q_2)) = \sum_{\substack{(a_1,q_1)=1\\ a_1\leq q_1}} e(a_1n/q_1) \sum_{\substack{(a_2,q_2)=1\\ a_2\leq q_2}} e(a_2n/q_2) \\ &= c_{q_1}(n)c_{q_2}(n). \end{aligned}$$

b)

$$c_q(p) = \sum_{1\leq a\leq p-1} e(a/p) = \left(\sum_{0\leq a\leq p-1} (e(1/p))^a \right) - 1 = -1.$$

c) Por a) es suficiente comprobarlo para $q = p^r$ potencias de primos. Si q es primo, es b). Si q=p^r, con $r \geq 2$, entonces, teniendo en cuenta que cualquier residuo modulo q, $(a, q) = 1$ se puede escribir como $a = a_1 + a_2p$ con $1 \leq a_1 \leq p-1$, y $0 \leq a_2 < p^{r-1}$ se tiene

$$c_q(n) = \sum_{\substack{1\leq a_1\leq p-1\\ 0\leq a_2\leq p^{r-1}}} e((a_1+a_2p)/p^r) = \sum_{1\leq a_1\leq p-1} e(a_1/p^r) \sum_{0\leq a_2<p^{r-1}} (e(1/p^{r-1}))^{a_2} = 0.$$

Ya tenemos $F(\alpha)$ para poder integrar. El siguiente lema nos da una cota explícita de $S(\beta)$.

Lemma 2. *Para cualquier numero real α y $0 \leq n < m$, se tiene*

$$\sum_{n<k\leq m} e(\alpha k) \leq \text{mín}\{m-n, ||\alpha||^{-1}\},$$

donde $||\alpha||$ denota la distancia de α al entero más cercano.

Demostración. La primera desigualdad es trivial. Para la segunda, observamos que la suma no es mas que una serie geométrica de razón $e(\alpha)$ con lo que se tiene (**Ejercicio 6**)

$$\sum_{n<k\leq m} e(\alpha k) = \frac{e(([m]+1)\alpha) - e(([n]+1)\alpha)}{e(\alpha)-1} \leq \frac{1}{|\operatorname{sen}(\pi\alpha)|} \leq ||\alpha||^{-1}. \tag{8}$$

Utilizando la cota trivial obtenemos

$$F(\alpha)^3 = \frac{\mu(q)}{\varphi(q)^3} S(\beta)^3 + O\left(N^3 e^{-C\sqrt{\log N}}\right),$$

con lo que al integrar sobre los arcos mayores, se tiene para $Q = \frac{(\log N)^B}{N}$

$$\int_{\mathfrak{M}} F(\alpha)^3 e(-N\alpha) d\alpha \quad = \quad \left(\sum_{q\leq (\log N)^B} \frac{\mu(q)}{\varphi(q)^3} c_q(N)\right) I_Q$$

donde

$$I_Q = \int_{-1/Q}^{1/Q} S(\beta)^3 e(-N\beta) d\beta + O\left(N^2 e^{-C\sqrt{\log N}}\right).$$

Teniendo en cuenta la cota trivial $|c_q(N)| \leq \varphi(q)$, vemos que la suma es convergente. El siguiente lema nos da una cota para el error.

Lema 7. *Para todo* $0 < \varepsilon < 2^{-8}$ *y* $n > n_\varepsilon = (2\varepsilon^{-1}\log_2(1/\varepsilon))^{1/\varepsilon}$ *se tiene*

$$\varphi(n) > n^{1-\varepsilon}.$$

Demostración. Supongamos $\omega(n) = l$. Entonces

$$\varphi(n) = n\prod_{p|n}\left(1-\frac{1}{p}\right) > n\prod_{i=2}^{l+1}\left(1-\frac{1}{i}\right) = \frac{n}{l+1}. \tag{9}$$

Si $l \leq 2$, entonces $\varphi(n) > \frac{n}{3} > n^{1-\varepsilon}$ para todo $n > 3^{1/\varepsilon}$. En cualquier otro caso $n > 2^{l+1}$, con lo que

$$\frac{n}{l+1} > \frac{n}{\log_2(n)} > n^{1-\varepsilon},$$

siempre que $n^\varepsilon > \log_2(n)$ que es cierto para cualquier $n > n_\varepsilon$.

Sustituyendo en la suma queda

$$\left(\sum_{q\leq (\log N)^B} \frac{\mu(q)}{\varphi(q)^3} c_q(N)\right) = \sum_{q\geq 1} \frac{\mu(q)}{\varphi(q)^3} c_q(N) + O((\log N)^{-B+\varepsilon})$$

El sumando es una función multiplicativa, con lo que análogamente a la función zeta tenemos

$$\begin{aligned}\sum_{q\geq 1} \frac{\mu(q)}{\varphi(q)^3} c_q(N) &= \prod_p \left(\sum_{r\geq 0} \frac{\mu(p^r)}{\varphi(p^r)^3} c_{p^r}(N)\right) = \prod_p \left(1 - \frac{c_p(N)}{(p-1)^3}\right) \\ &= \prod_{p|N}\left(1-\frac{1}{(p-1)^2}\right)\prod_{p\nmid N}\left(1+\frac{1}{(p-1)^3}\right) = \mathfrak{S}(N).\end{aligned}$$

La parte analítica I_Q, se puede integrar facilmente. Primero observamos que

$$\int_0^1 S(\beta)^3 e(-N\beta)d\beta = I_Q + \int_{1/Q}^{1-1/Q} S(\beta)^3 e(-N\beta)d\beta$$

Por otro lado, por (8)

$$\int_{1/Q}^{1-1/Q} S(\beta)^3 e(-N\beta)d\beta = O\left(\int_{1/Q}^{1-1/Q} \frac{1}{\beta^3}d\beta\right) = O\left(Q^2\right)$$

Por último

$$\begin{aligned}\int_0^1 S(\beta)^3 e(-N\beta)d\beta &= \sum_{k\leq 3N}\sum_{k_1+k_2+k_3=k}\int_0^1 e((k-N)\beta)d\beta = \sum_{k_1+k_2+k_3=N} 1\\ &= \sum_{k_1\leq N} 1 \sum_{k_2+k_3=N-k_1} 1 = \sum_{k_1\leq N}(N-k_1) = \frac{N(N+1)}{2}.\end{aligned}$$

Agrupando todos los términos queda

$$I_{\mathfrak{M}} = \int_{\mathfrak{M}} F(\alpha)^3 e(-N\alpha)d\alpha = \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{(\log N)^{B-1}}\right).$$

4.2. Arcos menores. Nuestro objetivo por tanto es dar una cota superior de la integral

$$I_{\mathfrak{m}} = \int_{\mathfrak{m}} F(\alpha)^3 e(-N\alpha)d\alpha.$$

Trivialmente se tiene

$$|I_{\mathfrak{m}}| \leq \max_{\mathfrak{m}} |F(\alpha)| \int_0^1 |F(\alpha)|^2 d\alpha \ll \left(\max_{\mathfrak{m}} F(\alpha)\right) N(\log N)^2, \tag{10}$$

pues (**Ejercicio 7**)

$$\begin{aligned}\int_0^1 F(\alpha)\overline{F(\alpha)}d\alpha &= \sum_{0\leq k_1,k_2\leq N}\Lambda(k_1)\Lambda(k_2)\int_0^1 e((k_1-k_2)\alpha)d\alpha\\ &= \sum_{k\leq N}\Lambda(k)^2 \ll N(\log N)^2,\end{aligned}$$

con lo que el resto lo dedicaremos a encontrar una cota superior de $F(\alpha)$ en los arcos menores. De nuevo esta cota depende de la oscilación con lo que vamos a tomar racionales cercanos a α.

Teorema 8. *(Dirichlet)Para todo $X \geq 1$, y $\alpha \in [0,1]$ existen $(a,q) = 1$, $1 \leq a \leq q \leq X$ tal que*

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

Demostración. Sea $d = [X] + 1$. Si $\alpha j - [\alpha j] < \frac{1}{d}$, o $\alpha j - [\alpha j] > 1 - \frac{1}{d}$, para algún $1 \leq j \leq d$, entonces tomamos $q = j$, $a = [\alpha j]$, o $q = j$, $a = [\alpha j] + 1$. Si ningún j cumple ninguna de esas condiciones, entonces para todos los $j \leq d-1$ enteros menores que X, $\alpha j - [j\alpha]$ se encuentran en $[\frac{1}{d}, 1 - \frac{1}{d}]$, con lo que existen $1 \leq i < j \leq d$ tal que

$$|\alpha(j-i) - ([\alpha j] - [\alpha i]) = |\alpha j - [\alpha j] - (\alpha i - [\alpha i])| < \frac{1}{d}.$$

En ese caso $q = (j - i)$, $a = [\alpha j] - [\alpha i]$.

Así pues para acotar $F(\alpha)$ en los arcos menores, comparamos su valor con el del racional $\frac{a}{q}$ garantizado por el teorema anterior, con $(\log N)^B < q \leq Q$. Concretamente tenemos el siguiente resultado

Proposición 9. *Dados $(a, q) = 1$, $1 \leq q \leq N$ y $\left|\alpha - \frac{a}{q}\right| < \frac{1}{q^2}$, se tiene*

$$F(\alpha) \ll \left(\frac{N}{\sqrt{q}} + N^{4/5} + \sqrt{Nq}\right)(\log N)^4.$$

Demostración. La idea de la demostración se basa en localizar la cancelación de la suma trigonométrica $F(\alpha)$, que viene de la oscilación de la exponencial. Esta cancelación se puede entender gracias al Lema 2 en términos de la distancia al entero más cercano.

Ahora, lo que sabemos sobre α es que está cerca de un racional de denominador q por el Teorema 8, y pasar de un racional a un entero, pasa por multiplicar por un entero. Si multiplicamos por q el teorema es equivalente a decir que $|q\alpha - a| < \frac{1}{q}$. Teniendo en cuenta que querremos calcular sumas exponenciales con denominador q, vamos a interpretar la desigualdad anterior diciendo que los múltiplos de α, $n\alpha$ estarán cerca de un entero cuando n sea multiplo de q. Esto, de hecho, fuerza a que para cualquier otra congruencia de n módulo q $n\alpha$ se aleje suficientemente de los enteros. Concretamente tenemos la siguiente proposición.

Proposición 10. *Sea α, $X \geq 1$, $Y \geq 1$ números reales, y sean a, q enteros tal que $q \geq 1$, $(a, q) = 1$ y $|\alpha - \frac{a}{q}| < \frac{1}{q^2}$. Entonces*

$$S(X, Y, q) = \sum_{1 \leq n \leq X} \text{mín}\left(\frac{XY}{n}, ||n\alpha||^{-1}\right) \ll \left(\frac{XY}{q} + X + q\right)\log(2Xq).$$

Es decir, si la distancia de $n\alpha$ a un entero es pequeña, entonces es porque n es un múltiplo de q, y da el primer término. Para los que no son múltiplos de q la distancia es grande, y la suma está acotada por el número de sumandos. Observese la ganancia de dividir por q pues estaremos trabajando en los arcos menores de denominador grande.

Demostración. Antes de nada, observese que podemos suponer $0 \leq \alpha < 1$, pues si $\alpha = m + \beta$ para algún entero m y $0 \leq \beta < 1$, entonces $||(n\alpha)|| = ||(n\beta)||$.

El caso $q = 1$ es trivial (**Ejercicio 8**), así que suponemos que $q \geq 2$. Por lo mencionado anteriormente dividimos la suma en congruencias módulo q y nos queda

$$S(X, Y, q) \leq \sum_{n \leq X/q} \sum_{j=1}^{q} \text{mín}\left(\frac{XY}{j + nq}, ||(j + nq)\alpha||^{-1}\right).$$

Vamos a analizar cada término por separado. Será conveniente incluir la notación $\rho = q^2\alpha - qa$. Nótese que $|\rho| < 1$, por el Teorema de Dirichlet. En términos de ρ podemos escribir

$$(j + nq)\alpha = \frac{e_n + aj}{q} + \frac{\{\alpha n q^2\}}{q} + \frac{j\rho}{q^2}, \tag{11}$$

donde $e_n = [\alpha n q^2]$. En el caso particular $n = 0$ y $j \leq q/2$ se tiene

$$j\alpha = \frac{ja}{q} + \frac{\rho j}{q^2}$$

con lo que

$$||j\alpha|| \geq \frac{||(ja/q)||}{2}, \tag{12}$$

y

$$\sum_{j=1}^{q/2} \text{mín}\left(\frac{XY}{j+nq}, ||(j+nq)\alpha||^{-1}\right) \leq \sum_{j=1}^{q/2} ||(j+nq)\alpha||^{-1} \leq 2\sum_{j=1}^{q/2} \frac{q}{j} \leq 2q\log q, \tag{13}$$

ya que $ja \not\equiv 0 \pmod q$, y si $j \neq i$ entonces $ja \not\equiv ia \pmod q$. En cualquier otro caso se tiene la desigualdad

$$q(n+1) \leq 2(qn+j), \tag{14}$$

Ademas (12) será casi siempre cierta. Concretamente para cada n fijo, por (11), se tiene

$$||(j+nq)\alpha|| \geq ||(e_n+aj)/q|| - \frac{2}{q} \geq ||(e_n+aj)/q||/3 \tag{15}$$

excepto si $e_n + aj \equiv 0, \pm 1, \pm 2 \pmod q$, que pasa exactamente para 5 valores de j, independientemente de n y q , pues $e_n + aj \not\equiv e_n + ai \pmod q$ si $j \neq i$. Utilizando (15), salvo en esos 5 casos que utilizaremos (14), junto con (13) obtenemos

$$\begin{aligned} S(X,Y,q) \quad \leq \quad & \sum_{j=1}^{q/2} \text{mín}\left(\frac{XY}{j+nq}, ||(j+nq)\alpha||^{-1}\right) + 10XY \sum_{n\leq X/q} \frac{1}{q(n+1)} \\ & +3q \sum_{n\leq X/q} \sum_{j=1}^{q} \frac{1}{j} \ll \left(\frac{XY}{q} + X + q\right)\log(2Xq) \end{aligned}$$

Así pues para utilizar la proposición anterior usaremos Lema 2, pero antes debemos relacionar $F(\alpha)$ con una suma no en α sino sobre múltiplos de α. Este es exactamente el arte de la convolución. Vamos a considerar las series de Dirichlet

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s} \qquad -\zeta'(s) = \sum_{n\geq 1} \frac{\log n}{n^s} \qquad -\frac{\zeta'(s)}{\zeta(s)} = \sum_{n\geq 1} \frac{\Lambda(s)}{n^s}, \tag{16}$$

y los polinomios trigonométricos

$$G(s) = \sum_{n\leq X} \frac{\mu(n)}{n^s} \qquad H(s) = \sum_{n\leq X} \frac{\Lambda(n)}{n^s}.$$

El parámetro X es necesario pues para aplicar la Proposición 10 debemos tener un número controlado de sumandos, que dependerá del tamaño de N, como veremos después. La identidad siguiente es trivial

$$0 = -\zeta' G - \zeta G H - \zeta G\left(-\frac{\zeta'}{\zeta} - H\right),$$

y por la identidad de convolución tenemos

$$0=\sum_{b\geq 1}\frac{1}{b^s}\sum_{\substack{nm=b\\ m\leq X}}\mu(m)\log n-\sum_{b\geq 1}\frac{1}{b^s}\sum_{\substack{nm=b\\ m\leq X^2}}C_m-\sum_{b\geq 1}\frac{1}{b^s}\sum_{\substack{nm=b\\ X<n}}\tau_m\Lambda(n),$$

donde

$$C_m=\sum_{\substack{k|m\\ k,m/k\leq X}}\mu(k)\Lambda(m/k),\qquad \tau_m=\sum_{\substack{d|m\\ d\leq X}}\mu(d).$$

Una serie de Dirichlet es básicamente la transformada tipo Fourier de una serie de potencias, con lo que solo puede ser cero si tiene todos los coeficientes 0 y por tanto

$$0=\sum_{\substack{nm=b\\ m\leq X}}\mu(m)\log n-\sum_{\substack{nm=b\\ m\leq X^2}}C_m-\sum_{\substack{nm=b\\ X<n}}\tau_m\Lambda(n).$$

Notese que ya tenemos los coeficientes escrito como producto de enteros. Para pasar esta identidad universal a $F(\alpha)$, multiplicamos por $e(b\alpha)$, y sumamos en b. Observese que $F(\alpha)$ aparecerá en la última suma utilizando que $\tau_1=1$ por (1). Así pues sumando a ambos lados $\sum_{X<b\leq N}\Lambda(b)e(\alpha b)$ obtenemos

$$\begin{aligned}\sum_{X<b\leq N}\Lambda(b)e(\alpha b) &= \sum_1^N e(\alpha b)\sum_{\substack{nm=b\\ m\leq X}}\mu(m)\log n-\sum_1^N e(\alpha b)\sum_{\substack{nm=b\\ m\leq X^2}}C_m-\\ &\quad-\left(\sum_1^N e(\alpha b)\sum_{\substack{nm=b\\ X<n}}\tau_m\Lambda(n)-\sum_{X<b\leq N}\Lambda(b)e(\alpha b)\right)\end{aligned}$$

La parte izquierda es trivialmente

$$\sum_{X<b\leq N}\Lambda(b)e(\alpha b)=F(\alpha)+O(\sqrt{N}\log N),$$

para cualquier $X\leq\sqrt{N}$. En la parte derecha basta invertir el orden de sumación y queda

$$\begin{aligned}F(\alpha) &= \sum_{m\leq X}\sum_{n\leq N/m}\mu(m)\log n e(\alpha mn)-\sum_{m\leq X^2}\sum_{n\leq N/m}C_m e(\alpha mn)-\\ &\quad-\sum_{X<m\leq N}\sum_{X<n\leq N/m}\tau_m\Lambda(n)e(\alpha mn)+O(\sqrt{N}\log N)\\ &= S_1-S_2-S_3+O(\sqrt{N}\log N),\end{aligned}$$

donde hemos usado que $\tau_m=0$ si $1<m\leq X$, y $\tau_1=1$ por (1). En lo que resta deberemos acotar cada una de las sumas S_1,S_2,S_3 usando la Proposición 10. Ahora

bien

$$\begin{aligned} S_1 &\leq \sum_{m\leq X}\left|\sum_{n\leq N/m} e(\alpha mn)\log n\right| = \sum_{m\leq X}\left|\int_1^{N/m}\sum_{t<n\leq N/m} e(\alpha mn)\frac{dt}{t}\right| \\ &\leq \sum_{m\leq X}\int_1^{N/m}\left|\sum_{t<n\leq N/m} e(\alpha mn)\right|\frac{dt}{t} \leq \log N \sum_{m\leq X} \text{mín}\left(\frac{N}{m}, ||\alpha m||^{-1}\right) \\ &\ll (\log N)\log(Xq)\left(\frac{N}{q}+X+q\right), \end{aligned}$$

en donde hemos utilizado tanto la Proposición 10 como el Lema 2.

La suma S_2 se trata de forma similar. Concretamente por definición se tiene la desigualdad $|C_m| \leq \sum_{d|m}\Lambda(d) = \log m$ por (2) con lo que analogamente al caso anterior se tiene

$$|S_2| \leq 2\log X \sum_{m\leq X^2}\left|\sum_{n\leq N/m} e(\alpha mn)\right| \ll (\log(Xq))^2\left(\frac{N}{q}+X^2+q\right).$$

En la suma S_3 el rango de sumación es demasiado grande, por lo que debemos dividir la suma en intervalos diádicos con lo que los términos en la suma interna son comparables y se puede controlar mejor la cancelación. Es importante observar primero que si $m > N/X$ la suma interna es cero. Vamos a considerar $k = \log_2(N/X^2)$, $X_l = 2^l X$ con lo que

$$S_3 = \sum_{l=0}^{k} S_{3,l}$$

donde

$$S_{3,l} = \sum_{m=X_l}^{2X_l}\sum_{X<n\leq N/m} \tau_m\Lambda(n)e(\alpha mn).$$

Para acotar $S_{3,l}$ debemos separar primero la aportación de τ_m. Para ello utilizamos Cauchy-Schwartz, con lo que

$$|S_{3,l}|^2 \leq \left(\sum_{m=X_l}^{2X_l}\tau_m^2\right)\sum_{X_l}^{2X_l}\left|\sum_{X<n\leq N/m}\Lambda(n)e(\alpha mn).\right|^2 \tag{17}$$

En la primera suma vamos a despreciar la oscilación de $\mu(n)$ y utilizar la cota trivial $\tau_m \leq d(m)$. El siguiente lema nos da la cota necesaria.

Lema 11.

$$\sum_{n\leq x} d^2(n) \ll X(\log X)^3.$$

Demostración. Se tiene para cualquier $x \geq 3$,

$$\sum_{n\leq x} d(n) = \sum_{n\leq x}\sum_{k|n} 1 = \sum_{k\leq x}\sum_{n\leq x/k} \leq x\sum_{k\leq x}\frac{1}{k} \leq 2x\log x,$$

con lo que

$$\begin{aligned}\sum_{n\leq x}(d(n))^2 &= \sum_{n\leq x}\sum_{k|n}d(n)=\sum_{k\leq x}\sum_{m\leq x/k}d(km)\\ &\leq \sum_{k\leq x}d(k)\sum_{m\leq x/k}d(m)\leq 2x\log x\sum_{k\leq x}\frac{d(k)}{k}\\ &< 4x(\log x)^3,\end{aligned}$$

En donde hemos utilizado el Lema 5 para la última desigualdad con $f(x)=1/x$ y $a_n=d(n)$. Así pues, falta acotar la segunda suma en (17). Ahora bien

$$\begin{aligned}\sum_{m=X_l}^{2X_l}\left|\sum_{X<n\leq N/m}\Lambda(n)e(\alpha mn).\right|^2 &= \sum_{m=X_l}^{2X_l}\sum_{X<n,k\leq N/m}\Lambda(n)\Lambda(k)e(\alpha m(n-k))\\ &\leq \sum_{X<n,k\leq N/X_l}\Lambda(n)\Lambda(k)\sum_{m=X_l}^{2X_l}e(\alpha m(n-k))\\ &\leq (\log N)^2\sum_{X<n,k\leq N/X_l}\text{mín}\left(X_l,||\alpha(n-k)||^{-1}\right).\end{aligned}$$

Para cada $d\leq N/X_l$ hay como mucho N/X_l parejas $n-k=d$. Teniendo en cuenta que $d\leq n\leq N/X_l$ se tiene $X_l\leq N/d$ con lo que la desigualdad anterior queda, separando el término diagonal $n=k$,

$$\begin{aligned}&\leq (\log N)^2\left(N+\frac{N}{X_l}\sum_{1\leq d\leq N/X_l}\text{mín}\left(\frac{N}{d},||\alpha d||^{-1}\right)\right)\\ &\leq (\log(qN))^3\left(N+\frac{N^2}{qX_l}+\frac{N^2}{X_l^2}+\frac{Nq}{X_l}\right).\end{aligned}$$

Juntando ambas estimaciones obtenemos

$$|S_{3,l}|\ll X_l^{1/2}(\log X_l)^{3/2}(\log(qN))^{3/2}\left(N^{1/2}+\frac{N}{\sqrt{qX_l}}+\frac{N}{X_l}+\frac{\sqrt{Nq}}{\sqrt{X_l}}\right)$$

y sumando en $0\leq l\leq \log N/X^2$, queda

$$|S_3|\leq(\log(qN))^4\left(\frac{N}{\sqrt{X}}+\frac{N}{\sqrt{q}}+\sqrt{Nq}\right).$$

Escogemos X para optimizar los errores en S_1,S_2,S_3, es decir, $X^2=N/\sqrt{X}$, es decir, $X=N^{2/5}<\sqrt{N}$, con lo que

$$F(\alpha)\ll(\log(qN))^4\left(\frac{N}{\sqrt{q}}+N^{4/5}+\sqrt{Nq}\right),$$

Lo que termina la demostración de la proposicion. Ahora bien, teniendo en cuenta que estamos en los arcos menores, se tiene $(\log N)^B<q<Q=\frac{N}{(\log N)^B}$, con lo que

$$F(\alpha)\ll N(\log N)^{4-B/2}.$$

Usando dicha cota en (10), queda

$$|I_{\mathfrak{m}}|\ll N^2(\log N)^{6-B/2},$$

y por tanto

$$r(n) = I_{\mathfrak{M}} + I_{\mathfrak{m}} = \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{(\log N)^A}\right)$$

para cualquier $A > 0$ escogiendo $B = 2A + 12$.

Referencias

El Método del círculo

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

[2] Chamizo, F., Cristóbal, E., Ubis, A., El método del círculo, La gaceta de la RSME, Vol. 9.2, 465-481, 2006.

El Teorema de Vinogradov

[3] Senén, A, Vinogradov´s theorem and the Goldbach conjecture, TFM, 2015

[4] Wong, P, Vinogradov´s theorem and its generalizations on primes in arithmetic progressions, TFM, 2009.

[5] Nathanson, M. B. Additive number theory. The classical bases. Graduate Texts in Mathematics, 164. Springer-Verlag, New York, 1996. xiv

[6] Hardy, G.H, Littlewood, J. E. Some problems of partitio numerorum,. III: On the expression of a number as a sum of primes. Acta Math. 44-1,1–70, 1923.

[7] Petrow, I. N. Vinogradov´s three primes theorem, TFM, 2008.

[8] Deshouillers J.-M., Effinger, G., Te Riele, H., Zinovieva, D. , A complete Vinogradov´s three primes theorem under the Riemann hypothesis, Electronic research announcements of the AMS, 3, 99–104 (September 17, 1997)

Libros de Teoría Analítica de Números

[9] Davenport, H. Multiplicative number theory, Third edition. Revised and with a preface by Hugh L. Montgomery. Graduate Texts in Mathematics, 74. Springer-Verlag, New York, 2000.

[10] Iwaniec, H.; Kowalski, E., Analytic number theory. American Mathematical Society Colloquium Publications, 53. American Mathematical Society, Providence, RI, 2004.

[11] Montgomery, H.L. Ten lectures on the interface between analytic number theory and harmonic analysis. CBMS Regional Conference Series in Mathematics, 84. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 1994.

Departamento de Matemáticas, Universidad Politécnica de Madrid, Madrid, Spain
Email address: jorge.urroz@upm.es