
Universidad Autónoma de Madrid

Facultad de Ciencias



Departamento de Matemáticas


---

Trabajo de fin de máster

# Sumando primos ¿hay tres sin dos?


*Autor:*
Rafael Tesoro

rafael.tesoro@estudiante.uam.es

*Tutor:*
Fernando Chamizo

fernando.chamizo@uam.es


---

12 de septiembre de 2011

# Resumen

En este trabajo se demuestra el teorema de Vinogradov, el cual afirma que cualquier entero impar suficientemente grande es la suma de tres primos. La demostración es completa salvo los resultados clásicos sobre la densidad y distribución de los números primos en progresiones aritméticas, que solamente se enuncian.

Previamente se introduce el método del círculo y los ingredientes necesarios para poder usarlo en el estudio de las representaciones de enteros como sumas de primos.

Se intercalan un par de argumentos heurísitos que sugieren una fórmula asintótica para las representaciones con dos primos. Se prueba también que la densidad de las excepciones a la conjetura binaria de Goldbach tiende a cero, y se concluye resaltando la dificultad de resolver la conjetura con el método del círculo.

*A mi padre*

## Agradecimientos

Agradezco a Fernando Chamizo que me sugiriese el tema de este trabajo fin de máster. Sus orientaciones, explicaciones y comentarios han enriquecido notablemente el resultado final.

Recuerdo con agrado mi asistencia a las clases de Antonio Córdoba, que hicieron que desde entonces me fascine la Teoría de Números. "De casi todo hace veinte años", decía Jaime Gil de Biedma. Más de veinte han pasado desde que comenzó mi amistad con Javier Cilleruelo quien sigue hoy, amablemente, alentado mi veterana pasión por las matemáticas.

Gracias a Leli por el dibujo de la palomas. Y por su paciencia y su apoyo que siempre mostraron una cariñosa tendencia a infinito mientras yo preparé este trabajo.

# Índice general

# Índice de figuras

# Prólogo

Algunos problemas aditivos en Teoría de Números son notoriamente difíciles. Sin embargo otros problemas estrechamente relacionados, que parecen a primera vista igual de arduos, sí han sido resueltos. Un ejemplo notable es el TEOREMA DE VINOGRADOV que afirma que cualquier entero *impar* suficientemente grande es la suma de *tres* primos.

Creo que la recompensa de hacer una incursión de decenas de páginas al territorio de la representación de los números naturales como sumas de primos incluye disfrutar comprendiendo un buen número de ideas perspicaces y culminar con la ascensión al *pico Vinogradov*, contemplando muy de cerca la aún hoy inaccesible cumbre CONJETURA DE GOLDBACH. Si el famoso problema de Goldbach fuera resuelto probablemente se revelaría algo nuevo acerca de los números primos [I-K, pág. 4].

En resumen el contenido de este trabajo es el siguiente:

- El capítulo 1 contiene un aperitivo de historia y un primer argumento heurístico favorable a la conjetura de Goldbach.
- Para continuar abriendo boca, el capítulo 2 introduce en pocas páginas el método del círculo.
- En el capítulo 3 se exponen los principales ingredientes y herramientas que se utilizan en el análisis de los arcos mayores que se hace en el capítulo posterior.
- En el capítulo 4 se encuentra el candidato a término principal en la estimación asintótica para la cantidad de representaciones de un número entero como suma de varios números primos.
- Los esfuerzos culminan en el capítulo 5 cuando, tras el estudio de los arcos menores, se completa la demostración del teorema de Vinogradov y se añade el resultado de que casi todo número par es suma de dos primos.
- En el capítulo 6 se recapitula acerca de la dificultad de resolver, con el método del círculo, precisamente la conjetura binaria de Goldbach.

> «El escritor actúa también como un rumiante: a todo lo que ha visto, todo lo que ha tocado y oído le da vueltas y más vueltas» JOSE LUIS SAMPEDRO

Durante mi particular bovino empeño he pastado, en esfuerzo placentero la mayoría de las veces, a lo largo de diversas secciones de los libros y los artículos que aparecen en la Bibliografía. Los prerrequisitos específicos para analizar las sumas de primos por el método del círculo se abordan en los capítulos 2 y 3 y en la sección 5.1; parece razonable suponer que el resto del bagaje necesario para leer este trabajo se adquiere durante los estudios de Grado de Matemáticas.

Termino animado por el deseo de Quevedo: «Dios te libre, lector, de prólogos largos y de malos epítetos» que he procurado cumplir en cada epígrafe de lo que sigue.

## Notación

En muchas ocasiones hablaremos de aproximaciones y para distinguirlas cualitativamente usaremos ciertos símbolos que recordamos a continuación. Si $f$ y $g$ son dos funciones reales con valores reales o complejos, al compararlas cuando $x \to \infty$ escribiremos

$f = O(g)$ o bien $f \ll g$ si existe $C > 0$ constante *implícita* tal que $|f(x)| \leq C\,|g(x)|$ en todo el dominio de $f$. Para resaltar el caso en que $C$ dependa de $a, b, \ldots$ escribiremos $f \ll_{a,b,\ldots} g$.

$f \sim g$ cuando $(f/g)(x) \overset{x\to\infty}{\longrightarrow} 1$ y $f = o(g)$ si $(f/g)(x) \overset{x\to\infty}{\longrightarrow} 0$.

Exhibiremos *estimaciones* que escribimos, como es habitual, con el patrón siguiente

$$F = P + Err = P\left(1 + \frac{Err}{P}\right),$$

en donde $F$ es la función que buscamos aproximar por otra función $P$ y $Err$ representa el error cometido. La fórmula de las funciones $F$ y $P$ será bien conocida y bastará acotar con precisión el término de error por otra función $C$ de modo que $F - P = Err \ll C$. En muchos casos además $C = o(P)$ y entonces $P$ será la parte principal prevaleciendo sobre $Err$, todo lo cual implicará en conclusión la *estimación asintótica* $F \sim P$.

Convendremos que $\mathbb{N} = \{1, 2, \ldots\} = \mathbb{Z}^+$ no incluye al número 0.

Utilizaremos $:=$ para resaltar que es definición en lugar de igualdad $=$

Para confirmar el significado de otros símbolos consultar la página siguiente.

| Expresión | Significado | Referencia |
|---|---|---|
| $A := B$ | definición de $A$ como igual a $B$ | |
| $(n, m)$ | máximo común divisor de $n$ y $m$ | |
| $a \equiv b \pmod{c}$ | $a - b$ es múltiplo de $c$ | |
| $\mid A \mid$ | cardinal del conjunto $A$ | |
| $\# A$ | cardinal del conjunto $A$ | |
| $\lvert x \rvert$ | valor absoluto del número $x$ | |
| $\lfloor x \rfloor$ | parte entera de $x$ | |
| $\{x\}$ | parte fraccionaria de $x$ | |
| $\Vert x \Vert$ | distancia de $x$ al entero más cercano | pág. 45 |
| $f \sim g$ | $f(x)/g(x) \to 1$ cuando $x \to \infty$ | pág. xii |
| $O, o, \ll, \ll_{a,b,\ldots}$ | | pág. xii |
| $Err$ | término de error en una estimación | pág. xii |
| $\mathcal{P}$ | conjunto de los números primos | pág. 1 |
| $r_2(N)$ | representaciones binarias de $N$ | pág. 1 |
| $r(n; k, \mathcal{A})$ | representaciones de $n$ con $k$ sumandos de $\mathcal{A} \subset \mathbb{N}$ | pág. 9 |
| $R(N; k, \mathcal{P})$ | representaciones de $N$ con $k$ sumandos de $\mathcal{P}$ y peso $\log p$ | pág. 36 |
| $e\,(x)$ | $\exp(2\pi i x)$ | pág. 10 |
| $\pi(x)$ | cantidad de números primos menores que $x$ | |
| $\mu(n)$ | función de Möbius | pág. 16 |
| $\phi(n)$ | función de Euler | pág. 17 |
| $\Lambda(n)$ | función de Von Mangoldt | pág. 20 |
| $\psi(x)$ | potencias de primos menores que $x$, con peso $\log p$ | pág. 26 |
| $c_q(n)$ | sumas de Ramanujan | pág. 21 |
| $\chi$ | caracteres de Dirichlet | pág. 26 |
| $\pi(x; a, q)$ | primos menores que $x$ con residuo $a$ módulo $q$ | pág. 30 |
| $\psi(x, \chi)$ | | pág. 30 |
| $\mathcal{M}$ | arcos mayores para representaciones con sumandos primos | pág. 39 |
| $\mathfrak{m}$ | los arcos menores: $[0, 1] \setminus \mathcal{M}$ | |
| $\mathfrak{S}_k(N)$, $\mathfrak{S}_k(N, x)$ | la serie singular para representaciones con sumandos primos | pág. 47 |
| $E(x)$ | número de excepciones a la conjetura de Goldbach | pág. 69 |
| $I_A(N; n)$ | | pág. 69 |
| $\mathbb{P}(A)$ | probabilidad del suceso $A$ | |
| $\complement A$ | suceso/conjunto complementario de $A$ | |
| $A \setminus B$ | elementos de $A$ que no están en $B$ | |
| $A \biguplus B$ | es $A \bigcup B$, cuando $A \cap B = \emptyset$ | |
| $\mathbb{C}[X]$ | anillo de polinomios con coeficientes en $\mathbb{C}$ | |
| $\mathcal{U}(A)$ | unidades del anillo $A$ | |

# Capítulo 1

# La conjetura de Goldbach, probablemente

La conjetura de Goldbach ocupa un puesto destacado dentro del grupo de problemas aún por resolver en la TEORÍA ADITIVA DE NÚMEROS. Se habla del problema *binario* cuando los sumandos son una pareja y del *problema ternario* cuando se suman tres primos.

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

Llamando $\mathcal{P} := \{p\colon p \text{ es número primo}\}$ esta conjetura se puede expresar así

$$\mathcal{P} + \mathcal{P} = \{4, 6, 8, \cdots\}.$$

Denotamos por $r_2(N)$ al *número de representaciones* de $N$ como suma de dos primos:

$$r_2(N) := \#\{(p_1, p_2) \in \mathcal{P} \times \mathcal{P} \mid N = p_1 + p_2\}, \tag{1.1}$$

donde $\# A$ representa el cardinal del conjunto $A$. Nos proponemos estimar el valor de $r_2(N)$.

## 1.1. Origen e historia

Euler conoció a Goldbach en San Petersburgo en 1727. Que se sepa, intercambiaron cerca de doscientas cartas. El 7 de junio de 1742 Goldbach escribe a Euler interesándose por las posibles aportaciones de los problemas sin solución

> « no considero inútil que se hagan proposiciones que son muy probables, incluso si no están aún sustentadas por una demostración, pues aunque con el tiempo se demuestre que son incorrectas pueden contribuir a descubrir una nueva verdad»

poco después añade

> « quiero aventurar una conjetura de este tipo: que todo número que está compuesto [como suma] de dos números primos es a la vez la suma de tantos números primos como queramos (incluyendo 1), hasta llegar a la suma que consiste sólo de unos»

En los ejemplos que utiliza en su carta intervienen tanto números pares como números impares. Es posible apreciar que Goldbach seguía dando vueltas a la idea hacia el final de esta misma carta, pues escribe en el margen un comentario adicional

> «después de leer esto otra vez, considero que la conjetura puede demostrarse con todo rigor para el caso $n+1$ si sucede para el caso $n$ y si $n+1$ puede dividirse en dos números primos. La demostración es muy fácil y parece al menos ser cierto que todo número mayor que 2 es la suma de tres números primos»

Goldbach se encontraba en Moscú y Euler en Prusia y el intervalo en las cartas conocidas era de tres semanas. Por esta razón se cree que la respuesta de Euler es la carta del 30 de junio del mismo año. En ella encontramos que Euler reconoce la iniciativa a Goldbach en el planteamiento del problema:

> « que todo número que es resoluble como [suma] de dos primos puede [a su vez] ser representado como [suma] de tantos primos como se quiera, puede ser ilustrado y confirmado por una observación, misma que usted me comunicó formalmente, concretamente, que todos los números pares son suma de dos primos [...]
>
> »Sin embargo que todo número par sea la suma de dos números primos, lo que considero un teorema correcto, es algo que no puedo demostrar»

Este último párrafo escrito por Euler marcaría el inicio de las referencias a lo que hoy se conoce como conjetura de Goldbach. "[...] no puede decirse que la conjetura binaria fuera propuesta por Goldbach, pero lo que sí se puede afirmar es que el primero en mencionarla - sin demostrarla - es Euler"(v. [G-O, pág. 77])

Antes que Goldbach, Descartes abordó el asunto cuando enunció que todo número par es la suma de uno, dos o tres primos. En 1770, Edward Waring publicó sus *Meditaciones Algebraicae* y en el problema 63 señala la representación de un número en diferentes formas escribiendo

> «aquí es apropiado mencionar algunas propiedades de los enteros y de los números primos, 1) todo número par es la suma de dos primos y todo número impar es primo o suma de tres primos»

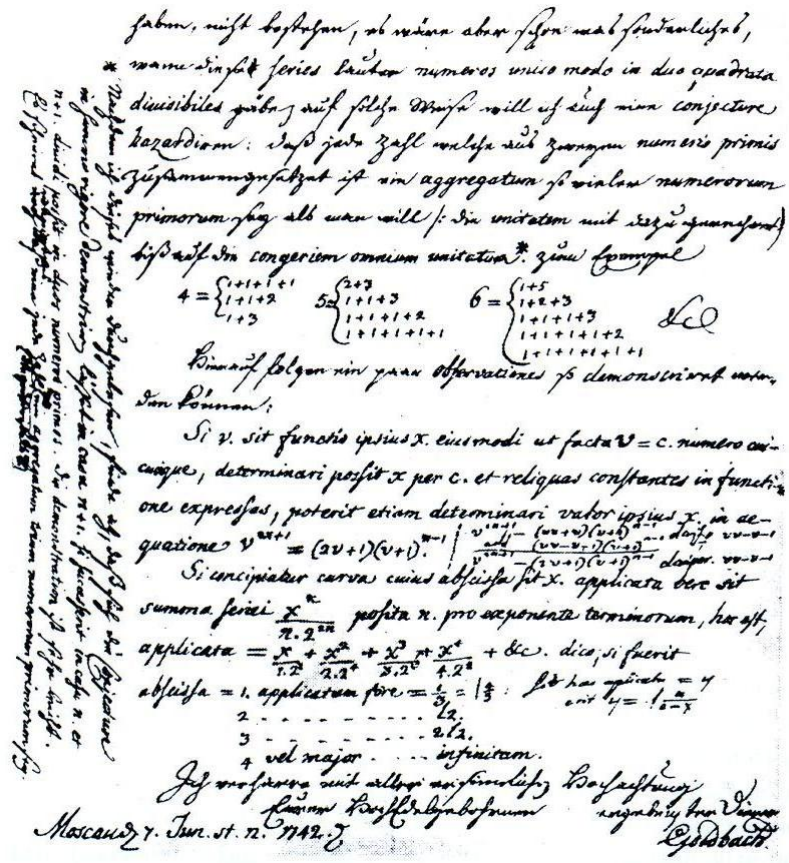

Figura 1.1: Carta de Goldbach a Euler de fecha 7 de junio 1742

Waring no tenía por qué conocer el enunciado de Descartes, cuyos manuscritos fueron publicados en 1908, ni el contenido de las cartas entre Goldbach y Euler, publicadas por primera vez en 1843.(v. [G-O, pág. 79])

El progreso en este "teorema" desde que fue identificado y enunciado ha ido lentamente apuntalando la hipótesis de que es correcto. Algunos de los hitos alcanzados son los siguientes:

En 1923 Hardy y Littlewood dieron el primer paso importante hacia una demostración de la conjetura de Goldbach. Usando su *método del círculo* probaron el teorema de Vinogradov suponiendo ciertas propiedades, todavía desconocidas, de los ceros de las funciones $L$.

En 1937 Vinogradov mostró que todo número impar suficientemente grande se puede escribir como suma de tres primos.

En 1966 Chen demostró que todo número par suficientemente grande puede escribirse como la suma de un primo más un *casi-primo* (primo o producto de dos primos).

En 1976 Montgomery y Vaughan mostraron que el número de excepciones es $O(x^{1-c})$ para cierto $c > 1$. En particular esto implica que casi todo número par se puede representar como suma de dos primos.

Ramaré probó en 1995 que todo entero par es la suma de como máximo seis primos.

El número de *representaciones* de $N$ como suma de dos primos parece crecer con el tamaño de $N$. Nótese que los factores primos de $N$ juegan también un papel relevante en este número (v. (1.5), la aproximación asintótica para $r_2(N)$ que se conjetura hoy en día).

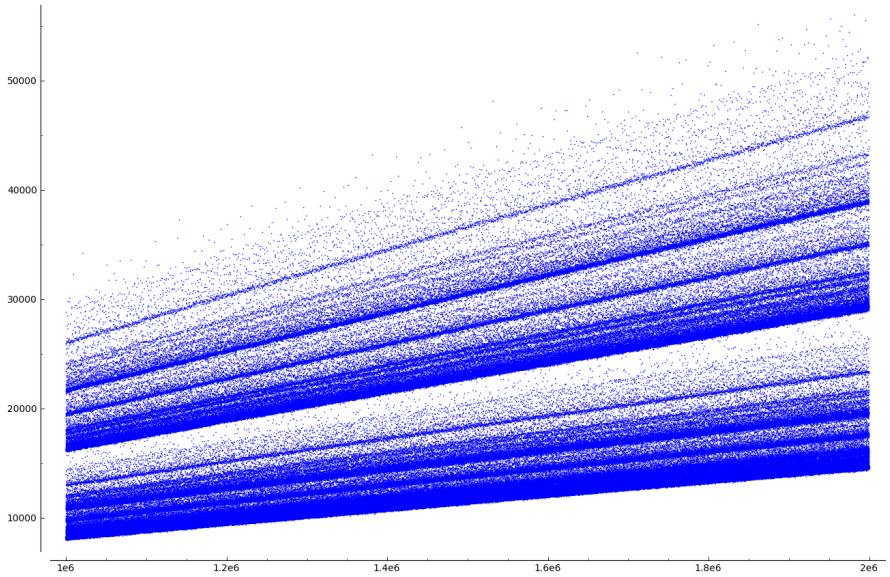


Figura 1.2: Número de representaciones como suma de dos primos

En el año 2008 la conjetura de Goldbach había sido verificada para todos los números pares menores que $12 \times 10^{17}$ (v. [mathworld]). Para algún detalle más acerca del avance en este problema se puede consultar por ejemplo [T-P-Glossary].

## 1.2. Primer acercamiento heurístico

Fijado un número par $N \in \mathbb{N}$ imaginemos un experimento aleatorio en que escogemos al azar un número $n$ menor o igual que $N$ y llamamos $B$ al suceso "$n$ es primo". La probabilidad de este suceso depende de $N$. Si la distribución de probabilidad fuera uniforme, por el TEOREMA DE LOS NÚMEROS PRIMOS (v. (3.9) en la página 25) la fórmula asintótica es

$$\mathbb{P}(B) = \pi(N)\frac{1}{N} \sim \frac{1}{\log N},$$

siendo $\pi(N) = \#\{p \leq N : p \text{ primo}\}$.

Si llamamos $C$ al suceso "$N - n$ es primo", también $\mathbb{P}(C) \sim 1/\log N \sim \mathbb{P}(B)$.

(Es claro que la distribución no es uniforme: la probabilidad de que $n$ sea primo decrece con el tamaño de $n$, se podría decir —en cierto sentido— que es como $1/\log n$. Pero sí podemos imaginar que la distribución es uniforme con un cierto grado de aproximación para los $n$ del mismo orden que $N$ y que son estos $n$ los que se espera que contribuyan más al valor de $r_2(N)$. Por ello proponemos asumir la atrevida hipótesis de que $\mathbb{P}(C) \sim 1/\log N \sim \mathbb{P}(B)$ que nos va a llevar con poco esfuerzo heurístico más a la estimación (1.4)).

¿Se puede estimar asintóticamente el valor de

$$r_2(N) := \#\{(p_1, p_2) \in \mathcal{P} \times \mathcal{P} \mid N = p_1 + p_2\},$$

como

$$\frac{r_2(N)}{N} = |\, B \cap C \,| \cdot \frac{1}{N} = \mathbb{P}(B \cap C) = \mathbb{P}(B) \cdot \mathbb{P}(C) \sim \frac{1}{(\log N)^2}? \tag{1.2}$$

La respuesta es negativa porque la condición de que $n$ sea primo no es independiente de que lo sea $N - n$ y en consecuencia no se da necesariamente la igualdad más a la derecha de (1.2). Como ejemplo de dependencia entre ambas condiciones notemos que en el caso de que $p$ sea un factor primo del número $N$ entonces la correlación es total entre $p \mid n$ y $p \mid N - n$. También los casos particulares por ejemplo $N = 12$

$$B: \quad n \in \{2, 3, 5, 7, 11\} \qquad C: \quad n \in \{5, 7, 9, 10\}$$

$$\mathbb{P}(B \cap C) = \frac{2}{12} \neq \frac{5}{12} \cdot \frac{4}{12} = \mathbb{P}(B) \cdot \mathbb{P}(C)$$

muestran la dependencia entre los sucesos $B$ y $C$.

Usando la estimación asintótica para cada una de las dos probabilidades individuales lo que sí tenemos es

$$r_2(N) = N\, \mathbb{P}(B \cap C) \sim \frac{N}{(\log N)^2}\, \frac{\mathbb{P}(B \cap C)}{\mathbb{P}(B)\mathbb{P}(C)}. \tag{1.3}$$

Llamamos ahora $\rho(N)$ al factor $\frac{\mathbb{P}(B \cap C)}{\mathbb{P}(B)\mathbb{P}(C)}$ el cual querríamos aproximar asintóticamente. Supongamos que podemos hacerlo con la estrategia de

a) reemplazar el suceso $B$ por un cúmulo de sucesos más elementales, cada uno de ellos consistiendo en que $n$ no sea divisible por un número primo $p$.

b) hacer lo mismo para el suceso $C$.

c) acumular las probabilidades elementales multiplicándolas.

Esta es una idea que en ocasiones sí resulta exitosa [Ch-4, §1].

Manos a la obra: reemplazamos la condición "$n$ es primo" por la equivalente de que no sea divisible por todos los primos $p$ menores que $\sqrt{N}$ y fijamos la atención en el suceso $B_p$ "$n$ no es múltiplo del primo $p$" (y en el suceso análogo $C_p$). Ahora estimamos el factor

$$\rho_p(N) := \frac{\mathbb{P}(B_p \cap C_p)}{\mathbb{P}(B_p)\mathbb{P}(C_p)}$$

Notamos primero que $\mathbb{P}(B_p) = 1 - \mathbb{P}(\complement B_p) = 1 - \left\lfloor \frac{N}{p} \right\rfloor \frac{1}{N} \sim 1 - 1/p$ y por simetría $\mathbb{P}(C_p) = \mathbb{P}(B_p)$. ¿Podemos calcular $\mathbb{P}(B_p \cap C_p)$?

Caso 1. $p \mid N$. En este caso se tiene $B_p = C_p$ porque $N - n$ es múltiplo de $p$ si y sólo si $n$ es múltiplo de $p$, y entonces

$$\rho_p(N) = \mathbb{P}(B_p \cap C_p)/\mathbb{P}(B_p)^2 = 1/\mathbb{P}(B_p) \sim \frac{p}{p-1} = 1 + \frac{1}{p-1}.$$

(En particular recordando que $2 \mid N$, tenemos que $\rho_2(N) \sim \frac{1/2}{(1/2)^2} = 2$).

Caso 2. $p \nmid N$. Ahora ha de ser $p > 2$ pues $N$ es par. Contaremos clases residuales módulo $p$. Sea $r_N > 0$ el resto de dividir $N$ por $p$. El número $n$ escogido al azar puede estar en una de las $p$ clases residuales con probabilidad $1/p$ (por la hipótesis de distribución uniforme en el experimento aleatorio). El suceso $B_p$ es la unión de los casos en que el residuo de $n \equiv r_n \pmod p$ es uno de $1, 2, \ldots, p-1$ y entonces $\mathbb{P}(B_p) = (p-1)/p$. También tenemos $\mathbb{P}(C_p) = (p-1)/p$. El suceso $B_p \cap C_p$ equivale a $r_n \in \{1, \ldots, p-1\} \setminus \{r_N\}$ de modo que ahora

$$\rho_p(N) = \frac{\mathbb{P}(B_p \cap C_p)}{\mathbb{P}(B_p)\mathbb{P}(C_p)} = \frac{(p-2)/p}{(p-1)^2/p^2} = \frac{p(p-2)}{(p-1)^2} = 1 - \frac{1}{(p-1)^2}$$

Cuando $p$ aumenta de tamaño $\rho_p(N)$ se aproxima a 1, es decir está más cercana la condición de independencia entre los dos sucesos "$n$ no es múltiplo de $p$" y "$N - n$ no es múltiplo de $p$". Escogidos dos primos de tamaño similar $p_1, p_2$ tales que el primero es factor de $N$ y el segundo no lo es, la proximidad a dicha independencia es relativamente menor para el primo $p_2$.

Multiplicando

$$\rho(N) \sim \prod_{p \le \sqrt{N}} \rho_p(N) \sim \prod_{\substack{p \le \sqrt{N} \\ p \mid N}} \left(1 + \frac{1}{p-1}\right) \quad \cdot \prod_{\substack{p \le \sqrt{N} \\ p \nmid N}} \left(1 - \frac{1}{(p-1)^2}\right)$$

Si ahora llamamos

$$P^*(N) = \prod_{\substack{p \le \sqrt{N} \\ p \mid N}} \left(1 + \frac{1}{p-1}\right) \qquad \text{y} \qquad P(N) = \prod_{p \mid N} \left(1 + \frac{1}{p-1}\right)$$

estos dos productos son equivalentes asintóticamente. Efectivamente $N$ tiene como mucho un factor primo $p^*$ mayor que $\sqrt{N}$ y por tanto

$$1 \leq \frac{P^*(N)}{P(N)} \leq 1 + \frac{1}{p^* - 1} \leq 1 + \frac{1}{\sqrt{N} - 1} \overset{N\to\infty}{\longrightarrow} 1.$$

Del mismo modo en el segundo producto se puede prescindir de la restricción $p \leq \sqrt{N}$. Finalmente

$$r_2(N) \sim \frac{N}{(\log N)^2} \prod_{p|N} \left(1 + \frac{1}{p-1}\right) \prod_{p\nmid N} \left(1 - \frac{1}{(p-1)^2}\right) \qquad N \text{ par} \tag{1.4}$$

De este modo probabilista hemos hallado una *probable* expresión asintótica para la cantidad de representaciones de un número par $N$ como suma de dos primos. La fórmula (1.4) ha sido contrastada por extensos cálculos computacionales.

Notamos que esta fórmula se puede escribir también así:

$$r_2(N) \sim \frac{2\,N}{(\log N)^2} \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{\substack{p|N \\ p>2}} \left(1 + \frac{1}{p-2}\right) \qquad N \text{ par}, \tag{1.5}$$

donde el primer producto recorre todos los primos impares, ya que cuando $p > 2$,

$$(1 - (p-1)^{-2})(1 + (p-2)^{-1}) = 1 + (p-1)^{-1}.$$

En [Ci, pág. 559] se observa que:

"Sin embargo este argumento, basado simplemente en la densidad de los primos, no sólo no es riguroso, sino que ofrece una visión equivocada del problema. Podemos ofrecer ejemplos de conjuntos de impares más "numerosos" que los primos donde hay infinitos pares que no son suma de dos elementos del conjunto. Por ejemplo, con los impares de la forma $4k + 1$ que son mucho más numerosos que los primos, no podemos representar los múltiplos de 4.

Esta última observación nos invita a pensar que no sólo debemos tener en cuenta que hay muchos primos, sino que también habrá que ver cómo se distribuyen en progresiones aritméticas".

# Capítulo 2

# El método del círculo

En 1923 Hardy y Littlewood desarrollaron el *método del círculo*, que ya había sido usado previamente por Hardy y Ramanujan para estudiar la cantidad de *particiones*: ¿de cuántas maneras distintas se puede expresar un número como suma de otros números?

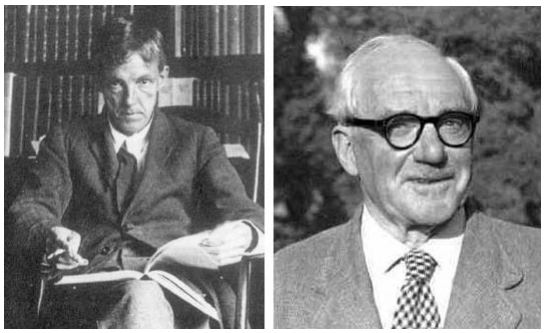

Figura 2.1: G. H. Hardy y J. E. Littlewood

En la Teoría Aditiva de Números este método es uno de los instrumentos más útiles para tratar aquellos problemas que buscan calcular la cantidad de representaciones de un número $n$ entero positivo como suma de otros números.

Dado cualquier subconjunto de los enteros positivos $\mathcal{A} \subset \mathbb{N}$ y un número $k$ fijo de sumandos se pretende encontrar el orden de magnitud de la función $r(\,\cdot\,; k, \mathcal{A})\colon \mathbb{N} \to \mathbb{N}$ definida como

$$r(n; k, \mathcal{A}) := \#\{(a_1, \ldots, a_k) \in \mathcal{A}^k \mid n = a_1 + \ldots + a_k\},$$

que cuenta el número de representaciones de $n$ con $k$ sumandos del conjunto $\mathcal{A}$.

Llamando $\mathcal{P} := \{p\colon p \text{ es primo}\}$ y $\mathcal{R} := \{n^r\colon n \in \mathbb{N}\}$ para un exponente entero positivo $r$ fijado, algunos ejemplos son:

- Si $\mathcal{A} = \mathbb{N}$ y $k$ no está fijo, el problema es el de la cantidad de *particiones* de un número entero positivo.

- Si $\mathcal{A} = \mathcal{P}$ y $k = 2$ el objeto de estudio es $\mathcal{P} + \mathcal{P}$, en donde ocupa un lugar destacado la conjetura de Goldbach para los números pares.
- Si $\mathcal{A} = \mathcal{P}$ y $k = 3$ se trata de investigar $\mathcal{P} + \mathcal{P} + \mathcal{P}$. El *teorema de Vinogradov* confirma que todo número impar suficientemente grande está en este conjunto.
- Cuando $\mathcal{A} = \mathcal{R}$ y fijamos $k$ queremos analizar $\mathcal{R} \overset{(k \text{ veces})}{+ \cdots +} \mathcal{R}$. Conocido como *Problema de Waring* busca las formas de expresar un número entero positivo como suma de $k$ potencias $r$-ésimas.

## Funciones generatrices

Comenzamos observando que el valor buscado aparece como coeficiente del término $n$-ésimo en ciertas series. En primer lugar si definimos $F_{\mathcal{A}} \colon \{z \colon |z| < 1\} \to \mathbb{C}$

$$F_{\mathcal{A}}(z) := \sum_{a \in \mathcal{A}} z^a,$$

elevando $F_{\mathcal{A}}$ a $k$ obtenemos una nueva serie de potencias donde el coeficiente de la potencia $n$-ésima es precisamente $r(n; k, \mathcal{A})$:

$$[F_{\mathcal{A}}(z)]^k = \sum_{a_1 \in \mathcal{A}} z^{a_1} \times \ldots \times \sum_{a_k \in \mathcal{A}} z^{a_k} = \sum_{n=0}^{\infty} r(n; k, \mathcal{A}) z^n.$$

En particular $F_{\mathcal{A}}^k$ es una función holomorfa en el interior del disco de centro 0 y radio 1 y por ello, tomando cualquier circunferencia $C_\rho = \{|z| = \rho\}$ de radio $\rho < 1$, podemos expresar el coeficiente de $z^n$ por medio de la fórmula integral de Cauchy

$$r(n; k, \mathcal{A}) = \frac{1}{2\pi i} \int_{C_\rho} \frac{[F_{\mathcal{A}}(z)]^k}{z^{n+1}} \, \mathrm{d}z.$$

La parametrización habitual en coordenadas polares del contorno $C_\rho$ (v. figura 2.2) sugiere una aproximación ligeramente alternativa a la anterior. Abreviaremos por comodidad

$$e\,(t) := \exp(2\pi i t) = \cos 2\pi t + i \operatorname{sen} 2\pi t.$$

Tomando ahora como función generatriz

$$f_{\mathcal{A}} \colon [0,1] \times [0,1] \to \mathbb{C} \qquad\qquad f_{\mathcal{A}}(\rho, x) = \sum_{a \in \mathcal{A}} \rho^a \, e\,(ax)\,,$$

aprovechando la siguiente versión particular de la fórmula integral de Cauchy

$$\int_0^1 e\,(mx) \, \mathrm{d}x = \begin{cases} 1 & \text{si } m = 0, \\ 0 & \text{en otro caso} \end{cases} \qquad m \in \mathbb{Z}, \tag{2.1}$$

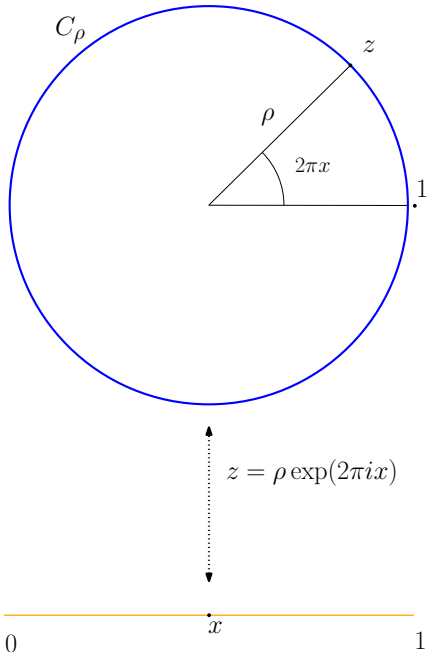


Figura 2.2: Desenrollando el círculo

y despreocupándonos por un momento de la convergencia -considerando a $f_{\mathcal{A}}(\rho, x)$ como una serie formal- tenemos que

$$[f_{\mathcal{A}}(1,x)]^k = \sum_{n=0}^{\infty} r(n;k,\mathcal{A}) e\left(nx\right) \qquad \text{y entonces}$$
$$r(n;k,\mathcal{A}) = \int_0^1 [f_{\mathcal{A}}(1,x)]^k e\left(-nx\right)\, \mathrm{d}x.$$

## Truncamiento de la serie y expresión como integral

En los casos interesantes $\mathcal{A}$ es infinito y no está garantizada la convergencia de la serie que define $f_{\mathcal{A}}$ cuando $\rho \to 1$. Para circunvalar este escollo se trunca dicha serie trigonométrica en el término $N$-ésimo, lo que deja un polinomio trigonométrico $f_N \colon [0,1] \to \mathbb{C}$

$$f_{\mathcal{A}_N}(1,x) = f_N(x) = \sum_{a \in \mathcal{A}_N} e\left(ax\right) \qquad \text{siendo } \mathcal{A}_N = \mathcal{A} \cap [1,N]$$

$f_N$ es una función entera (holomorfa en todo $\mathbb{C}$) y ahora tenemos

$$[f_N(x)]^k = \sum_{a_1 \in \mathcal{A}_N} e\,(a_1 x) \times \ldots \times \sum_{a_k \in \mathcal{A}_N} e\,(a_k x) = \sum_{n=1}^{n=kN} r_N(n;k,\mathcal{A})\, e\,(nx)\,,$$

donde el coeficiente $r_N(n;k,\mathcal{A})$ cuantifica el número de representaciones de $n$ con $k$ sumandos de $\mathcal{A}$ que además son menores o iguales que $N$.

Aprovechamos también una consecuencia de que los elementos de $\mathcal{A}$ son positivos: cuando $n \leq N$ se cumple $r_N(n;k,\mathcal{A}) = r(n;k,\mathcal{A})$ porque siempre que $a_1 + \ldots + a_k = n$ necesariamente $a_i \leq n \leq N$, es decir $a_i \in \mathcal{A}_N$. Apelando de nuevo a (2.1) concluimos que

**Lema 2.1.** *Sea $\mathcal{A} \subset \mathbb{N}$ y $k$ un número entero positivo. Sea $r(n;k,\mathcal{A})$ el número de representaciones de $n$ con $k$ sumandos de $\mathcal{A}$, entonces*

$$r(n;k,\mathcal{A}) = \int_0^1 [f_N(x)]^k e\,(-nx)\,\mathrm{d}x \qquad \textit{cuando} \quad n \leq N, \tag{2.2}$$

*en donde*

$$f_N(x) = \sum_{a \in \mathcal{A}\,,\, a \leq N} e\,(ax) \qquad\qquad e\,(ax) := \exp(2\pi i a x).$$

A partir de esta fórmula habitualmente el trabajo consistirá en estimar la integral de la derecha intentando al menos asegurar que está acotada inferiormente por un valor estrictamente mayor que cero.

## 2.1. Arcos mayores y menores

En numerosas aplicaciones exitosas del método del círculo se procede del modo siguiente

1. Se construye el polinomio generatriz $f_N$ para $\mathcal{A}_N$. Como es una suma oscilatoria de números complejos de módulo 1 se espera bastante cancelación en la suma.

2. Se subdivide $[0,1]$ en dos partes disjuntas denominadas los **arcos mayores** $\mathcal{M}$ y los **arcos menores** $\mathfrak{m}$. La construcción de $\mathcal{M}$ dependerá del problema concreto. Entonces se subdivide el análisis en dos integrales para su estudio por separado:

$$\begin{aligned} r(n;k,\mathcal{A}) &= \int_0^1 [f_N(x)]^k e\,(-nx)\,\mathrm{d}x = \\ &= \int_{\mathcal{M}} [f_N(x)]^k e\,(-nx)\,\mathrm{d}x + \int_{\mathfrak{m}} [f_N(x)]^k e\,(-nx)\,\mathrm{d}x. \end{aligned}$$

3. En los arcos mayores $\mathcal{M}$ *se extrae información de las singularidades.* Por un lado se espera que los valores de $f_N$ en este conjunto sean grandes debido a que se define $\mathcal{M}$ de manera que su imagen por la aplicación $t \mapsto e(t)$ esté cerca de los puntos singulares que tiene $F_{\mathcal{A}}$ (la función de variable compleja que fue el punto de partida desde el que llegamos a $f_N$). Por otro lado en $\mathcal{M}$ se encuentra una función que se parece a $(f_N)^k$ y es sencilla de integrar. Cuando se integra se obtiene una contribución en los arcos mayores que se puede acotar inferiormente lejos de 0 y además es grande.

4. Se comprueba que, al hacer $N \to \infty$, la contribución a la integral de los arcos menores $\mathfrak{m}$ es de un orden de magnitud menor que la contribución de los arcos mayores $\mathcal{M}$. Esto implica que, para $N$ suficientemente grande, $r(N; k, \mathcal{A}) > 0$ es decir que cualquier $N$ suficientemente grande se puede expresar como suma de $k$ elementos de $\mathcal{A}$.

En [M-TB, pág. 312] se destaca lo siguiente:

> "La suma $f_N$ tiene $|\,\mathcal{A}_N\,|$ sumandos cada uno de ellos con valor absoluto igual a 1. En muchos problemas para la mayoría de $x \in (0,1)$ el tamaño de $f_N(x)$ es como $\sqrt{|\,\mathcal{A}_N\,|}$ y para unos $x$ particulares se tiene que $f_N(x)$ es de tamaño $|\,\mathcal{A}_N\,|$. Cuando se pueda demostrar además que en el resto de los $x$ la contribución es más pequeña, tendremos una cota inferior de $r(N; k, \mathcal{A})$ lejos de cero.
>
> El paso más difícil es el último. Cuando se puede conseguir la cancelación deseada sobre los arcos menores, ello requiere habitualmente la mayor parte del esfuerzo."

En las primeras aplicaciones del método se usaba la serie de potencias en variable compleja y se partía $C_\rho = \{|z| = \rho\}$ en dos subconjuntos disjuntos de arcos de circunferencia. Es por esta razón que se sigue hablando de *círculo* y de *arcos* aun después de haberlos desenrollarlo en un intervalo de longitud 1 dentro de $\mathbb{R}$ (ver figura 2.2 en la página 11).

Los arcos mayores habitualmente reposan sobre puntos singulares de la función de variable compleja subyacente. Por ejemplo la función generatriz para el problema concreto de las particiones de un número es

$$\begin{aligned} F_{\mathbb{N}}(z) &= 1 + \sum_{n=1}^{\infty} P_n(z) z^n \\ &= (1 + \cdots + z^k + \cdots)(1 + \cdots + (z^2)^k + \cdots) \ldots (1 + \cdots + (z^m)^k + \cdots) \ldots \\ &= \frac{1}{(1-z)(1-z^2)(1-z^3)\cdots} \end{aligned}$$

Esta función es singular en todos los números complejos de la circunferencia unidad cuyo argumento dividido entre $2\pi$ es un número racional: $z = e(n/d)$. En consecuencia

se espera poder *extraer información* suficiente de estas singularidades de modo que al integrar sobre $\mathcal{M}$ se obtenga una contribución predominante respecto a la de los arcos menores.

En otros casos, como veremos más adelante, la función $f_N$ que aparece en el integrando de (2.2) también toma valores de gran tamaño (en valor absoluto) en la cercanía de ciertos racionales. Para $x = n/d$ racional tenemos

$$f_N\left(\frac{n}{d}\right) = \sum_{a\in\mathcal{A}\,,\,a\le N} \left[e\left(\frac{n}{d}\right)\right]^a.$$

Observamos que, cuando $a-a'$ es múltiplo de $d$, los valores de ambos sumandos coinciden

$$\left[e\left(\frac{n}{d}\right)\right]^a = \left[e\left(\frac{n}{d}\right)\right]^{a'},$$

y podemos decir que los dos exponentes $a, a'$ han *resonado* a la frecuencia $n/d$. El estudio de tales resonancias está íntimamente relacionado con la distribución de los elementos de $\mathcal{A}$ módulo $d$. La suma total se subdivide en tantas sumas como residuos distintos $r_1, \cdots, r_M$ módulo $d$ aparezcan entre los enteros de $\mathcal{A}$:

$$f_N\left(\frac{n}{d}\right) = \sum_{a\in\mathcal{A}\,,\,a\le N} e\left(\frac{n}{d}\,a\right) = \sum_{1\le i\le M} A(N; r_i, d)\; e\left(\frac{n}{d}\,r_i\right),$$

en donde $A(N; r_i, d)$ cuenta los elementos de $\mathcal{A}$ menores o iguales que $N$ cuyo residuo módulo $d$ es $r_i$.

Cuanto más pequeño es el denominador $d$ es más fácil que los exponentes enteros y las frecuencias racionales resuenen. En consecuencia tendremos menos residuos distintos y previsiblemente habrá menos cancelación en la suma total. Por tanto es esperable que $f_N(n/d)$ sea de tamaño más grande en los racionales de denominador pequeño, que por esta razón serán buenos candidatos a integrar los arcos mayores.

# Capítulo 3

# Los *mayores* ingredientes

Durante el resto del trabajo analizaremos el número $r(N;k,\mathcal{P})$ de representaciones de un entero positivo $N$ como suma de $k$ números primos. Comenzamos en este capítulo concretando los ingredientes que, combinados siguiendo el método del círculo (v. capítulo 2), proporcionarán la parte principal de la estimación para $r(N;k,\mathcal{P})$.

## El producto de Euler

Una versión analítica del Teorema Fundamental de la Aritmética es la identidad

$$\sum_{n=1}^{\infty}\frac{1}{n^x}=\prod_{p\text{ primo}}^{\infty}\frac{1}{1-1/p^x}\qquad 1<x\in\mathbb{R}, \tag{3.1}$$

que es también un ejemplo de una idea perspicaz: *extraer información a partir de las singularidades.*

**Proposición 3.1.** *Definimos la función de variable compleja*

$$\zeta(s):=\sum_{n=1}^{\infty}1/n^s\qquad Re\,(s)>1.$$

*Entonces $\zeta$ se puede extender al semiplano abierto $Re\,(s)>0$ como una función meromorfa con un polo simple en $s=1$.*

*Demostración.* Observamos que la extensión de $\zeta$ al semiplano abierto $\mathrm{Re}\,(s)>0$ se puede formular como

$$\zeta(s)=\frac{1}{s-1}+1-s\int_1^{\infty}\frac{\{u\}}{u^{s+1}}\,\mathrm{d}u\qquad \mathrm{Re}\,(s)>0, \tag{3.2}$$

donde $\{u\}$ es la parte fraccionaria de $u$. Una manera de deducir esta fórmula es usar sumación por partes como sigue. Fijado $N$, por el lema 3.5 con $f(t)=1\quad g(t)=1/t^s$ podemos escribir

$$\sum_{n\leq N}\frac{1}{n^s}=\frac{s}{s-1}-s\int_1^N\frac{\{u\}}{u^{s+1}}\,\mathrm{d}u-\frac{1}{(s-1)N^{s-1}}\quad \mathrm{Re}\,(s)>1.$$

Haciendo tender $N$ a infinito, nótese que la función $s\int_1^\infty\{u\}/u^{s+1}\,\mathrm{d}u$ es holomorfa en el semiplano abierto derecho del plano complejo. Por la propiedad de unicidad en la continuación analítica de las funciones holomorfas se concluye (3.2). □

Centrando la atención en el punto singular $s=1$ se puede desvelar información valiosa. Euler se percató de que haciendo tender $1<x\in\mathbb{R}$ hacia el 1 se consigue otra demostración de que los números primos son infinitos. Además tomando logaritmos en ambos miembros de (3.1) y recordando que $-\log(1-x)=x+O(x^2)$ obtuvo

$$\log\left(\sum_n\frac{1}{n^x}\right)=\sum_p\frac{1}{p^x}+Err(x)\quad x>1\qquad\text{con }\left|Err(1^+)\right|<\infty,$$

y de este modo *extrajo la información* añadida de que la serie $\sum 1/p$ diverge, hecho que viene a engrandecer la infinitud de los números primos.

## 3.1. Algunas funciones aritméticas

Una función $f\colon\mathbb{N}\to\mathbb{C}$ se dice aritmética porque inicialmente su dominio son los números naturales. Se extiende a todos los reales mayores que 1 como sigue $f(x):=f(\lfloor x\rfloor)$, con $\lfloor\cdot\rfloor$ denotando la parte entera.

### La función $\mu$ de Möbius

Aparece al poner invertido el producto de Euler (3.1)

$$\frac{1}{\zeta(s)}=\prod_p\left(1-\frac{1}{p^s}\right)=\sum_n^\infty\frac{\mu(n)}{n^s}\qquad\mathrm{Re}\,(s)>1$$

definiendo $\mu(1)=1,\quad\mu(p_1\times\cdots\times p_k)=(-1)^k$ y $\mu(n)=0$ en otro caso.

En Teoría de Números se asocia a una función $f$ la serie de Dirichlet $D_f=\sum f(n)/n^s$ cuyos coeficientes son precisamente $f(n)$. Nuestros primeros ejemplos han sido

$$D_1=\sum 1/n^s=\zeta(s)\qquad D_\mu=\sum\mu(n)/n^s=\zeta(s)^{-1}.$$

Cuando $D_f$ y $D_g$ convergen absolutamente entonces también converge la serie de Dirichlet $D_f\cdot D_g$ y sus coeficientes son la **convolución de $f$ y $g$**:

$$(f\star g)(n)=\sum_{d|n}f\left(\frac{n}{d}\right)\,g(d).$$

Como $1 + \sum_{n>1} 0/n^s = \zeta(s)\zeta(s)^{-1} = D_1 D_\mu$ la convolución $1 \star \mu$ es

$$\sum_{d|n} \mu(d) = 0 \quad \text{si } n > 1 \quad \text{y} \quad \sum_{d|1} \mu(d) = 1. \tag{3.3}$$

Con esto podemos ya probar el siguiente resultado

**Lema 3.1** (Inversión de Möbius)**.**
*Si $f$ es una función aritmética y llamamos $g(n) = \sum_{d|n} f(d)$ entonces*

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(n).$$

*Demostración.* De hecho

$$\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \left[\sum_{c|\frac{n}{d}} f(c)\right] = \sum_{cd|n} \mu(d) f(c) = \sum_{c|n} f(c) \left[\sum_{d|\frac{n}{c}} \mu(d)\right] = f(n),$$

porque la última suma interior vale 1 si $n/c = 1$ y 0 en otro caso. □

## La función $\phi$ de Euler

Los coeficientes de la serie de Dirichlet

$$\left(\sum n/n^s\right)\left(\sum \mu(n)/n^s\right) = \frac{\zeta(s-1)}{\zeta(s)} = \sum \phi(n)/n^s = D_\phi,$$

son la convolución $\mathrm{Id} \star \mu$

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

Podemos expandir esta suma como sigue

$$\phi(n) = \sum_{d|n} \frac{n}{d}\, \mu(d) = \sum_{i=1}^{n} \sum_{d|(i,n)} \mu(d),$$

pues fijado $d$, en la última suma el sumando $\mu(d)$ aparece exactamente cuando $i \in \{d, 2d, \ldots \frac{n}{d} d\}$. Por (3.3) la suma interior es 0 salvo si $(i, n) = 1$ en cuyo caso es 1. Concluimos que $\phi(n)$ es la cantidad de números menores que y coprimos con $n$:

$$\phi(n) = \sum_{\substack{i \le n \\ (i,n)=1}} 1.$$

También esta otra fórmula

$$\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d} = n \prod_{p|n} \left(1 - \frac{1}{p}\right), \tag{3.4}$$

resalta la interpretación de $\phi(n)/n$ como la probabilidad de que un número menor que $n$ sea coprimo con $n$.

Usando la inversión de Möbius (lema 3.1) obtenemos

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

Una función aritmética $f$ es *multiplicativa* cuando

$$(m,n) = 1 \quad \text{(i.e. } m,n \text{ primos entre sí)} \Rightarrow f(m \cdot n) = f(m) \cdot f(n)$$

y es *completamente multiplicativa* si se cumple siempre $f(m \cdot n) = f(m) \cdot f(n)$.

**Lema 3.2.** *Si $f$ es función aritmética multiplicativa también lo es $F(n) := \sum_{d|n} f(d)$.*

*Demostración.* Si $n_1, n_2$ son coprimos entonces todo divisor de su producto $n_1 n_2$ se escribe de forma única como $d = d_1 d_2$ con $d_i$ divisor de $n_i$ y con $d_1, d_2$ coprimos; por tanto

$$F(n_1 n_2) = \sum_{\substack{(d_1,d_2)=1 \\ d_1|n_1 \\ d_2|n_2}} f(d_1 d_2) = \sum_{\substack{d_1|n_1 \\ d_2|n_2}} f(d_1) f(d_2) = \sum_{d_1|n_1} f(d_1) \cdot \sum_{d_2|n_2} f(d_2) = F(n_1) F(n_2).$$

□

**Lema 3.3.** *$\phi$ y $\mu$ son funciones multiplicativas.*

*Demostración.*

Si $m = p_1^{e_1} \dots p_r^{e_r}$ y $n = q_1^{f_1} \dots q_s^{f_s}$ son coprimos entonces no tienen factores primos comunes y la factorización de su producto en primos es $mn = p_1^{e_1} \dots p_r^{e_r} \cdot q_1^{f_1} \dots q_s^{f_s}$.

Si ambos números están libres de cuadrados también lo está su producto y entonces $\mu(mn) = (-1)^{r+s} = \mu(m)\mu(n)$. En otro caso o bien $\mu(m) = 0$ o bien $\mu(n) = 0$ (o ambas), entonces $\mu(mn) = 0 = \mu(m)\mu(n)$.

Visto que $n \mapsto \mu(n)$ es multiplicativa también lo son tanto $n \mapsto \mu(n)/n$ como (por el lema 3.2)

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

y finalmente también es multiplicativa $n \mapsto n \cdot \frac{\phi(n)}{n} = \phi(n)$.

□

Para evaluar las funciones multiplicativas basta encontrar el valor que toman en las potencias de primos. Como ejemplo reencontramos la fórmula para $\phi$.

En primer lugar los números menores que y que *no son coprimos con* cualquier potencia de un primo $p^e$ son los múltiplos de $p$ menores o iguales que $p^e$: $\{1, p, 2p, \cdots, p^e\}$, que son $p^e/p$ números distintos; así $\phi(p^e) = p^e - p^{e-1}$ y entonces, si la factorización de $n$ es $n = p_1^{e_1} \dots p_r^{e_r}$,

$$\phi(n) = \prod_{i=1}^{r} \phi(p^{e_i}) = \prod_{i=1}^{r} (p^{e_i} - p^{e_i - 1}) = \prod_{i=1}^{r} p^{e_i} \left(1 - \frac{1}{p^{e_i}}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

De esta fórmula en particular se desprende que si $n$ es múltiplo de $d$ entonces también $\phi(n)$ es múltiplo de $\phi(d)$.

Acabamos esta reseña acerca de la función $\phi$ mostrando la propiedad (3.6) sobre su comportamiento asintótico, que usaremos más adelante. Para demostrarla usamos el resultado (3.5) que exponemos previamente

**Lema 3.4.** *Sea $f(n)$ una función multiplicativa. Si*

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

*cuando $p^m$ recorre la secuencia de todas las potencias de todos los primos, entonces*

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

*Demostración.* Existe una cantidad finita de potencias $p^m$ tales que $|f(p^m)| \geq 1$. Sea

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

Sea un $\epsilon$ cualquiera on $0 < \epsilon < A$. Existe una cantidad finita de potencias $p^m$ tales que $|f(p^m)| \geq \epsilon/A$. Entonces existe una cantidad finita de enteros $n$ tales que, para cada potencia de primo $p^m$ que *divide exactamente* a $n$[1], se cumple $|f(p^m)| \geq \epsilon/A$. En consecuencia, si $n$ es suficientemente grande, entonces $n$ es múltiplo de al menos una potencia de primo $p^m$ tal que $|f(p^m)| < \epsilon/A$, y por tanto podemos escribir

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

en donde $p_1, \cdots, p_{r+s+t}$ son números primos distintos tales que

$$\begin{aligned} 1 \leq |f(p_i^{m_i})| & \qquad \text{para } 1 \leq i \leq r, \\ \epsilon/A \leq |f(p_i^{m_i})| < 1 & \qquad \text{para } r+1 \leq i \leq r+s, \\ |f(p_i^{m_i})| \leq \epsilon/A & \qquad \text{para } r+s+1 \leq i \leq r+s+t, \end{aligned}$$

[1] Se dice que $p^m$ divide exactamente a $n$ cuando $p^m \mid n$ y $p^m \nmid n$.

y $t \geq 1$. Se termina la prueba notando que

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

□

**Proposición 3.2.**

$$\lim_{x\to\infty} \frac{\phi(x)}{x^{1-\delta}} = \infty \qquad \forall\ \delta > 0. \tag{3.5}$$

*Demostración.* Como

$$f(x) = \frac{x^{1-\delta}}{\phi(x)}$$

es multiplicativa y además

$$f(p^m) = \frac{p^{m(1-\delta)}}{\phi(p^m)} = \frac{1}{p^{m\delta}\,(1-1/p)} \leq \frac{2}{p^{m\delta}},$$

para cualquier potencia de cualquier primo, entonces $f(p^m) \to 0$ cuando $p^m$ recorre la secuencia de todas las potencias de todos los primos y podemos aplicar el lema 3.4. □

**Corolario 3.1.** *La función $\phi$ de Euler*

$$\phi(x) := \sum_{\substack{1\leq i\leq \lfloor x\rfloor \\ (i,\lfloor x\rfloor)=1}} 1,$$

*cumple lo siguiente*

$$x^{1-\delta} \ll \phi(x) \ll x \qquad \forall\ \delta > 0. \tag{3.6}$$

## La función $\Lambda$ de Von Mangoldt

Tomando la derivada en ambos lados del producto de Euler (3.1) aparece una nueva función aritmética

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_p \frac{\log p}{(1-1/p^s)} = \sum_p \log p \cdot \left(1 + \frac{1}{p^s} + \frac{1}{(p^2)^s} + \cdots\right) = \sum_n \frac{\Lambda(n)}{n^s},$$

con $\Lambda(n) = \log p$ si $n = p^k$ y $\Lambda(n) = 0$ en otro caso.

La nueva serie de Dirichlet ahora en escena es $D_L = -\zeta'(s) = \sum \log n/n^s$ asociada a la función $L(n) = \log n$ y como $D_L = D_1 D_\Lambda$ la convolución $L = 1 \star \Lambda$ desvela la propiedad

$$\sum_{d|n} \Lambda(d) = \log n. \tag{3.7}$$

### Sumación por partes

**Lema 3.5** (Abel)**.** *Sean $f$ cualquier función aritmética y $g\colon [1,\infty) \to \mathbb{C}$ una función con derivada continua. Llamamos $M_f(x) := \sum_{n\le x} f(n)$. Entonces*

$$M_{fg}(x) = M_f(x)g(x) - \int_1^x M_f(t)g'(t)dt.$$

(Si vemos a $f$ como *la derivada* de $M_f$, esta fórmula recuerda fuertemente a la integración por partes).

*Demostración.* Convengamos $M_f(0) = 0$. Recordamos que cualquier función aritmética toma en $x$ el mismo valor que toma en su parte entera $\lfloor x \rfloor$; así $M_f$ es constante tanto en $[n, n+1)$ como en $[\lfloor x \rfloor, x)$. Entonces

$$\begin{aligned}
\sum_{1\le n\le x} f(n)g(n) &= \sum_{0\le n\le \lfloor x\rfloor -1} \left[M_f(n+1) - M_f(n)\right] g(n+1) \\
&= -M_f(0)g(1) + \sum_{1\le n\le \lfloor x\rfloor -1} M_f(n)\left[g(n) - g(n+1)\right] + M_f(\lfloor x\rfloor)g(\lfloor x\rfloor) \\
&= \sum_{1\le n\le \lfloor x\rfloor -1} M_f(n)\left(-\int_n^{n+1} g'(t)\,\mathrm{d}t\right) + M_f(\lfloor x\rfloor)g(\lfloor x\rfloor) \\
&= M_f(x)g(x) - \sum_{1\le n\le \lfloor x\rfloor -1} \left(\int_n^{n+1} M_f(t)g'(t)\,\mathrm{d}t\right) - M_f(x)\left(f(x) - f(\lfloor x\rfloor)\right) \\
&= M_f(x)g(x) - \int_1^{\lfloor x\rfloor} M_f(t)g'(t)\,\mathrm{d}t - \int_{\lfloor x\rfloor}^x M_f(t)g'(t)\,\mathrm{d}t \\
&= M_f(x)g(x) - \int_1^x M_f(t)g'(t)\,\mathrm{d}t.
\end{aligned}$$

□

### Sumas de Ramanujan

Abreviaremos por comodidad

$$e\left(t\right) := \exp\left(2\pi i t\right) = \cos 2\pi t + i \operatorname{sen} 2\pi t.$$

Como $e\left(k\right) = 1$ para todo entero $k$, dado cualquier $q$ entero positivo se tiene

$$\forall\, k, k' \in \mathbb{Z} \quad k \equiv k' \pmod{q} \Longrightarrow e\left(\frac{k}{q}\right) = e\left(\frac{k'}{q}\right) \qquad \forall\, q \in \mathbb{N}.$$

Se define la función aritmética de dos variables $\mathbb{N}\times\mathbb{N} \to \mathbb{C}$

$$(q,n) \mapsto c_q(n) := \sum_{\substack{k=1 \\ (k,q)=1}}^{q} e\left(\frac{nk}{q}\right),$$


Figura 3.1: Sello conmemorando el 75 aniversario del nacimiento de S. Ramanujan

conocida como *sumas de Ramanujan* en honor al matemático que las introdujo.

Recordamos que para cada $q > 1$ entero una $q$-raíz primitiva de la unidad es aquel número complejo $\xi$ tal que $\xi^q = 1$ y $\xi^r \neq 1$ si $0 < r < q$. Resultan ser los $\phi(q)$ números $\xi_k = e\,(k/q)$ con $k$ menor que $q$ y coprimo con $q$. De modo que en una suma de Ramanujan se suman precisamente las potencias $n$-ésimas de todas las $q$-raíces primitivas de la unidad.

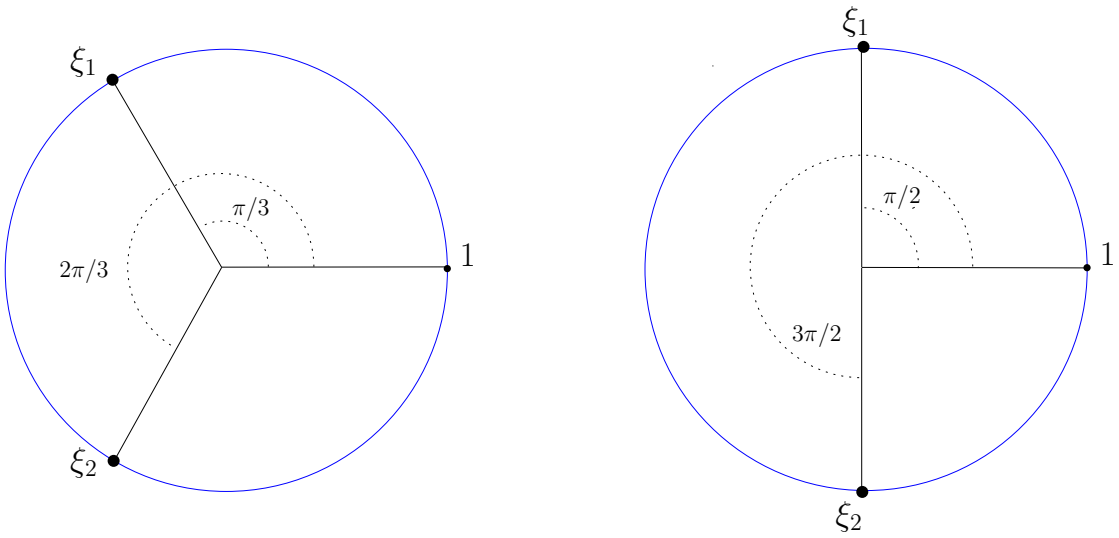


Figura 3.2: Las 3-raíces de la unidad y las dos 4-raíces primitivas de la unidad

**Lema 3.6.** *Si $\rho_1, \ldots, \rho_N$ $(N > 1)$ son todas las $N$-raíces de la unidad entonces para todo exponente $r \in \mathbb{N}$ coprimo con $N$*

$$\sum_{i=1}^{N} \rho_i^r = 0.$$

*Demostración.* Como $(r, N) = 1$ entonces $\{\rho_i^r\}_{i=1,\dots,N}$ son $N$ raíces distintas del polinomio $P(X) = X^N - 1 \in \mathbb{C}[X]$, por tanto son las $N$-raíces de la unidad. Como el polinomio $P$ se factoriza de modo único en el anillo $\mathbb{C}[X]$

$$X^N - 1 = \prod_{i=1}^{N}(X - \rho_i^r) = X^N - (\rho_1^r + \ldots + \rho_N^r)X^{N-1} + \ldots + (-1)^N \rho_1^r \ldots \rho_N^r,$$

el coeficiente del monomio $X^{N-1}$ en $P$ ha de ser tanto 0 como el opuesto de la suma de sus raíces. □

Apuntamos que se puede seguir usando otras propiedades de las raíces de la unidad y la inversión de Möbius para desvelar que

$$c_q(n) = \sum_{d|(q,n)} d\, \mu\left(\frac{n}{q}\right).$$

Sin embargo nos centraremos en demostrar otra fórmula que relaciona las sumas de Ramanujan con las dos funciones $\phi$ de Euler y $\mu$ de Möbius.

**Lema 3.7.** *$c_q$ es función multiplicativa respecto a la variable $q$:*

$$(q_1, q_2) = 1 \Rightarrow c_{q_1 \cdot q_2}(n) = c_{q_1}(n) \cdot c_{q_2}(n)$$

*Demostración.* Tenemos que

$$c_{q_1}(n) \cdot c_{q_2}(n) = \left[\sum_{\substack{i=1 \\ (i,q_1)=1}}^{q_1} e\left(n\frac{i}{q_1}\right)\right] \cdot \left[\sum_{\substack{j=1 \\ (j,q_2)=1}}^{q_2} e\left(n\frac{j}{q_2}\right)\right] = \sum_{\substack{i=1 \\ (i,q_1)=1}}^{q_1} \sum_{\substack{j=1 \\ (j,q_2)=1}}^{q_2} e\left(n\frac{(iq_2 + jq_1)}{q_1 q_2}\right)$$

de modo que todo lo que hay que mostrar es que los $\phi(q_1 q_2) = \phi(q_1)\phi(q_2)$ números menores que y coprimos con $q_1 q_2$ son precisamente

$$\text{los residuos de } \{iq_2 + jq_1 \mid (i, q_1) = 1 = (j, q_2)\} \text{ módulo } q_1 q_2.$$

Cada uno de ellos es coprimo con $q_1 q_2$. Si alguno no lo fuera entonces existiría un primo $p$ divisor tanto de $q_1 q_2$ como de $iq_2 + jq_1$. Como $(q_1, q_2) = 1$ sólo uno de ambos podría ser múltiplo de $p$: supongamos que $p \mid q_2$ (y que no divide a $q_1$). Ahora ocurriría que, como también $p \mid iq_2 + jq_1$, necesariamente $p \mid jq_1$ y por fin -como no divide a $q_1$- $p$ dividiría a $j$. Pero entonces $p \mid (j, q_2)$ y esto contradice que $j$ y $q_2$ son coprimos.

Todos son distintos entre sí. Supongamos que $iq_2 + jq_1 \equiv i^* q_2 + j^* q_1 \pmod{q_1 q_2}$. En este caso $(i - i^*)q_2 - (j - j^*)q_1$ es múltiplo de $q_1 q_2$. En particular $q_1$ divide a $i - i^*$ (pues no puede dividir a $q_2$) y análogamente $q_2$ divide a $j - j^*$. □

**Proposición 3.3.**

1. *Si $n, q$ son primos entre sí entonces $c_q(n) = \mu(q)$.*

2. *Cuando $(n, q) = D > 1$ entonces $c_q(n) = \mu(q/D)\dfrac{\phi(q)}{\phi(q/D)}$.*

*Resumiendo*

$$\boxed{c_q(n) = \mu\left(\frac{q}{(n,q)}\right)\frac{\phi(q)}{\phi\left(\dfrac{q}{(n,q)}\right)} \qquad \forall\, n, q \in \mathbb{N}} \tag{3.8}$$

Una consecuencia de esto es que $c_q(n)$ toma siempre valores enteros, recordando (3.4).

*Demostración.*

1. Dado que $c_q$ es multiplicativa en la variable $q$ (v. lema 3.7), bastará comprobar esta propiedad para las potencias de primo $q = p^r$.

   *a*) En el caso $q = p^1$ por hipótesis $p \nmid n$ y la suma de Ramanujan es la suma de las potencias $n$-ésimas de las $p$-raíces primitivas de la unidad. Puesto que $p \nmid n$ estas potencias $\{e\left(n\frac{i}{p}\right)\}_{i=1,\cdots,p-1}$ son todas distintas entre sí y resultan ser todas las $p$-raíces de la unidad excepto el 1. Por el lema 3.6 $c_p(n) = 0 - 1 = -1 = \mu(p)$.

   *b*) Sea $q = p^r$ $r > 1$ con $p \nmid n$. Los números menores que $p^r$ y que *no* son coprimos con $p^r$ son precisamente los $p^r/p$ múltiplos de $p$ y entonces

   $$c_{p^r}(n) = \sum_{i=1}^{p^r} e\left(n\frac{i}{p^r}\right) - \sum_{j=1}^{p^r/p} e\left(n\frac{jp}{p^r}\right) = 0 - 0 = \mu(p^r),$$

   ya que, teniendo en cuenta que $p \nmid n$ y el lema 3.6, las dos sumas anteriores son nulas porque son, respectivamente, la suma de todas las $p^r$-raíces de la unidad y la suma de todas las $p^{r-1}$-raíces de la unidad.

   Como ejemplo —que se puede confirmar visualmente observando la figura 3.2— notamos que $c_3(1) = \mu(3) = -1$ y que $c_4(1) = \mu(4) = 0$.

2. Sean $q' = q/D$ y $n' = n/D$ entonces $n/q = n'/q'$ y

   $$c_q(n) := \sum_{\substack{i=1\\(i,q)=1}}^{q} e\left(n\frac{i}{q}\right) = \sum_{\substack{i=1\\(i,q)=1}}^{q} e\left(n'\frac{i}{q'}\right).$$

   Por (3.4) cuando $q$ es múltiplo de $q'$ también $\phi(q') \mid \phi(q)$. Si denotamos

   $$A_n := \{i \in \mathbb{N}\colon (i, n) = 1\} \cap [1, n],$$

observamos que $A_q \cap [1, q'] = A_{q'}$ porque $q' \mid q$. Los índices de la última suma son los $\phi(q)$ elementos del conjunto $A_q$ el cual se puede partir en $\frac{\phi(q)}{\phi(q')}$ partes iguales (cada parte con $\phi(q')$ elementos):

$$A_q = \biguplus A_{q'}(j) \qquad \text{siendo } A_{q'}(j) = jq' + A_{q'} \quad j = 0, 1, \ldots$$

es decir $A_{q'}(j)$ es el trasladado de $A_{q'}$ por medio de $jq'$.

El comienzo de la suma, cuando los índices están en $A_{q'}$, es

$$\sum_{\substack{i=1 \\ (i,q')=1}}^{q'} e\left(n' \frac{i}{q'}\right) =: c_{q'}(n').$$

$e\left(n' \frac{i}{q'}\right)$ considerada como función de la variable $i$ es una función con período $q'$

$$e\left(n' \frac{i + jq'}{q'}\right) = e\left(n' \frac{i}{q'}\right),$$

de modo que la suma restringida a los índices de cada una de las partes $A_{q'}(j)$ es siempre igual a $c_{q'}(n')$. Para acabar se utiliza la parte primera de la proposición dado que $n'$ y $q'$ son coprimos

$$\sum_{\substack{i=1 \\ (i,q)=1}}^{q} e\left(n' \frac{i}{q'}\right) = \frac{\phi(q)}{\phi(q')} c_{q'}(n') = \frac{\phi(q)}{\phi(q')} \mu(q').$$

□

## 3.2. Densidad y distribución de los números primos

Recordamos en esta sección algunos resultados clásicos acerca de la densidad y de la distribución de los números primos, que se usan más adelante en este trabajo.

### El teorema de los números primos

Se suele representar por $\pi(n)$ la cantidad de primos menores o iguales que un número entero positivo $n$. Esta función $\pi$ se extiende para cualquier número real mayor que 1 $x \mapsto \pi(\lfloor x \rfloor)$, donde $\lfloor\ \rfloor$ denota la parte entera.

**Teorema 3.1** (Hadamard y De la Vallée-Poussin)**.** Teorema de los números primos
*Si* $\pi(x) = \sum_{p \le x} 1$ *entonces*

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1. \tag{3.9}$$

Definimos también las funciones auxiliares

$$\psi(x) := \sum_{n \le x} \Lambda(n) \qquad \text{y} \qquad \theta(x) := \sum_{p \le x} \log p,$$

que cuentan respectivamente las potencias de primos o bien sólo los primos menores que $x$, dándoles un peso de $\log p$.

**Teorema 3.2** (Chebyshev)**.**

$$\frac{\pi(x)}{x/\log x} \sim \frac{\psi(x)}{x} \sim \frac{\theta(x)}{x}$$

*Demostración.*

$$\theta(x) \le \psi(x) = \sum_{p \le x} \log p \sum_{\substack{m \\ \text{tal que } p^m \le x}} 1 \le \sum_{p \le x} \log p \left\lfloor \frac{\log x}{\log p} \right\rfloor \le (\log x)\pi(x);$$

por otro lado para todo $0 < \alpha < 1$

$$\theta(x) \ge \sum_{x^\alpha < p < x} \log p \ge [\pi(x) - \pi(x^\alpha)] \log(x^\alpha) \ge [\pi(x) - x^\alpha] \log(x^\alpha),$$

entonces

$$\frac{\theta(x)}{x} \ge \alpha \left( \frac{\pi(x)}{x/\log x} - \frac{\log x}{x^{1-\alpha}} \right).$$

□

En este trabajo nos apoyaremos en estimaciones que, como consecuencia del teorema de Chebyshev, son variantes de (3.9). En particular

$$\sum_{p \le x} \log p = x + o(x). \tag{3.10}$$

En muchos libros y otros trabajos se pueden encontrar más detalles sobre el Teorema de los Números Primos (por ejemplo en [M-TB, I-K, M-V] y en español [C-C, Te]).

### 3.2.1. Primos en progresiones aritméticas

#### Caracteres de Dirichlet

Un *carácter de Dirichlet* $\chi\colon \mathbb{Z} \to \mathbb{C}$ es una función aritmética completamente multiplicativa y periódica. Fijado el periodo $m$ entero positivo, para todo entero $n$ se cumple $\chi(n+m) = \chi(n)$; diremos que $\chi$ es un *carácter módulo* $m$.

Conviene definir los caracteres en cualquier grupo finito abeliano de orden $m$: con la notación multiplicativa en $G$ cada carácter es un homomorfismo de grupos $\chi\colon G \to \mathbb{C}^*$.

Se tiene que $\chi(1) = 1$. Como el orden del grupo es $m$ será $1 = \chi(x)^m$ así que el recorrido de $\chi$ son raíces de la unidad, en particular $\overline{\chi(x)} = \chi(x)^{-1}$.

Los caracteres forman también el grupo dual $\widehat{G}$, con la operación multiplicación definida por $(\chi_1\chi_2)(x) := \chi_1(x)\chi_2(x)$. El carácter trivial $\chi_0$, que toma el valor constante 1, es el neutro de $\widehat{G}$.

En el caso particular de que $G$ sea cíclico con generador $g$, cada carácter $\chi$ de $G$ queda totalmente determinado por el valor que toma en $g$:

$$\chi_a(x = g^k) = \chi_a(g)^k = e\left(\frac{ak}{m}\right),$$

en donde $a$ es un residuo entero módulo $m$. Por ello en este caso es sencillo ver que los dos grupos $G$ y $\widehat{G}$ son isomorfos. Esto resulta ser cierto en el caso más general como vemos a continuación y de paso comprobamos que los caracteres multiplicativos detectan a los elementos neutros.

**Lema 3.8** (Relaciones de ortogonalidad)**.** *Si $G$ es grupo abeliano finito con elemento neutro* 1

$$\sum_{x\in G}\chi(x) = \begin{cases} |G| & \textit{si } \chi = \chi_0 \\ 0 & \textit{cuando } \chi \neq \chi_0 \end{cases}$$

$$\sum_{\chi\in\widehat{G}}\chi(x) = \begin{cases} |\widehat{G}| & \textit{si } x = 1 \\ 0 & \textit{cuando } x \neq 1 \end{cases}$$

*Demostración.* Supongamos primero que $G$ es cíclico de orden $m$. Fijado un carácter $\chi \neq \chi_0$

$$\sum_{x\in G}\chi(x = g^k) = \sum_{k=0}^{m-1}\chi(g)^k = \frac{\chi(g)^m - 1}{\chi(g) - 1} = 0.$$

Sea ahora un $x = g^y \in G$ fijo. Tenemos que

$$\sum_{\chi\in\widehat{G}}\chi(x) = \sum_{a=0}^{m-1} e\left(\frac{y}{m}\right)^a.$$

Cuando $x = 1$ es $y = m$ y la suma da $m$, y cuando $y < m$ la raíz de la unidad $e\left(\frac{y}{m}\right) = \rho$ es distinta del 1 y satisface la ecuación

$$0 = \rho^m - 1 = (\rho - 1)(\rho^{m-1} + \rho^{m-2} + \cdots + 1),$$

por tanto la suma (que es el segundo factor en la derecha) se anula.

En el caso más general en que $G$ es un grupo abeliano finito recordamos un teorema en virtud del cual se puede poner como producto directo de varios grupos cíclicos. El

ingrediente que falta para completar la prueba del lema es el siguiente. Ahora sean $G_1$ y $G_2$ grupos finitos y abelianos y tomemos $G = G_1 \otimes G_2$, entonces todo carácter $\chi$ multiplicativo en $G$ se expresa de modo único como producto

$$\chi = \chi_1 \, \chi_2,$$

donde $\chi_i$ es un carácter multiplicativo en $G_i$ $i = 1, 2$. Efectivamente si $e_i$ es el elemento neutro de $G_i$ dado $\chi \in \widehat{G}$ ponemos $\chi_1(x_1) = \chi(x_1, e_2)$ y $\chi_2(x_2) = \chi(e_1, x_2)$ de modo que para cualquier elemento $x = (x_1, x_2)$ de $G$ se tiene $\chi(x) = \chi_1(x_1)\chi_2(x_2)$. Se deduce que $G$ y su dual son isomorfos

$$\widehat{G} \cong \widehat{G}_1 \otimes \widehat{G}_2 \cong G_1 \otimes G_2 = G.$$

Además

$$\text{fijado } \chi \in \widehat{G} \qquad \sum_{x \in G} \chi(x) = \left( \sum_{x_1 \in G_1} \chi_1(x_1) \right) \left( \sum_{x_2 \in G_2} \chi_2(x_2) \right),$$

$$\text{fijado } x \in G \qquad \sum_{\chi \in \widehat{G}} \chi(x) = \left( \sum_{\chi_1 \in \widehat{G}_1} \chi_1(x_1) \right) \left( \sum_{\chi_2 \in \widehat{G}_2} \chi_2(x_2) \right).$$

En consecuencia $G$ satisface las relaciones de ortogonalidad si ambos $G_1$ y $G_2$ las cumplen. □

| | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $\chi_0$ | 0 | 1 | 1 | 1 | 1 |
| $\chi_1$ | 0 | 1 | $-i$ | $i$ | $-1$ |
| $\chi_2$ | 0 | 1 | $-1$ | $-1$ | 1 |
| $\chi_3$ | 0 | 1 | $i$ | $-i$ | $-1$ |

Figura 3.3: Caracteres de Dirichlet módulo 5

**Ejemplo** (v. figura 3.3) $g = 3$ es generador de $\mathcal{U}(\mathbb{F}_5)$ : $2 = 3^3,\ 3 = 3^1,\ 4 = 3^2$.

$$\chi_1(2) = i^3 = -i \qquad \chi_1(3) = e\,(1/4) = i \qquad \chi_1(4) = i^2 = -1$$
$$\chi_2(2) = (-1)^3 = -1 \qquad \chi_2(3) = e\,(2/4) = -1 \qquad \chi_2(4) = (-1)^2 = 1$$
$$\chi_3(2) = (-i)^3 = i \qquad \chi_3(3) = e\,(3/4) = -i \qquad \chi_3(4) = (-i)^2 = -1$$

Cada carácter de Dirichlet $\chi$ módulo $m$ se define en todos los enteros partiendo de un carácter módulo $m$ en el grupo multiplicativo de las unidades del anillo $\mathbb{Z}/m\mathbb{Z}$. La extensión a todo $\mathbb{Z}$ como una función aritmética se completa definiendo $\chi(n) = 0$ cuando $(n, m) > 1$ y luego extendiendo a todo $n \in \mathbb{Z}$ con periodicidad $m$: $\chi(n + m) = \chi(n)$.

De las relaciones de ortogonalidad se deduce una fórmula que, usando como ingredientes todos los caracteres de Dirichlet módulo $q$, permite detectar a los miembros de una progresión aritmética. Sea $1_A$ la función característica de un conjunto $A$ cualquiera, y sea

$$\mathcal{A}[a, q] = \{n \in \mathbb{Z} \colon q \mid n - a\}$$

una progresión aritmética con diferencia $q$.

**Lema 3.9.** *Si $a, n$ son enteros y $(a, q) = 1$*

$$\frac{1}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi}(a)\chi(n) = \left\{ \begin{array}{ll} 1 & \textit{si } n \equiv a \pmod q \\ 0 & \textit{en otro caso} \end{array} \right\} = 1_{\mathcal{A}[a,q]}(n).$$

*donde la suma recorre todos los caracteres módulo $q$.*

*Demostración.* El grupo multiplicativo $\mathcal{U}(\mathbb{Z}/q\mathbb{Z})$ de las unidades de $\mathbb{Z}/q\mathbb{Z}$ es abeliano y finito, así que podemos usar el lema 3.8. Dado que $(a, q) = 1$, llamemos $a^{-1}$ al inverso de $a$ módulo $q$.

Cuando $n \equiv a \pmod q$ entonces $a^{-1}n \equiv 1 \pmod q$ y

$$\frac{1}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi(a)}\chi(n) = \frac{1}{\phi(q)} \sum_{\chi \bmod q} \chi(a)^{-1}\chi(n) = \frac{1}{\phi(q)} \sum_{\chi \bmod q} \chi(a^{-1}n) = 1.$$

Suponemos ahora que $n \not\equiv a \pmod q$. Tendremos $a^{-1}n \not\equiv 1 \pmod q$ y

$$0 = \frac{1}{\phi(q)} \sum_{\chi \bmod q} \chi(a^{-1}n) = \frac{1}{\phi(q)} \sum_{\chi \bmod q} \chi(a)^{-1}\chi(n) = \frac{1}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi(a)}\chi(n).$$

□

Como cualquier carácter de Dirichlet es una función completamente multiplicativa, se tiene una identidad del tipo producto de Euler que generaliza la ecuación (3.1):

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p)^2}{(p^2)^s} \cdots\right) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

V. en [R] un estudio más amplio y general acerca de los caracteres.

Figura 3.4: P.G. *Lejeune* Dirichlet

**El teorema de los primos en progresiones aritméticas**

Un ingrediente fundamental para abordar en los capítulos siguientes las sumas de primos será su distribución en progresiones aritméticas.

Sea $\pi(x;a,q)$ la cantidad de primos menores o iguales que $x$ en una progresión aritmética $\{qn+a\}$ con $a,q$ primos entre sí

$$\pi(x;a,q) := \sum_{\substack{p\leq x \\ p\equiv a \text{ mód } q}} 1.$$

Definimos también

$$\psi(x;a,q) := \sum_{\substack{n\leq x \\ n\equiv a \text{ mód } q}} \Lambda(n),$$

y para cualquier carácter de Dirichlet $\chi$ módulo $q$

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

El Teorema de los números primos en progresiones aritméticas afirma que cada clase residual $a$ módulo $q$, con $(a,q)=1$, contiene la misma proporción de números primos:

**Teorema 3.3.**

$$\pi(x;a,q) \sim \frac{1}{\phi(q)}\pi(x) \tag{3.11}$$

$$\psi(x;a,q) \sim \frac{1}{\phi(q)}\psi(x) \tag{3.12}$$

Más importante que el término de error en las estimaciones anteriores es el rango de uniformidad para el módulo $q$ en términos de $x$ que nos da el resultado siguiente.

**Teorema 3.4** (Siegel-Walfisz)**.** *Dados cualesquiera $C > 0$ y $a, q$ enteros positivos primos entre sí, tenemos para todo $x \geq 2$:*

$$\psi(x; a, q) = \frac{x}{\phi(q)} + O\left(\frac{x}{(\log x)^C}\right) = \frac{x}{\phi(q)}\left(1 + O\left(\frac{\phi(q)}{(\log x)^C}\right)\right) \tag{3.13}$$

$$\sum_{\substack{p \leq x \\ p \equiv a \bmod q}} \log p = \frac{x}{\phi(q)}\left(1 + O\left(\frac{\phi(q)}{(\log x)^C}\right)\right) \tag{3.14}$$

$$\psi(x, \chi) = O\left(\frac{x}{(\log x)^C}\right) \quad si \quad \chi \neq \chi_0 \qquad y \quad \psi(x, \chi_0) = x + O\left(\frac{x}{(\log x)^C}\right) \tag{3.15}$$

*La constante implícita en el término $O$ sólo depende de $C$.*

Para más detalles se puede consultar por ejemplo [Ch-3], [I-K, §5.9] y/o [Ch-2, §3.3].

Recordamos en este punto las acotaciones (3.6) (v. página 20)

$$q^{1-\delta} \ll \phi(q) \leq q \qquad \text{para todo } \delta > 0.$$

Nótese que la estimación en (3.13) es no trivial solamente si $q \ll (\log x)^C$ pues la cota del cociente entre los (candidatos a) término de error y a término principal es

$$\frac{\phi(q)}{(\log x)^C} \gg \frac{q^{1-\delta}}{(\log x)^C} \qquad \forall\, \delta > 0, \quad C > 0.$$

« Se puede interpretar el Teorema de Siegel-Walfisz diciendo que cada clase residual tiene, con una aproximación de primer orden, el mismo número de primos. Explícitamente: fijado $q$ hay $\phi(q)$ números coprimos con $q$. Salvo por términos de menor magnitud cada clase residual tiene $\pi(x)/\phi(q)$ primos. [...] Si tomásemos $q$ tan grande como $x^\epsilon$ para algún $\epsilon > 0$ entonces el término de error superaría al término principal; queremos aplicar este teorema cuando $q$ es mucho más pequeño que $x$.» [M-TB, pág. 314]

# Capítulo 4

# Pequeños grandes arcos

En este capítulo introducimos y estudiamos una función $F_N(x)$ cercana a la función $f_N(x) := \sum_{p\leq N} e(px)$ que aparece dentro de la integral

$$r(N;k,\mathcal{P}) = \int_0^1 [f_N(x)]^k e(-Nx)\,\mathrm{d}x, \tag{4.1}$$

(v. lema 2.1) con el propósito de identificar al conjunto $\mathcal{M}$ de arcos mayores más apropiado para el problema de la representación con $k$ sumandos primos. El fruto principal de este empeño es la proposición 4.3, resultado que prepara el terreno para abordar con éxito en el capítulo 5 el caso de $k \geq 3$ sumandos.

El *objeto de deseo* es abrir camino hacia la solución de la conjetura de Goldbach. El método del círculo permite "reducir" el problema original al de estimar la integral

$$\int_0^1 \left(\sum_{p\leq N} e(px)\right)^k e(-Nx)\,\mathrm{d}x.$$

¿Se puede estimar una expresión como $\sum_{p\leq N} e(px)$ que mezcla números primos y exponenciales? Como ya anticipamos al concluir el capítulo 2, la estrategia será estimar, en torno a los $x$ adecuadamente elegidos, las sumas que van recorriendo todos los números primos $\mathcal{P}$ menores o iguales que $N$, subdividiéndolas en distintas sumas que recorren progresiones aritméticas de primos. Para poner en funcionamiento esta idea echaremos mano de los ingredientes presentados en el capítulo 3.

## 4.1. Segunda intuición heurística

Siguiendo a [Ch-2, §4.2] empezamos *a vueltas con el círculo*, para engrasar la intuición.

Como ejemplo de lo expuesto en el Capítulo 2, pongamos ahora $\mathcal{A} = \mathcal{P}$, $k = 2$ y soltemos lastre de notación escribiendo $r_2(N)$ en lugar de $r(N;2,\mathcal{P})$. Recordando (2.2), en este contexto tenemos que

$$r_2(N) = \int_0^1 [f_N(x)]^2 e(-Nx)\,\mathrm{d}x \qquad f_N(x) = \sum_{p\le N} e(px). \tag{4.2}$$

Llamando $D_N(x) := \sum_{n\le N} e(nx)$, tanto $D_N$ como $f_N$ son funciones continuas y cuando $x$ está cerca de 0, por el TEOREMA DE LOS NÚMEROS PRIMOS (3.9),

$$x \approx 0 \qquad \Rightarrow \qquad f_N(x) \approx f_N(0) = \pi(N) \sim \frac{N}{\log N} = \frac{D_N(0)}{\log N} \approx \frac{D_N(x)}{\log N};$$

es decir $f_N(x) \approx D_N(x)/\log N$ cuando $x \approx 0$ y $N$ es grande (ponemos $g \approx h$ para expresar que $g$ está cerca de $h$).

Analizamos ahora el valor de $f_N(x)$ en las cercanías de un $x \in (0,1)$ cualquiera que tenga la forma de una fracción irreducible $x = a/q$. Para hacerlo echamos mano del TEOREMA DE LOS NÚMEROS PRIMOS EN PROGRESIONES ARITMÉTICAS (v. teorema 3.3).

Por ejemplo para $a = 1, q = 3$ y $N$ suficientemente grande, aproximadamente la mitad de los primos menores que $N$ son congruentes con 1 módulo 3 y la (otra) mitad de los primos menores que $N$ son congruentes con 2 módulo 3. Además cuando $p \equiv 1 \pmod 3$ se tiene $e(p/3) = e(1/3)$ y análogamente $e(p/3) = e(2/3)$ cuando $p \equiv 2 \pmod 3$. En consecuencia cuando $x$ está cerca de $1/3$

$$\begin{aligned} f_N(x) &\approx f_N(1/3) \sim \frac{\pi(N)}{2} e(1/3) + \frac{\pi(N)}{2} e(2/3) \\ &\sim \frac{N/\log N}{2} e(1/3) + \frac{N/\log N}{2} e(2/3) \\ &= \left(\frac{e(1/3)}{2\log N} + \frac{e(2/3)}{2\log N}\right) N = \frac{-1}{2\log N} N = -\frac{D(0)}{2\log N} \approx -\frac{D_N(x-1/3)}{2\log N} \end{aligned}$$

En el caso general para cualquier número entero positivo $q \ge 2$ hay aproximadamente $\pi(N)/\phi(q)$ primos menores que $N$ y congruentes con $r_i$, para cada uno de los $r_i \in \{r_1, \dots r_{\phi(q)}\}$ residuos coprimos con $q$, por (3.11).

Para cualquier primo $p$ menor que $N$ existe $i$ tal que $p \equiv r_i \pmod q$ y como $p = r_i + mq$ entonces $e\left(p\frac{a}{q}\right) = e\left(r_i\frac{a}{q}\right)$. Cuando $x$ está cerca de la fracción irreducible $a/q$

$$\begin{aligned} f_N(x) \approx f_N(a/q) &= \sum_{p\le N} e\left(p\frac{a}{q}\right) = \sum_{i=1}^{\phi(q)} \sum_{\substack{p\equiv r_i(q)\\ p\le N}} e\left(r_i\frac{a}{q}\right) \\ &\sim \frac{\pi(N)}{\phi(q)} \left[e\left(\frac{r_1}{q}\right)^a + \cdots + e\left(\frac{r_{\phi(q)}}{q}\right)^a\right] \sim \frac{N}{\phi(q)\log N} c_q(a) \\ &= \frac{c_q(a)}{\phi(q)\log N} D_N(0) \approx \frac{\mu(q)}{\phi(q)\log N} D_N(x - a/q). \end{aligned}$$

Aquí hemos reconocido a la suma de Ramanujan $c_q(a)$ cuyo valor es igual $\mu(q)$ (v. proposición 3.3 en la página 23). Todo lo antedicho sugiere que es posible aproximar $f_N$ del modo siguiente:

$$f_N(x) = \frac{\mu(q)}{\phi(q)\log N} D_N\left(x - \frac{a}{q}\right) + Err(x), \tag{4.3}$$

confiando en acotar convenientemente el término de error $Err(x)$ cuando $x$ está cerca de la fracción irreducible $a/q$. De modo que en torno a cada uno estos puntos tengamos un arco mayor. De ser así el conjunto $\mathcal{M}$ de estos arcos mayores aportaría una estimación de $f_N$ suficientemente buena que a su vez contribuiría significativamente a la estimación asintótica de $r_2$ por medio de la fórmula (4.2).

Pasamos ahora de puntillas por encima de varios detalles —que se analizarán más adelante en este trabajo— como son (entre otros): que los intervalos alrededor de los racionales $a/q$ que componen $\mathcal{M}$ son disjuntos, que $q$ no puede ser demasiado grande y que no se pierde mucho aproximando

$$\int_{|u|<\epsilon} D^2(u) e\left(-Nu\right)\,\mathrm{d}u \qquad \text{por} \qquad \int_0^1 D^2(u) e\left(-Nu\right)\,\mathrm{d}u.$$

La contribución a $r_2(N)$ de la parte principal de la aproximación 4.3 en los arcos mayores es (sin usar de momento el pincel fino):

$$\begin{aligned}
&\int_{\mathcal{M}} [f_N(x)]^2 e\left(-N(x)\right)\,\mathrm{d}x \approx \int_{\mathcal{M}} \left[\frac{\mu(q)}{\phi(q)\log N} D_N\left(x-\frac{a}{q}\right)\right]^2 e\left(-N(x)\right)\,\mathrm{d}x = \\
&= \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \frac{\mu^2(q)}{\phi^2(q)(\log N)^2} \int_{|u|<\epsilon} [D_N(u)]^2 \cdot e\left(-N\left(u+\frac{a}{q}\right)\right)\,\mathrm{d}u \approx \\
&\approx \int_0^1 [D_N(u)]^2 e\left(-Nu\right)\,\mathrm{d}u \cdot \sum_{q=1}^{\infty} \left[\frac{\mu^2(q)}{\phi^2(q)(\log N)^2} \cdot \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e\left(-Na/q\right)\right] \sim \\
&\sim N \cdot \sum_{q=1}^{\infty} \frac{\mu^2(q)}{\phi^2(q)(\log N)^2} \cdot c_q(-N) = \frac{N}{(\log N)^2} \sum_{q=1}^{\infty} \frac{\mu^2(q) c_q(-N)}{\phi^2(q)},
\end{aligned}$$

tras un cambio de variable en la integral y notando que —como veremos más adelante en el lema 4.4—

$$\int_0^1 [D_N(u)]^2 e\left(-Nu\right)\,\mathrm{d}u \sim N.$$

La suma $\sum c_q(-N)\mu^2(q)/\phi^2(q)$ se puede estimar asintóticamente por un cierto producto con números primos (v. proposición 4.2 en la página 48).

Si pudiésemos además contar con que la contribución a $r_2(N)$ en los arcos menores —haciendo honor a su apellido— fuese relativamente *menor* en orden de magnitud, entonces la conclusión podría ser

$$r_2(N) \sim \frac{N}{(\log N)^2} \prod_{p|N}\left(1+\frac{1}{p-1}\right) \prod_{p\nmid N}\left(1-\frac{1}{(p-1)^2}\right) \qquad N \text{ par}, \tag{4.4}$$

fórmula que coincide con (1.4), que ya conjeturamos probabilísticamente en la página 7.

Nótese que cuando $N$ es impar el factor correspondiente al primo $p = 2$ es cero y anula todo el producto evaporándose la estimación en este caso.

En [Ch-2, §4.2] se observa lo siguiente:

> "El fallo no está en los pasos anteriores, que son incondicionalmente ciertos, sino en la imposibilidad de probar que la contribución de los arcos menores es pequeña. [...] ¿No significa esto que es imposible que la contribución heurística de los arcos mayores que hemos hallado antes sea correcta? De ningún modo, porque al estimar la contribución de los arcos menores mediante una cota superior estamos perdiendo el signo, es plausible que al integrar y sumar en los arcos menores haya mucha cancelación."

## 4.2. La función generatriz en los arcos mayores

Tal y como se hace en otros contextos en Teoría de Números ponderamos la aportación de cada primo $p$ con el peso $\log p$. De esta manera se simplifican algunos pasos y fórmulas. Casi al final de este trabajo se deduce con poco esfuerzo desde el resultado para este caso ponderado el resultado correspondiente al caso más natural en que cada primo contribuye con peso igual a 1 (v. teorema 5.3).

Esta decisión produce la siguiente variante de *caja de herramientas* con el método del círculo (v. capítulo 2):

$$F_{\mathcal{P}}(z) := \sum_{p\in\mathcal{P}} \log p \cdot z^p, \qquad F_N(x) := \sum_{p\le N} \log p \cdot e\left(px\right).$$

$$R(N;k,\mathcal{P}) := \sum_{p_1+\cdots+p_k=N} (\log p_1)\cdots(\log p_k) = \int_0^1 [F_N(x)]^k e\left(-Nx\right)\,\mathrm{d}x.$$

En valor absoluto $F_N$ está acotada por una función que asintóticamente es como $N$

$$|F_N(x)| \le \sum_{p\le N} \log p = N + o(N),$$

por el Teorema de los Números Primos (3.10).

Como veremos $|F_N|$ es de tamaño $N$ para ciertos $x$ que serán los puntos centrales de los arcos mayores. En primera instancia lo es para $x = 0, 1$ y para $x = 1/2$:

$$F_N(0) = F_N(1) = \sum_{p \le N} \log p = N + o(N).$$

Como para todo primo impar $e\,(p/2) = e\,(1/2) = -1$ entonces

$$F_N(1/2) = \log 2\; e\,(1) + \sum_{3 \le p \le N} \log p\; e\,(1/2) = \log 2 - \sum_{3 \le p \le N} \log p = -N + o(N).$$

Sin embargo $(F_N)^2$ es, en valor medio, significativamente menor que $N^2$.

**Lema 4.1.**

$$\int_0^1 |F_N(x)|^2 \, \mathrm{d}x = N \log N + o(N \log N) \tag{4.5}$$

*Demostración.*

$$\begin{aligned}
\int_0^1 |F_N(x)|^2 \, \mathrm{d}x &= \int_0^1 F_N(x)\overline{F_N(x)} \, \mathrm{d}x \\
&= \int_0^1 \left( \sum_{p_1 \le N} \log p_1 \cdot e\,(p_1 x) \right) \left( \sum_{p_2 \le N} \log p_2 \cdot e\,(-p_2 x) \right) \mathrm{d}x \\
&= \sum_{p_1, p_2 \le N} \log p_1 \log p_2 \int_0^1 e\,((p_1 - p_2)x) \, \mathrm{d}x = \sum_{p \le N} (\log p)^2 \\
&= N \log N + o(N \log N),
\end{aligned}$$

en donde hemos usado (2.1). La última estimación se obtiene de (3.10) como sigue

$$\sum_{p \le N} \log^2 p \le \log N \sum_{p \le N} \log p \sim \log N (N + o(N)).$$

□

Asintóticamente el valor máximo de $(F_N)^2$ es $N^2$ y la media de $(F_N)^2$ es como $N \log N$, significativamente menos que el máximo. Consistentemente, $F_N$ en media ha de parecerse a $\sqrt{N \log N}$. Esto lleva a sospechar que, para muchos $x$ en el intervalo $[0, 1]$, dentro de la suma $F_N(x)$ se producen gran cantidad de cancelaciones entre distintos sumandos, haciendo que $F_N(x)$ sea comparable a $\sqrt{N \log N}$ en estos $x$.

Vamos a deslindar estos candidatos a arcos menores $\mathfrak{m}$ identificando con precisión a su complementario $\mathcal{M}$.

### Tamaño de la función en racionales de denominador pequeño

Sea un número real $B > 0$ fijo cualquiera y tomemos $Q = (\log N)^B$. Dentro de $[0,1]$ fijamos la atención en los racionales $0 < a/q < 1$ que cumplen $q \leq Q$ y $(a,q) = 1$; su denominador es pequeño en comparación con $N$. En estos puntos analizamos $F_N$ desglosando la suma según progresiones aritméticas, recordando que cuando $p \equiv r$ mód $q$ entonces $e\,(pa/q) = e\,(ra/q)$:

$$F_N\left(\frac{a}{q}\right) = \sum_{p\leq N} \log p \cdot e\left(p\frac{a}{q}\right) = \sum_{r=1}^{q} e\left(r\frac{a}{q}\right) \left[\sum_{\substack{p\leq N \\ p\equiv r \text{ mód } q}} \log p\right]$$

$$= \sum_{\substack{r=1 \\ (r,q)=1}}^{q} e\left(r\frac{a}{q}\right) \left[\sum_{\substack{p\leq N \\ p\equiv r \text{ mód } q}} \log p\right] + Err(a/q), \tag{4.6}$$

en donde separamos en la última suma los residuos que son coprimos con $q$ de los que no lo son. También hemos reconocido a la suma de Ramanujan $c_q(a)$ cuyo valor, al ser $(a,q) = 1$, es $\mu(q)$, por la proposición 3.3 en la página 23.

Los residuos que no son coprimos con $q$ forman un término de error $Err$ despreciable respecto a la aportación de los residuos coprimos. Efectivamente $p \equiv r \pmod q$ y $(q,r) > 1$ si y sólo si $p \mid q$ : como $p = qk + r \quad (r,q) > 1$ necesariamente $p = r, k = 0$ porque el primo $p$ no puede ser múltiplo de $(r,q) > 1$. Esto implica que $p \mid q$. Así

$$Err(a/q) = \sum_{\substack{r=1 \\ (r,q)>1}}^{q} e\left(r\frac{a}{q}\right) \left[\sum_{\substack{p\leq N \\ p\equiv r \text{ mód } q}} \log p\right] = \sum_{\substack{p\leq N \\ p\mid q}} e\left(p\frac{a}{q}\right) \log p \ll$$

$$\ll \sum_{\substack{p\leq N \\ p\mid q}} \log p \leq \log q \ll \log Q.$$

En este punto echamos mano del Teorema de Siegel-Walfisz (3.14) para estimar la suma que aparece entre corchetes dentro del candidato a término principal en (4.6). Esto nos da la siguiente estimación para cualquier $C > 0$

$$F_N\left(\frac{a}{q}\right) = \sum_{\substack{r=1 \\ (r,q)=1}}^{q} e\,(ar/q) \left[\frac{N}{\phi(q)} + O\left(\frac{N}{\log^C N}\right)\right] + O\,(\log Q)$$

$$= \frac{N}{\phi(q)} c_q(a) + O\left(\frac{qN}{\log^C N}\right) + O\,(\log Q) =$$

$$= \frac{N}{\phi(q)} c_q(a) + O\left(\frac{QN}{\log^C N}\right) = \frac{N}{\phi(q)}\mu(q) + O\left(\frac{N}{(\log N)^{C-B}}\right). \tag{4.7}$$

Observamos que si escogemos $C$ más grande que $B$ (por ejemplo $C > 2B$) el primer término prevalece asintóticamente sobre el segundo término y en conclusión $F_N(a/q)$ es asintóticamente de tamaño proporcional a $N$ si $q$ es libre de cuadrados.

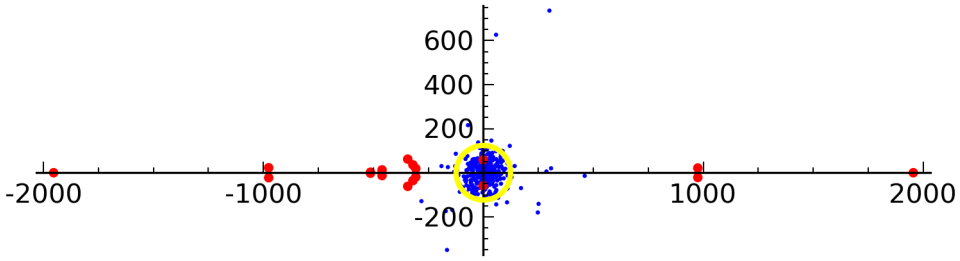


Figura 4.1: Algunos valores de $F_{2011}(a/q)$

En la figura (4.1) exhibimos la gráfica de una muestra (pseudo)aleatoria de la imagen de la función $F_N(x) = \sum_{p \leq N} \log p \cdot e(px)$ en el plano complejo, calculada con el valor $N = 2011$. Aparecen dibujados más de 300 números complejos $F_N(a/q)$ con $a/q$ racional menor que 1. Los puntos para los que $q \leq (\log N)^{3/2}$ y $(a, q) = 1$ son de color rojo y el resto de puntos tienen color azul. En amarillo se muestra la circunferencia de radio $\sqrt{N \log N}$ centrada en el origen. (Preparado con SAGE www.sagemath.org)

### Tamaño de la función en el arco mayor

La elección de los arcos mayores está influida de modo crucial por el término de error del Teorema 3.4 (Siegel-Walfisz). En primer lugar definimos un *pequeño arco mayor*, intervalo centrado en el racional $a/q$

$$\mathcal{M}_{a/q} = \left\{ x \in [0,1] \colon \left| x - \frac{a}{q} \right| < \frac{Q}{N} \right\} \qquad q \leq Q = (\log N)^B.$$

Para $N$ suficientemente grande estos intervalos son siempre disjuntos dos a dos. Efectivamente si se diera el caso de que $y \in \mathcal{M}_{a/q} \cap \mathcal{M}_{a'/q'}$ tendríamos una pareja de estos racionales a distancia menor que $2Q/N$

$$\left| \frac{a}{q} - \frac{a'}{q'} \right| \leq \left| \frac{a}{q} - y \right| + \left| y - \frac{a'}{q'} \right| < \frac{2Q}{N}$$

y a la vez mayor que $1/Q^2$

$$\left| \frac{a}{q} - \frac{a'}{q'} \right| = \frac{|aq' - a'q|}{qq'} \geq \frac{1}{qq'} \geq \frac{1}{Q^2}$$

y por tanto $N < 2Q^3 = 2(\log N)^{3B}$ lo que es falso para $N$ suficientemente grande porque como $B > 0$ ocurre que $(\log N)^{3B} = o(N)$.

Tras desenrollar el círculo (v. figura 2.2 en la página 11) no olvidamos el arco mayor que reposa en el 0 (o en el 1)

$$\mathcal{M}_{1/1} = \left(1 - \frac{Q}{N}, 1\right] \cup \left[0, \frac{Q}{N}\right)$$

Finalmente el conjunto de **los arcos mayores** es la reunión de todos estos intervalos:

$$\mathcal{M} = \bigcup_{1 \le q \le Q} \bigcup_{\substack{a=1 \\ (a,q)=1}}^{q} \mathcal{M}_{a/q}$$

Nótese que $\mathcal{M}$ depende de $N$ y de $B$, aunque no lo reflejaremos en la notación. Se trata de una parte esquelética de $[0,1]$ en el sentido de que su medida $m$ de Lebesgue tiende a cero

$$m(\mathcal{M}) \le \sum_{q=1}^{Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} m(\mathcal{M}_{a/q}) \le Q\phi(Q)\frac{2Q}{N} \le \frac{2Q^3}{N} = 2\frac{(\log N)^{3B}}{N} \overset{N\to\infty}{\longrightarrow} 0.$$

Definimos **los arcos menores** como

$$\mathfrak{m} := [0,1] \setminus \mathcal{M}.$$

El adjetivo *mayores* resalta que la aportación estos *arcos* es predominante respecto a la del resto de puntos del *círculo*; aunque la mayoría del círculo consista de *arcos menores*.

Si evitamos la frontera de $[0,1]$ tomando $q \ge 2$, a lo largo de cada intervalo $\mathcal{M}_{a/q}$ la función $F_N(x)$ es asintóticamente similar a $F_N(a/q)$ (porque el diámetro del intervalo se estrecha cuando $N$ crece) y por tanto -cuando $q$ es libre de cuadrados- es grande en valor absoluto, de tamaño similar a $N$ según la estimación (4.7).

Esta observación se precisa con el siguiente resultado que culmina esta sección del trabajo.

**Proposición 4.1.** *Sea $\mathcal{M}_{a/q}$ un arco mayor, es decir, un intervalo de diámetro $Q/N$ centrado en el racional irreducible $a/q$, el cual tiene denominador $q$ menor que $Q$. Aquí $Q = (\log N)^B$ es pequeño en relación con $N$ ($B > 0$ es una constante cualquiera).*

*En $\mathcal{M}_{a/q}$ la función $F_N(x) := \sum_{p \le N} \log p \; e(px)$ se aproxima asintóticamente de modo que*

$$\boxed{F_N(x) = \frac{\mu(q)}{\phi(q)} D_N(x - a/q) + O\left(\frac{N}{(\log N)^{4B}}\right) \quad \forall\, x \in \mathcal{M}_{a/q},} \tag{4.8}$$

*en donde $D_N(x) = \sum_{n \le x} e(nx)$ y $\mu, \phi$ son las funciones aritméticas presentadas en la sección 3.1*

*Demostración.*

**Primer paso**

Añadiendo a la suma $F_N$ las potencias de los primos y quedándose sólo con los términos $n$-ésimos cuando $n$ es coprimo con $q$ tenemos otra suma cuya distancia a $F_N$ podemos acotar convenientemente:

$$F_N(x) = \sum_{\substack{n\leq N\\(n,q)=1}} \Lambda(n)e\,(nx) + O(\sqrt{N}). \tag{4.9}$$

La razón es que tenemos para el término de error

$$Err(x) = \sum_{\substack{n\leq N\\(n,q)=1}} e(nx)\Lambda(n) - F_N(x) = \sum_{\substack{p^r\leq N\ r>1\\(p,q)=1}} e(p^r x)\log p - \sum_{\substack{p\leq N\\(p,q)>1}} e(px)\log p,$$

y $(p,q) > 1$ precisamente cuando $p$ es un factor primo de $q$. Además $p^r \leq N$ $r > 1$ implica $p \leq \sqrt{N}$. En consecuencia, si la factorización de $q$ es $q = \pi_1^{e_1}\cdots\pi_k^{e_k}$

$$\begin{aligned}|Err(x)| &\leq \sum_{p^r\leq N\ r>1} \log p + \sum_{j=1}^{k}\log \pi_k \leq \sum_{p\leq\sqrt{N}} \log p + \sum_{j=1}^{k} e_k \log \pi_k \ll\\ &\ll \sqrt{N} + o(\sqrt{N}) + \log q \leq \sqrt{N} + o(\sqrt{N}) + B\log\log N = \sqrt{N} + o(\sqrt{N}),\end{aligned}$$

en donde hemos usado el Teorema de los Números Primos (3.10).

**Segundo paso**

Abreviamos $h = x - a/q$ de modo que $e\,(nx) = e\,(na/q)\,e\,(nh)$.

Cuando $n \equiv r \pmod q$ se tiene $e\,(na/q) = e\,(ra/q)$ y usando los caracteres módulo $q$ para detectar progresiones aritméticas (v. lema 3.9 en la página 29) tenemos

$$\begin{aligned}F_N(x) &= \sum_{\substack{n\leq N\\(n,q)=1}} \Lambda(n)e\,(nx) + O(\sqrt{N})\\ &= \sum_{\substack{r=1\\(r,q)=1}}^{q} e\left(r\frac{a}{q}\right) \sum_{\substack{n\leq N\\ n\equiv r \bmod q}} \Lambda(n)e\,(nh) + O(\sqrt{N})\\ &= \sum_{\substack{r=1\\(r,q)=1}}^{q} e\left(r\frac{a}{q}\right) \left[\sum_{n\leq N}\left(\frac{1}{\phi(q)}\sum_{\chi \bmod q}\overline{\chi}(r)\chi(n)\right)\Lambda(n)e\,(nh)\right] + O(\sqrt{N})\\ &= \frac{1}{\phi(q)}\sum_{r=1}^{q} e\left(r\frac{a}{q}\right)\left[\sum_{\chi \bmod q}\overline{\chi}(r)\sum_{n\leq N}\chi(n)\Lambda(n)e\,(nh)\right] + O(\sqrt{N}),\end{aligned}$$

puesto que si $(q,r)>1$ se tiene $\overline{\chi}(r)=0$. La suma $\sum_{\chi \bmod q}$ recorre todos los caracteres módulo $q$.

Llamando

$$\tau(\overline{\chi},a) := \sum_{m=1}^{q} \overline{\chi}(m) e\left(m\frac{a}{q}\right),$$
$$\psi_h(N,\chi) := \sum_{n\le N} \chi(n)\Lambda(n) e\,(nh)\,, \qquad \text{en particular } \psi(N,\chi)=\psi_0(N,\chi),$$

y reagrupando sumandos esto es lo mismo que

$$F_N(x) = \frac{1}{\phi(q)} \sum_{\chi \bmod q} \tau(\overline{\chi},a)\ \psi_h(N,\chi) + O(\sqrt{N}), \tag{4.10}$$

donde la suma recorre todos los caracteres módulo $q$.

- Analizamos primero el caso $\chi \neq \chi_0$.

  Por un lado sumando por partes (v. lema 3.5) con $f(n)=\chi(n)\Lambda(n)$ y $g(n)=e\,(nh)$

  $$\psi_h(N,\chi) = \psi(N,\chi)e\,(Nh) - 2\pi i h \int_1^N \psi(u,\chi)e\,(uh)\ \mathrm{d}u,$$

  y entonces

  $$\begin{aligned}|\psi_h(N,\chi)| &\le |\psi(N,\chi)| + 2\pi\,|h| \int_1^N |\psi(u,\chi)|\ \mathrm{d}u \\ &\ll \frac{N}{(\log N)^{6B}} + |h|N\ \frac{N}{(\log N)^{6B}} = (1+|h|N)\ \frac{N}{(\log N)^{6B}}.\end{aligned}$$

  En el último paso hemos usado el Teorema de Siegel-Walfisz escogiendo $C=6B$ (v. (3.15) en la página 31).

  Por otro lado

  $$\begin{aligned}\sum_{\substack{\chi \bmod q\\ \chi\neq\chi_0}} |\tau(\overline{\chi},a)|^2 &\le \sum_{\chi \bmod q} |\tau(\overline{\chi},a)|^2 = \sum_{\chi \bmod q} \overline{\tau(\overline{\chi},a)}\tau(\overline{\chi},a) \\ &= \sum_{\chi \bmod q} \left[\sum_{m=1}^{q} \chi(m) e\left(-m\frac{a}{q}\right)\right]\left[\sum_{n=1}^{q} \overline{\chi}(n) e\left(n\frac{a}{q}\right)\right] = \\ &= \sum_{m=1}^{q} e\,(0) \sum_{\chi \bmod q} \chi(m)\overline{\chi}(m) + \\ &+ \sum_{1\le m<n\le q} e\left((m-n)\frac{a}{q}\right) \sum_{\chi \bmod q} \chi(m)\overline{\chi}(n) = \\ &= \sum_{m=1}^{q} \sum_{\chi \bmod q} \chi_0(m) + 0 = \sum_{m=1}^{q} \phi(q)\chi_0(m) \le q\phi(q),\end{aligned}$$

en donde hemos usado que, por el lema 3.9, cuando $m \neq n,\ 1 \leq m, n \leq q$

$$\sum_{\chi \text{ mód } q} \chi(m)\overline{\chi}(n) = 0.$$

Combinando lo anterior, la desigualdad de Cauchy-Schwarz nos permite acotar la contribución cuando $\chi \neq \chi_0$

$$\begin{aligned}
&\frac{1}{\phi(q)} \sum_{\substack{\chi \text{ mód } q \\ \chi \neq \chi_0}} \tau(\overline{\chi}, a)\psi_h(N, \chi) \\
&\leq \frac{1}{\phi(q)} \left( \sum_{\chi \text{ mód } q} |\tau(\overline{\chi}, a)|^2 \right)^{1/2} \times \left( \sum_{\chi \text{ mód } q} |\psi_h(N, \chi)|^2 \right)^{1/2} \\
&\leq \frac{1}{\phi(q)} \sqrt{q}\sqrt{\phi(q)} \times \sqrt{\phi(q)}(1 + |h|N) O\left( \frac{N}{(\log N)^{6B}} \right) = O\left( \frac{(1 + |h|N)\sqrt{q}N}{(\log N)^{6B}} \right).
\end{aligned}$$

- En el caso particular del carácter $\chi_0$, de nuevo por (3.15) y sumando por partes,

$$\begin{aligned}
\psi_h(N, \chi_0) - \sum_{n \leq N} e\,(nh) &= \sum_{n \leq N} (\Lambda(n) - 1) e\,(nh) = \\
&= (\psi(N) - N) e\,(Nh) - h2\pi i \int_1^N (\psi(u) - u) e\,(hu)\ \mathrm{d}u \\
&\ll \frac{N}{(\log N)^{6B}} + |h|N \frac{N}{(\log N)^{6B}} \ll (1 + |h|N) \frac{N}{(\log N)^{6B}}.
\end{aligned}$$

Ahora nos encontramos con la suma de Ramanujan y como $(a, q) = 1$,

$$\tau(\overline{\chi_0}, a) = \sum_{m=1}^{q} \chi_0(k) e\left( m\frac{a}{q} \right) = \sum_{\substack{m=1 \\ (m,q)=1}}^{q} e\left( m\frac{a}{q} \right) = c_q(a) = \mu(q);$$

por lo tanto, dado que $\sum_{n \leq N} e\,(nh) \ll N$,

$$\tau(\overline{\chi_0}, a)\ \psi_h(N, \chi_0) = \mu(q) \sum_{n \leq N} e\,(nh) + O\left( \frac{(1 + |h|N)N}{(\log N)^{6B}} \right).$$

Juntando todo lo anterior en la ecuación (4.10) obtenemos

$$F_N(x) = \frac{\mu(q)}{\phi(q)} \sum_{n \leq N} e\,(n(x - a/q)) + O\left( \frac{(1 + |h|N)\sqrt{q}N}{(\log N)^{6B}} \right),$$

ya que $h = x - a/q$. Como $x \in \mathcal{M}_{a/q}$, $h$ es menor en valor absoluto que $Q/N = (\log N)^B/N$ y esto implica que

$$(1+|h|N)\sqrt{q} \le (1+Q)Q^{1/2} = (1+(\log N)^B)(\log N)^{B/2} \ll (\log N)^{3B/2},$$

lo que completa la demostración.

□

Para estudiar la representación como suma de $k$ primos necesitamos aproximar la potencia $k$-ésima de la función generatriz y esto es ahora una consecuencia directa de lo anterior:

**Corolario 4.1.**

$$[F_N(x)]^k = \left[\frac{\mu(q)}{\phi(q)}\, D_N(x-a/q)\right]^k + O\left(\frac{N^k}{(\log N)^{4B}}\right) \quad \forall\, k \ge 1, \quad \forall\, x \in \mathcal{M}_{a/q}. \tag{4.11}$$

*Demostración.* La proposición 4.1 nos da $F_N(x) = P_N(x) + Err_N(x)$ con las siguientes cotas para el término principal y el término de error:

$$P_N(x) = \frac{\mu(q)}{\phi(q)}\, D_N(x-a/q) \ll |D_N(x-a/q)| \ll N \qquad Err_N(x) \ll \frac{N}{(\log N)^{4B}},$$

y entonces

$$\begin{aligned} F_N(x)^k - P_N(x)^k &= \sum_{i=1}^{k} \binom{k}{i} P_N(x)^{k-i} \cdot Err_N(x)^i \\ &\ll \sum_{i=1}^{k} \binom{k}{i} N^{k-i} \frac{N^i}{((\log N)^{4B})^i} \ll_k \frac{N^k}{(\log N)^{4B}}. \end{aligned}$$

□

## 4.3. Contribución de los arcos mayores a la suma de primos

En esta sección comprobaremos que la contribución de la integral en los arcos mayores se aproxima asintóticamente por un producto de dos factores

$$\int_{\mathcal{M}} [F_N(x)]^k e\,(-Nx)\, \mathrm{d}x \sim \mathfrak{S}_k(N)\, J_k(N).$$

Esta expansión corresponde a la singularidad de la función $F_{\mathcal{P}}(z) = \sum_{p\in\mathcal{P}} (\log p) z^p$ en $z = e\,(a/q)$, en vista de lo cual Hardy y Littlewood acuñaron los términos serie singular e integral singular para $\mathfrak{S}_k(N)$ y $J_k(N)$ respectivamente.

Estudiamos en primer lugar el ingrediente $J_k(N)$ que proviene de integrar la función $D_N(x)$.

### La integral singular

La distancia al entero más cercano se define como

$$\|x\| := \text{mín}(\{x\}, 1 - \{x\}),$$

donde $\{x\} = x - \lfloor x \rfloor$ representa la parte fraccionaria de $x$. Se trata de una función de período 1, que en el intervalo $[0, 1]$ es simétrica respecto al punto $1/2$: $\|x\| = \|1 - x\|$. La función $|\operatorname{sen} \pi x|$ tiene estas mismas propiedades. Además en el intervalo $[0, 1/2]$:

$$|\operatorname{sen} \pi x| = \operatorname{sen}(\pi \|x\|) = \operatorname{sen} \pi x \qquad x \in [0, 1/2].$$

Hemos desvelado así que

$$|\operatorname{sen} \pi x| = \operatorname{sen}(\pi \|x\|) \qquad \text{para todo número real } x, \tag{4.12}$$

lo que nos permite probar el siguiente resultado

**Lema 4.2.** *Para todo número real $x$*

$$\left| \sum_{n \le N} e(nx) \right| \le \text{mín}\left(N, \frac{1}{2\|x\|}\right) = O\left(\frac{1}{\|x\|}\right),$$

*en donde $\|x\|$ denota la distancia de $x$ al entero más cercano.*

*Demostración.* Es inmediato $\left|\sum_{n \le N} e(nx)\right| \le N$ pues cada sumando tiene módulo 1. Ahora

$$\begin{aligned} \left| \sum_{n \le N} e(nx) \right| = \left| \sum_{n \le N} [e(x)]^n \right| = \left| \frac{e((N+1)x) - e(x)}{e(x) - 1} \right| \le \\ \le \frac{2}{|e(x) - 1|} = \frac{2}{|e(x/2) - e(-x/2)|} = \\ = \frac{2}{|i\, 2 \operatorname{sen} \pi x|} = \frac{1}{\operatorname{sen}(\pi \|x\|)} \le \frac{1}{2\|x\|}. \end{aligned}$$

en donde hemos usado (4.12) y también que la función $g(x) = 2x - \operatorname{sen} \pi x$ satisface $g([0, 1/2]) \le 0$ pues al tener derivada segunda positiva es convexa en $[0, 1/2]$ y además $g(0) = g(1/2) = 0$. □

Usando el lema 4.2 podemos acotar convenientemente la diferencia entre cierta integral sobre el intervalo $[-1/2, 1/2]$ y el valor de esa misma integral sobre otro intervalo más pequeño:

**Lema 4.3.** *Para cualquier número $0 < t \le N/2 \quad k \ge 2$ se tiene*

$$\int_{-t/N}^{t/N} [D_N(u)]^k e(-Nu)\, \mathrm{d}u = \int_{-1/2}^{1/2} [D_N(u)]^k e(-Nu)\, \mathrm{d}u + O\left(\left(\frac{N}{t}\right)^{k-1}\right).$$

*Demostración.* Como $|u| = \|u\| \leq 1/2$, por el lema 4.2 tenemos

$$|D_N(u)| \ll \frac{1}{\|u\|} = |u|^{-1},$$

por lo tanto

$$\int_{t/N}^{1/2} [D_N(u)]^k \, e(-Nu) \, \mathrm{d}u \ll \int_{t/N}^{1/2} |D_N(u)|^k \, \mathrm{d}u \ll \int_{t/N}^{1/2} |u|^{-k} \, \mathrm{d}u =$$
$$= \frac{1}{k-1} \left( \left( \frac{N}{t} \right)^{k-1} - \, 2^{k-1} \right) \ll_k \left( \frac{N}{t} \right)^{k-1},$$

y análogamente

$$\int_{-1/2}^{-t/N} [D_N(u)]^k \, e(-Nu) \, \mathrm{d}u \ll_k \left( \frac{N}{t} \right)^{k-1}.$$

□

Por último aproximamos asintóticamente la integral sobre $[-1/2, 1/2]$.

**Lema 4.4.** *Si* $D_N(x) = \sum_{n \leq N} e(nx)$ *entonces*

$$J_k(N) := \int_{-1/2}^{1/2} [D_N(u)]^k e(-Nu) \, \mathrm{d}u = \binom{N-1}{k-1} = \frac{N^{k-1}}{(k-1)!} + O\left(N^{k-2}\right) \qquad k \geq 2,$$

*donde la constante implícita depende de* $k$.

*Demostración.* Por el lema 2.1 en la página 12, esta integral es igual que

$$J_k(N) = r(N; k, \mathbb{N}) := \#\{(n_1, \ldots, n_k) \in \mathbb{N}^k \mid N = n_1 + \ldots + n_k\}.$$

Veamos a continuación que se cumple

$$r(N; k, \mathbb{N}) = \binom{N-1}{k-1}.$$

Dada una representación cualquiera de $N$ como suma de $k$ números naturales, descomponemos cada uno de los sumandos en suma de unos:

$$\overset{n_1 \text{ veces}}{1 + \cdots + 1} + \quad \overset{n_2 \text{ veces}}{1 + \cdots + 1} + \quad \ldots + \quad \overset{n_k \text{ veces}}{1 + \cdots + 1} = N.$$

A continuación miramos la expresión así obtenida como una ristra de $N$ unos a la que añadimos $k-1$ separadores que vamos dibujando con el símbolo $\|$ en los intersticios donde hay transición desde un $n_i$ hasta el siguiente $n_{i+1}$:

$$1 + \cdots + 1 + \| \, 1 + \, \cdots \, + 1 + \| \, \ldots + \| \, 1 + \cdots + 1 = N.$$

Observamos que el número total de representaciones distintas es igual que el número total de elecciones distintas de intersticios que pueden ocupar los separadores. Enumeramos todos los intersticios disponibles desde 1 hasta $N-1$, con este convenio cada elección de $k-1$ intersticios se representa por un subconjunto de $k-1$ elementos del conjunto $\{1, 2, \dots N-1\}$, como queríamos.

Finalmente como

$$\overbrace{((N-1)(N-2)\times\cdots\times(N-1-(k-1)+1))}^{k-1 \text{ factores}} - N^{k-1} = O\left(N^{k-2}\right),$$

entonces

$$\binom{N-1}{k-1} - \frac{N^{k-1}}{(k-1)!} \ll_k N^{k-2}.$$

□

## La serie singular

El otro ingrediente del término principal en la contribución de los arcos mayores será cierta serie $\mathfrak{S}_k(N)$ que se adjetiva como *singular* para resaltar que precisamente en estos arcos se encuentran las singularidades de la función compleja original del método del círculo. La serie $\mathfrak{S}_k(N)$ sintetiza la información que se extrae de estas singularidades. Definimos

$$\mathfrak{S}_k(N,x) := \sum_{q\le x} \frac{\mu^k(q)\, c_q(-N)}{\phi^k(q)} \qquad \text{y} \qquad \mathfrak{S}_k(N) := \mathfrak{S}_k(N,\infty).$$

En el análisis que hacemos acotamos primero las colas de la serie y a continuación mostramos que la serie se puede expresar como un cierto producto de primos.

**Lema 4.5.** *La serie singular converge absolutamente y para todo $k \ge 2$*

$$\mathfrak{S}_k(N) = \mathfrak{S}_k(N,x) + O\left(x^{-(1-\epsilon)}\right) \qquad \forall\, \epsilon > 0, \quad x > 1. \tag{4.13}$$

*Demostración.* Resolvemos primero el caso $k \ge 3$. Tenemos $|c_q(-N)| \le \phi(q)$. Tomamos $\delta < \epsilon$ positivo y recordando ahora (3.6) tenemos que, para $q$ suficientemente grande

$$\frac{\mu^k(q)\, c_q(-N)}{\phi^k(q)} \ll \frac{1}{\phi(q)^{k-1}} \ll \frac{1}{q^{(k-1)(1-\delta)}} < \frac{1}{q^{2-\delta}},$$

de modo que la serie singular converge absolutamente y —para $k \ge 3$ — uniformemente en $N$. Finalmente

$$\begin{aligned}
\mathfrak{S}_k(N) - \mathfrak{S}_k(N,x) &\ll \sum_{q>x} \frac{1}{q^{2-\delta}} = \sum_{q>x} \left(\frac{1}{q}\right)^{1-\epsilon} \left(\frac{1}{q}\right)^{1+\epsilon-\delta} \\
&< \frac{1}{x^{1-\epsilon}} \sum_{q=1}^{\infty} \left(\frac{1}{q}\right)^{1+\epsilon-\delta} \\
&\ll \frac{1}{x^{1-\epsilon}}.
\end{aligned}$$

En el caso $k = 2$ usando la fórmula (3.8) y la propiedad (3.6), tenemos que para todo $\delta > 0$

$$\begin{aligned}\mathfrak{S}_2(N) - \mathfrak{S}_2(N,x) &= \sum_{q>x} \mu\left(q/(q,N)\right) \frac{1}{\phi(q)\,\phi(q/(q,N))} \\ &\ll \sum_{q>x} \frac{1}{q^{1-\delta}\left(\frac{q}{(q,N)}\right)^{1-\delta}} = \sum_{q>x} \frac{(q,N)^{1-\delta}}{q^{2-2\delta}} \\ &\leq N^{1-\delta} \sum_{q>x} \frac{1}{q^{2-2\delta}} = N^{1-\delta} \sum_{q>x} \frac{1}{q^{1-3\delta}} \frac{1}{q^{1+\delta}} \\ &\ll_N \frac{1}{x^{1-3\delta}},\end{aligned}$$

y tomando $\delta = \epsilon/3$ se completa la demostración. □

**Proposición 4.2.** *Para cualesquiera $k \geq 2$ y $N$ entero positivo sea la serie singular*

$$\mathfrak{S}_k(N) := \sum_q \frac{\mu^k(q) c_q(-N)}{\phi^k(q)},$$

*donde la suma se extiende a todos los enteros positivos. Se tiene*

$$\boxed{\mathfrak{S}_k(N) = \prod_{p|N} \left(1 + \frac{(-1)^k}{(p-1)^{k-1}}\right) \quad \prod_{p\nmid N} \left(1 + \frac{(-1)^{k+1}}{(p-1)^k}\right),} \tag{4.14}$$

*donde el producto se extiende a todos los números primos.*

*Demostración.* $f(q) = \frac{\mu^k(q) c_q(-N)}{\phi^k(q)}$ es función aritmética multiplicativa porque sus tres ingredientes son multiplicativas. Como $f(1) = 1$ tenemos el producto de Euler

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

Cuando $k > 1$ se tiene $f(p^k) = 0$ porque $\mu(p^k) = 0$. Esto reduce el producto a

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

Además en los primos $\mu^k(p) = (-1)^k$ y $\phi(p) = p - 1$. Como $c_p(N)$ es un número entero $c_p(-N) = \overline{c_p(N)} = c_p(N)$. Lo que resta es evaluar $c_q(N)$ (v. proposición 3.3 ) :

- Cuando $p \nmid N$ tenemos que $c_p(N) = \mu(p) = -1$ y $f(p) = (-1)^{k+1}/(p-1)^k$.

- Cuando $p \mid N$ tenemos que $p = (N, p)$ y

$$c_p(N) = \mu(p/(N,p))\frac{\phi(p)}{\phi(p/(N,p))} = \mu(1)\frac{\phi(p)}{\phi(1)} = p - 1,$$

por lo tanto para estos primos $f(p) = (-1)^k/(p-1)^{k-1}$.

□

Visto $\mathfrak{S}_k(N)$ como un producto infinito, todos los factores en la fórmula (4.14) son no negativos porque $p \geq 2$. Recordamos que en general cuando $\sum |a_n| < \infty$ entonces el producto infinito $\prod(1 + a_n)$ converge; además se anula si y sólo si uno de sus factores es cero. Este es el caso de $\mathfrak{S}_k(N)$, por consiguiente será nulo cuando alguno de sus factores se anule:

o bien

$$p \mid N \text{ y } \quad 0 < (p-1)^{k-1} = (-1)^{k-1} \iff \qquad k \text{ es impar y } p = 2 \text{ es decir } N \text{ es par,}$$

o bien

$$p \nmid N \text{ y } \quad 0 < (p-1)^{k} = (-1)^{k} \iff \qquad k \text{ es par y } p = 2 \text{ es decir } N \text{ es impar.}$$

Así llegamos a la siguiente conclusión

**Corolario 4.2.** *Si $N$ y $k$ tienen la misma paridad existen dos constantes $0 < c < C$ tales que*

$$0 < c < \mathfrak{S}_k(N) < C \qquad \forall\, N \in \mathbb{N},\ k \geq 2 \quad \textit{con } k \equiv N \text{ mód } 2.$$

*Cuando $N$ y $k$ tienen distinta paridad entonces $\mathfrak{S}_k(N) = 0$.*

Detengámonos a reflexionar qué significa esto para el caso particular de la conjetura ternaria de Goldbach. Nos preguntamos ahora por el valor de $\mathfrak{S}_3(2n)$. Supongamos por un momento que para todo número $2n$ par suficientemente grande se cumpliera $\mathfrak{S}_3(2n) > 0$. El número $r(2n; 3, \mathcal{P})$ de representaciones con tres sumandos primos de cualquier par suficientemente grande sería positivo —razonando de modo análogo a lo que ciertamente ocurre con $r(N; 3, \mathcal{P})$ cuando $N$ es impar, como comprobaremos más adelante. Si este fuera el caso, tomemos $2n$ un número par cualquiera suficientemente grande, tendríamos que $2n+2 = p_1+p_2+p_3$ para algún trío de primos y necesariamente uno de los sumandos ha de ser el (único primo par) 2, pongamos que $p_1 = 2$. En consecuencia $2n = p_2 + p_3$ y ... ¡habríamos tocado con la punta de los dedos la conjetura binaria de Goldbach!

Y en este punto el corolario 4.2 nos despierta del breve espejismo, confirmando que $\mathfrak{S}_3(2n) = 0$. Hemos topado con una gatera hacia la conjetura de Goldbach que resulta estar cerrada, lo que viene a confirmarnos la dificultad del problema binario ($k = 2$).

### Estimación para la contribución de los arcos mayores

Tras todas las averiguaciones precedentes podemos ya exhibir el término protagonista en la aportación de los arcos mayores a las representaciones de un número como sumas de primos.

**Proposición 4.3.** *Sea $Q = (\log N)^B$. Entonces sobre el conjunto de los arcos mayores*

$$\mathcal{M} = \bigcup_{1\le q\le Q} \bigcup_{\substack{a=1\\(a,q)=1}}^{q} \mathcal{M}_{a/q},$$

*donde*

$$\mathcal{M}_{a/q} = \left\{ x\in[0,1]\colon \left| x - \frac{a}{q}\right| < \frac{Q}{N}\right\} \quad (a,q)=1, \qquad \mathcal{M}_{1/1} = \left(1-\frac{Q}{N},1\right]\cup\left[0,\frac{Q}{N}\right);$$

*se cumple que*

$$\boxed{\int_{\mathcal{M}} [F_N(x)]^k e\left(-Nx\right)\,\mathrm{d}x = \mathfrak{S}_k(N)\,\frac{N^{k-1}}{(k-1)!} + O\left(\frac{N^{k-1}}{(\log N)^{B-1}}\right) \qquad \forall\, k\ge 2} \tag{4.15}$$

*donde $F_N(x) := \sum_{p\le N} \log p\, e\left(px\right)$.*

*Demostración.* Por el corolario 4.1 tenemos que cuando $x$ está sobre el arco mayor $\mathcal{M}_{a/q}$

$$[F_N(x)]^k = \left[\frac{\mu(q)}{\phi(q)} D_N(x-a/q)\right]^k + O\left(\frac{N^k}{Q^4}\right),$$

así que

$$\begin{aligned}
&\int_{\mathcal{M}_{a/q}} [F_N(x)]^k e\left(-Nx\right)\,\mathrm{d}x = \\
&\qquad = \left[\frac{\mu(q)}{\phi(q)}\right]^k \int_{\mathcal{M}_{a/q}} [D_N(x-a/q)]^k\, e\left(-Nx\right)\,\mathrm{d}x + O\left(\int_{\mathcal{M}_{a/q}} \frac{N^k}{Q^4}\right) \\
&\qquad = \left[\frac{\mu(q)}{\phi(q)}\right]^k e\left(-N\,\frac{a}{q}\right) \int_{-Q/N}^{Q/N} [D_N(u)]^k\, e\left(-Nu\right)\,\mathrm{d}u + O\left(\frac{N^{k-1}}{Q^3}\right),
\end{aligned}$$

que, por el lema 4.3, es igual a

$$\begin{aligned}
&= \left[\frac{\mu(q)}{\phi(q)}\right]^k e\left(-N\,\frac{a}{q}\right)\left(J_k(N) + O\left(\frac{N^{k-1}}{Q^{k-1}}\right)\right) + O\left(\frac{N^{k-1}}{Q^3}\right) \\
&= J_k(N)\,\left[\frac{\mu(q)}{\phi(q)}\right]^k e\left(-N\,\frac{a}{q}\right) + O\left(\frac{N^{k-1}}{Q^3}\right).
\end{aligned}$$

Los arcos mayores son disjuntos dos a dos para $N$ suficientemente grande (ref. página 39) así que

$$\begin{aligned}
&\int_{\mathcal{M}} [F_N(x)]^k e\left(-Nx\right)\,\mathrm{d}x = \\
&= \sum_{q\leq Q}\sum_{\substack{(a,q)=1\\ a\leq q}} \int_{\mathcal{M}_{a/q}} [F_N(x)]^k e\left(-Nx\right)\,\mathrm{d}x = \\
&= J_k(N)\sum_{q\leq Q}\left[\frac{\mu(q)}{\phi(q)}\right]^k \sum_{\substack{(a,q)=1\\ a\leq q}} e\left(-N\,\frac{a}{q}\right) + O\left(\sum_{q\leq Q}\sum_{\substack{(a,q)=1\\ a\leq q}} \frac{N^{k-1}}{Q^3}\right) \\
&= J_k(N)\sum_{q\leq Q}\left[\frac{\mu(q)}{\phi(q)}\right]^k C_q(-N) + O\left(\frac{N^{k-1}}{Q}\right) \\
&= J_k(N)\,\mathfrak{S}_k(N,Q) + O\left(\frac{N^{k-1}}{Q}\right) \\
&= J_k(N)\,\left(\mathfrak{S}_k(N) + O\left(\frac{1}{Q^{1-\epsilon}}\right)\right) + O\left(\frac{N^{k-1}}{Q}\right) \qquad \forall\,\epsilon>0 \\
&= J_k(N)\,\mathfrak{S}_k(N) + \left(\frac{N^{k-1}}{(k-1)!} + O\left(N^{k-2}\right)\right) O\left(\frac{1}{Q^{1-\epsilon}}\right) + O\left(\frac{N^{k-1}}{Q}\right) \\
&= \mathfrak{S}_k(N)\,J_k(N) + O\left(\frac{N^{k-1}}{Q^{1-\epsilon}}\right),
\end{aligned}$$

en donde hemos usado (4.13) y el lema 4.4. Llegados a este punto de nuevo el lema 4.4 nos permite concluir la demostración del modo siguiente

$$\begin{aligned}
\int_{\mathcal{M}} [F_N(x)]^k e\left(-Nx\right)\,\mathrm{d}x &= \mathfrak{S}_k(N)\,J_k(N) + O\left(\frac{N^{k-1}}{Q^{1-\epsilon}}\right) \\
&= \mathfrak{S}_k(N)\,\frac{N^{k-1}}{(k-1)!} + O\left(N^{k-2}\right) + O\left(\frac{N^{k-1}}{(\log N)^{B(1-\epsilon)}}\right) \\
&= \mathfrak{S}_k(N)\,\frac{N^{k-1}}{(k-1)!} + O\left(\frac{N^{k-1}}{(\log N)^{B-1}}\right),
\end{aligned}$$

escogiendo convenientemente $\epsilon$. □

## Apéndice: La serie singular y la relación local-global

El *principio global-local* indica que es posible resolver algunas cuestiones en teoría de números respondiéndolas "localmente". [The-P-C-to-Maths, §III.51]

En [Ch-1, §2] se muestra cómo la serie singular $\mathfrak{S}_k(N)$ incluye la información local sobre congruencias. Me gustaría simplemente mencionar esta curiosa interpretación, que es diferente de las presentaciones habituales de la serie singular.

Para $q$ entero positivo denotemos por $\mathcal{U}(\mathbb{Z}/q\mathbb{Z})$ a las unidades del anillo $\mathbb{Z}/q\mathbb{Z}$. A continuación nos fijamos en las soluciones *locales* a la representación de un número entero positivo $N$ como suma de $k$ unidades de este anillo. Definimos la cantidad de representaciones locales por la fórmula:

$$r(N;k,\mathcal{P},q) := \#\{(n_1,\ldots,n_k) \in \mathcal{U}(\mathbb{Z}/q\mathbb{Z})^k \mid \ n_1+\ldots+n_k \equiv N \pmod{q}\},$$

y definimos su densidad como

$$\delta_q := \frac{r(N;k,\mathcal{P},q)}{[\#\mathcal{U}(\mathbb{Z}/q\mathbb{Z})]^k}.$$

Entonces se tiene la siguiente relación local-global:

$$\mathfrak{S}_k(N) = \prod_{p \text{ primo}} p \cdot \delta_q.$$

# Capítulo 5

# Arcos triunfales con tres o más primos

En este capítulo cosechamos los frutos de los esfuerzos precedentes en el caso de las sumas de primos con 3 o más sumandos. Poco antes de alcanzar la cumbre del *pico Vinogradov* (corolario 5.2) hemos de dejar a un lado la conjetura binaria de Goldbach, contentándonos por ahora con terminar la incursión comprobando que el conjunto de las excepciones a la conjetura tiene densidad asintóticamente nula (corolario 5.3).

El ingrediente que falta añadir al guiso antes de presentarlo en la vajilla de plata del método del círculo es una buena cota de la contribución de los arcos menores a las sumas con primos, que confirme que en la expresión

$$R(N;k,\mathcal{P}) = \int_{\mathcal{M}} [F_N(x)]^k e\left(-Nx\right)\,\mathrm{d}x + \int_{\mathfrak{m}} [F_N(x)]^k e\left(-Nx\right)\,\mathrm{d}x,$$

la parte principal de la estimación para la primera integral domina a la contribución de la segunda integral.

## 5.1. Otros ingredientes *menores*

Recopilamos en esta primera sección varios resultados necesarios para abordar, en las siguientes secciones, los argumentos principales de este capítulo.

En nuestro estudio de los arcos del método del círculo ha estado presente la aproximación de cualquier número real por números racionales.

**Teorema 5.1** (Dirichlet)**.** *Sean $\theta$ y $K \geq 1$ números reales cualesquiera. Entonces existe un racional $h/k$, $(h,k) = 1$ tal que $1 \leq k \leq K$ y cuya proximidad a $\theta$ es del orden siguiente:*

$$\left|\theta - \frac{h}{k}\right| \leq \frac{1}{kK}.$$

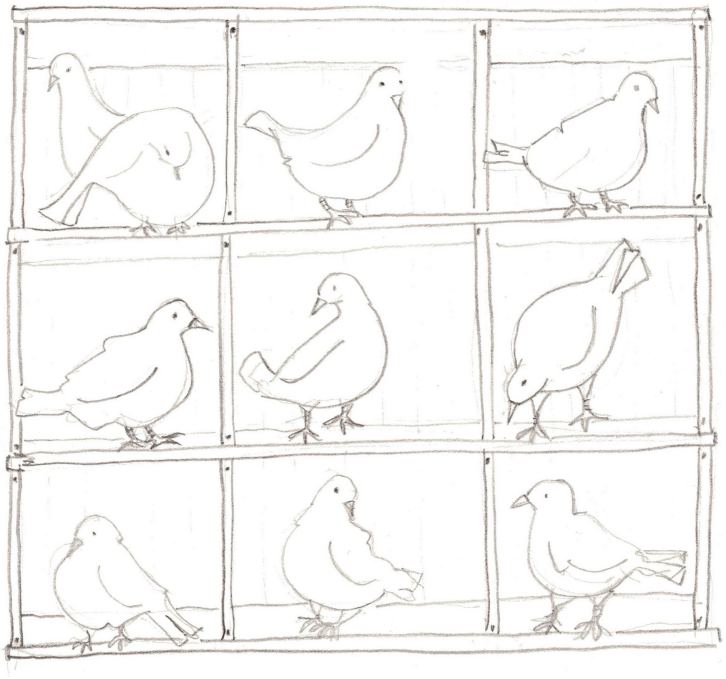

Figura 5.1: El principio del palomar

*Demostración.* Tomamos $N = \lfloor K \rfloor$.

Si existe $n \leq N$ tal que $\{n\theta\} \in \left[0, \dfrac{1}{N+1}\right)$ entonces

$$|n\theta - \lfloor n\theta \rfloor| < \frac{1}{N+1} \quad \Rightarrow \quad \left|\theta - \frac{\lfloor n\theta \rfloor}{n}\right| < \frac{1}{nK},$$

y usando el máximo común divisor $D = (\lfloor n\theta \rfloor, n)$ conseguimos el racional buscado:

$$\left|\theta - \frac{\lfloor n\theta \rfloor / D}{n/D}\right| < \frac{1}{(n/D)K} \qquad 1 \leq n/D \leq n \leq K.$$

En el caso de que exista $n \leq N$ tal que $\{n\theta\} \in \left[\dfrac{N}{N+1}, 1\right)$ tenemos

$$-\frac{1}{N+1} \leq n\theta - (\lfloor n\theta \rfloor + 1) < 0 \quad \Rightarrow \quad \left|\theta - \frac{\lfloor n\theta \rfloor + 1}{n}\right| < \frac{1}{nK},$$

y ahora podemos tomar el racional $(\lfloor n\theta \rfloor + 1)/n$ (o su fracción irreducible equivalente).

En otro caso, los $N$ números $\{n\theta\}$ $n = 1, 2, \ldots, N$ verifican $\{n\theta\} \in \left[\dfrac{1}{N+1}, \dfrac{N}{N+1}\right)$ y son todos distintos; porque, suponiendo que dos de ellos coincidiesen, tendríamos que existirían $1 \leq n_1 < n_2 \leq N$ con

$$(n_2 - n_1)\theta - \lfloor n_2\theta \rfloor - \lfloor n_1\theta \rfloor = \{n_2\theta\} - \{n_1\theta\} = 0,$$

por consiguiente $(n_2 - n_1)\theta$ sería un número entero, lo que a su vez implicaría $\{(n_2 - n_1)\theta\} = 0 \quad 1 \leq n_2 - n_1 \leq N$, que es falso en este tercer caso.

Por el *Principio del palomar* (v. figura 5.1), como tenemos $N$ números –las palomas– ocupando $N - 1$ intervalos de anchura $1/(N + 1)$ –los palomares–, entonces al menos existen $1 \leq n_1 < n_2 \leq N$ –dos palomas en el mismo palomar– tales que

$$|(n_2 - n_1)\theta - \lfloor n_2\theta \rfloor - \lfloor n_1\theta \rfloor| < \frac{1}{N+1},$$

de donde se deduce que

$$\left|\theta - \frac{\lfloor n_2\theta \rfloor - \lfloor n_1\theta \rfloor}{(n_2 - n_1)}\right| < \frac{1}{(n_2 - n_1)K},$$

y se completa este tercer caso análogamente a los dos anteriores. □

## Cotas para ciertas sumas trigonométricas

A continuación nuestro propósito es encontrar cotas no triviales para dobles sumas del tipo

$$\sum\sum e\left(xij\right),$$

con $i, j$ enteros que satisfacen ciertas restricciones. Concretaremos este objetivo en el lema 5.5 y para lograrlo exponemos previamente cuatro lemas consecutivos.

Recordamos que $\|x\|$ representa la distancia de $x$ al entero más cercano (v. página 45). Si tenemos un racional de la forma $1/q$ entonces

$$\sum_{1\leq i\leq q/2} \frac{1}{\|i \cdot 1/q\|} = \sum_{1\leq i\leq q/2} q\frac{1}{i} = q\left(\log q/2 + O(1)\right) = O\left(q \log q\right).$$

En el siguiente lema veremos que esta estimación también es válida para cualquier $x \in \mathbb{R}$ siempre que tenga una cierta cercanía a la fracción irreducible $a/q$.

**Lema 5.1.** *Sea $x \in \mathbb{R}$ aproximado del modo siguiente por la fracción irreducible $a/q$*

$$\left|x - \frac{a}{q}\right| \leq \frac{1}{q^2} \qquad (a, q) = 1 \quad q \geq 1.$$

*Entonces*

$$\sum_{1\leq i\leq q/2} \frac{1}{\|xi\|} \ll q \log q. \tag{5.1}$$

*Demostración.* La función $\|\ \|$ satisface la desigualdad triangular

$$\|x + y\| \leq \|x\| + \|y\|. \tag{5.2}$$

La estimación (5.1) se cumple trivialmente para $q = 1$. Supongamos en lo que sigue $q \geq 2$. Para cada entero $i$ existen enteros $s(i) \in [0, q/2]$ y $m(i)$ tales que

$$\frac{s(i)}{q} = \left\| \frac{ai}{q} \right\| = \pm \left( \frac{ai}{q} - m(i) \right).$$

Como $(a, q) = 1$ entonces $s(i) = 0$ si y sólo si $i$ es múltiplo de $q$ y entonces como $q/2 \geq i \geq 1$ también $s(i) \geq 1$. Por la cercanía de $x$ a $a/q$ podemos escribir

$$x - \frac{a}{q} = \frac{\theta}{q^2} \qquad |\theta| \leq 1,$$

y entonces

$$xi = \frac{ai}{q} + \frac{\theta'}{2q} \qquad \left|\theta'\right| = \left| \frac{2\theta i}{q} \right| \leq 1.$$

En consecuencia, teniendo en cuenta (5.2),

$$\begin{aligned} \|xi\| &= \left\| \frac{ai}{q} + \frac{\theta'}{2q} \right\| = \left\| m(i) \pm \frac{s(i)}{q} + \frac{\theta'}{2q} \right\| = \left\| \frac{s(i)}{q} \pm \frac{\theta'}{2q} \right\| \\ &\geq \left\| \frac{s(i)}{q} \right\| - \left\| \frac{\theta'}{2q} \right\| \geq \frac{s(i)}{q} - \frac{1}{2q}. \end{aligned}$$

A continuación comprobamos que para $1 \leq i_1 \leq i_2 \leq q/2$ se verifica que $i_1 = i_2$ cuando se tiene $s(i_1) = s(i_2)$. Efectivamente, cuando

$$\pm \left( \frac{ai_1}{q} - m(i_1) \right) = \left\| \frac{ai_1}{q} \right\| = \left\| \frac{ai_2}{q} \right\| = \pm \left( \frac{ai_2}{q} - m(i_2) \right),$$

entonces $ai_1 \equiv \pm ai_2 \pmod{q}$. Como $(a, q) = 1$ esto implica $i_1 \equiv \pm i_2 \pmod{q}$ y finalmente $i_1 = i_2$. Así que el entero $s = s(i)$ recorre los valores $[1, q/2]$ cuando el entero $i$ recorre los valores $[1, q/2]$. Concluimos que

$$\begin{aligned} \sum_{1 \leq i \leq q/2} \frac{1}{\|xi\|} &\leq \sum_{1 \leq i \leq q/2} \frac{1}{\frac{s(i)}{q} - \frac{1}{2q}} = \sum_{1 \leq s \leq q/2} \frac{1}{\frac{s}{q} - \frac{1}{2q}} \\ &= 2q \sum_{1 \leq s \leq q/2} \frac{1}{2s - 1} \leq 2q \sum_{1 \leq s \leq q/2} \frac{1}{s} \\ &\ll q \log q. \end{aligned}$$

□

**Lema 5.2.** *Sea $x \in \mathbb{R}$ aproximado del modo siguiente por la fracción irreducible $a/q$*

$$\left| x - \frac{a}{q} \right| \leq \frac{1}{q^2} \qquad (a, q) = 1 \quad q \geq 1.$$

*Entonces para cualquier entero no negativo $h$ y cualquier número real $y$ no negativo tenemos*

$$\sum_{i=1}^{q} \min \left( y, \frac{1}{\|x(hq + i)\|} \right) \ll y + q \log q \qquad 0 \leq y \in \mathbb{R} \quad 0 \leq h \in \mathbb{Z}. \tag{5.3}$$

*Demostración.* Si $x = a/q + \theta/q^2$ entonces

$$x(hq+i) = ah + \frac{ai}{q} + \frac{\lfloor \theta h \rfloor}{q} + \frac{\delta(i)}{q},$$

con

$$-1 \le \delta(i) = \{\theta h\} + \frac{\theta i}{q} < 2.$$

Si llamamos $i'$ a la parte entera de $x(hq+i) - ah$ tendremos que

$$\{x(hq+i)\} = \frac{ai + \lfloor \theta h \rfloor + \delta(i)}{q} - i',$$

puesto que $ah$ es entero. Sea ahora cualquier $t \in [0, 1 - 1/q]$. En el caso de que $\{x(hq+i)\} \in [t, t+1/q]$ esto implica

$$qt \le ai - qi' + \lfloor \theta h \rfloor + \delta(i) \le qt + 1,$$

lo que lleva a

$$qt - \lfloor \theta h \rfloor - 2 < qt - \lfloor \theta h \rfloor - \delta(i) \le ai - qi' \le qt - \lfloor \theta h \rfloor + 1 - \delta(i) \le qt - \lfloor \theta h \rfloor + 2.$$

Así el entero $ai - qi'$ está en el intervalo semiabierto de diámetro 4 centrado en el punto $qt - \lfloor \theta h \rfloor$. Dicho intervalo contiene exactamente cuatro enteros distintos. También como $(a, q) = 1$,

$$\text{cuando } 1 \le i_1 \le i_2 \le q \quad \text{y} \quad ai_1 - qi_1' = ai_2 - qi_2' \qquad \Rightarrow \qquad i_1 = i_2.$$

En consecuencia concluimos que para todo $t \in [0, (q-1)q]$ hay como mucho cuatro enteros $i \in [1, q]$ tales que $\{x(hq+i)\} \in t + [0, 1/q]$.

Observamos ahora que para que $\|x(hq+i)\| \in t + [0, 1/q]$ ha de ocurrir

$$\text{o bien que } \{x(hq+i)\} \in t + [0, 1/q] \quad \text{ o bien que } 1 - \{x(hq+i)\} \in t + [0, 1/q],$$

y en ese segundo caso tenemos que $\{x(hq+i)\} \in t' + [0, 1/q]$, donde $t' = 1 - 1/q - t$ y también $t' \in [0, (q-1)/q]$.

Se sigue de todo el análisis anterior que para todo $t \in [0, (q-1)q]$ existen como mucho ocho enteros $i \in [1, q]$ tales que

$$\|x(hq+i)\| \in [t, t+1/q].$$

Tomamos los intervalos $I(j) = [j/q, (j+1)/q]$ $j = 1, 2, \ldots$; entonces para cada $j$, se tiene que $\|x(hq+i)\| \in I(j)$ para un máximo de ocho enteros $i \in [1, q]$. Aplicamos este hecho para estimar la suma de (5.3).

- En el caso de que $\|x(hq+i)\| \in I(0)$ usamos la desigualdad

$$\text{mín}\left(y, \frac{1}{\|x(hq+i)\|}\right) \le y.$$

- En el caso de que $\|x(hq+i)\| \in I(j)$ para algún $j \geq 1$ entonces

$$\text{mín}\left(y, \frac{1}{\|x(hq+i)\|}\right) \leq \frac{1}{\|x(hq+i)\|} \leq \frac{q}{j}.$$

Como es seguro que para todo $i$ existe $j < q/2$ tal que $\|x(hq+i)\| \in J(j)$ concluimos la demostración del lema como sigue

$$\sum_{i=1}^{q} \text{mín}\left(y, \frac{1}{\|x(hq+i)\|}\right) \leq 8y + 8 \sum_{1 \leq j \leq q/2} \frac{q}{j} \ll y + q\log q.$$

□

**Lema 5.3.** *Sea $x \in \mathbb{R}$ aproximado del modo siguiente por la fracción irreducible $a/q$*

$$\left|x - \frac{a}{q}\right| \leq \frac{1}{q^2} \qquad (a,q) = 1 \quad q \geq 1.$$

*Entonces para cualesquiera números reales $y, z$ tenemos*

$$\sum_{1 \leq i \leq y} \text{mín}\left(z, \frac{1}{\|xi\|}\right) \ll \left(y + z + \frac{yz}{q} + q\right)\log 2q \qquad y, z \in \mathbb{R}. \tag{5.4}$$

*Demostración.* Escribimos $i = hq + j$ con $1 \leq j \leq q$ y $0 \leq h < y/q$. Entonces

$$S = \sum_{1 \leq i \leq y} \text{mín}\left(z, \frac{1}{\|xi\|}\right) \leq \sum_{0 \leq h \leq y/q} \sum_{1 \leq j \leq q} \text{mín}\left(z, \frac{1}{\|x(hq+j)\|}\right).$$

Estimamos a continuación la suma interior utilizando el lema 5.2

$$\begin{aligned} S &\ll \sum_{0 \leq h \leq y/q} (z + q\log q) \\ &\ll \left(\frac{y}{q} + 1\right)(z + q\log q) \\ &= q\log q + y\log q + z + \frac{yz}{q} \\ &\leq \left(q + y + z + \frac{yz}{q}\right)\text{máx}\{1, \log q\} \\ &\leq \left(y + z + \frac{yz}{q} + q\right)\log 2q. \end{aligned}$$

□

**Lema 5.4.** *Sea $x \in \mathbb{R}$ aproximado del modo siguiente por la fracción irreducible $a/q$*

$$\left|x - \frac{a}{q}\right| \leq \frac{1}{q^2} \qquad (a,q) = 1 \quad q \geq 1.$$

*Entonces para cualquier número real $y \geq 1$ y cualquier número real positivo $\lambda$ tenemos*

$$\sum_{1\leq i\leq y} \min\left(\frac{\lambda}{i}, \frac{1}{\|xi\|}\right) \ll \left(y + \frac{\lambda}{q} + q\right)\log 2qy \qquad 1 \leq y \in \mathbb{R} \quad 0 < \lambda \in \mathbb{R}. \tag{5.5}$$

*Demostración.* La prueba es similar a la del lema 5.3. Escribimos $i = hq+j$ con $1 \leq j \leq q$ y $0 \leq h < y/q$. Entonces

$$S = \sum_{1\leq i\leq y} \min\left(\frac{\lambda}{i}, \frac{1}{\|xi\|}\right) \leq \sum_{\substack{0\leq h\leq y/q \\ 1\leq j\leq q}}\sum \min\left(\frac{\lambda}{hq+j}, \frac{1}{\|x(hq+j)\|}\right).$$

Cuando $h = 0$ y $1 \leq j \leq q/2$ entonces por el lema 5.1 tenemos

$$\sum_{1\leq j\leq q/2} \min\left(\frac{\lambda}{hq+j}, \frac{1}{\|x(0q+j)\|}\right) \leq \sum_{1\leq j\leq q/2} \frac{1}{\|xj\|} \ll q\log q.$$

Para el resto de términos tenemos que $hq + j \geq \frac{1}{2}(h+1)q$, por tanto

$$S \ll q\log q + \sum_{0\leq h\leq y/q}\sum_{1\leq j\leq q} \min\left(\frac{\lambda}{(h+1)q}, \frac{1}{\|x(hq+j)\|}\right).$$

Estimamos a continuación la suma interior utilizando el lema 5.2 y obtenemos

$$\begin{aligned} S &\ll q\log q + \sum_{0\leq h\leq y/q}\left(\frac{\lambda}{(h+1)q} + q\log q\right) \\ &\ll q\log q + \frac{\lambda}{q}\sum_{0\leq h\leq y/q}\frac{1}{(h+1)} + \left(\frac{y}{q}+1\right)q\log q \\ &\ll q\log q + \frac{\lambda}{q}\log\left(\frac{y}{q}+1\right) + y\log q \\ &\ll \left(y + \frac{\lambda}{q} + q\right)\log 2qy, \end{aligned}$$

en donde hemos usado la desigualdad siguiente

$$\frac{y}{q} + 1 \leq y + q \leq 2\max(y, q) \leq 2qy,$$

que se mantiene tomando logaritmos en ambos miembros. □

Usando los lemas anteriores, podemos ahora demostrar rápidamente las dos siguientes acotaciones

**Lema 5.5.** *Sea $x \in \mathbb{R}$ verificando*

$$\left| x - \frac{a}{q} \right| \leq \frac{1}{q^2} \qquad (a,q) = 1 \quad q \geq 1.$$

*Para cualesquiera números $1 \leq y, z \in \mathbb{R}$, $0 < \lambda(i) \in \mathbb{R}$ tenemos*

$$\sum_{|i| \leq y} \left| \sum_{\substack{1 \leq j \leq z \\ j \leq \lambda(i)}} e\left(xij\right) \right| \ll \left( y + z + \frac{yz}{q} + q \right) \log 2q, \tag{5.6}$$

$$\sum_{1 \leq i \leq y} \left| \sum_{ij \leq \lambda} e\left(xij\right) \right| \ll \left( y + \frac{\lambda}{q} + q \right) \log 2qy. \tag{5.7}$$

*Demostración.* Por el lema 4.2 (v. página 45) tenemos

$$\left| \sum_{1 \leq j \leq U} e\left(xj\right) \right| \leq \text{mín} \left( U, \frac{1}{2 \left\| x \right\|} \right).$$

Por consiguiente para cualesquiera números $\lambda(i)$ se tiene

$$\sum_{|i| \leq y} \left| \sum_{\substack{1 \leq j \leq z \\ j \leq \lambda(i)}} e\left(xij\right) \right| \leq \sum_{|i| \leq y} \text{mín} \left( z \, , \lambda(i) \, , \frac{1}{2 \left\| xi \right\|} \right). \tag{5.8}$$

De aquí hasta (5.6) hay un sencillo paso porque, usando el lema 5.3,

$$\sum_{|i| \leq y} \text{mín} \left( z, \frac{1}{2 \left\| xi \right\|} \right) \ll \left( y + z + \frac{yz}{q} + q \right) \log 2q.$$

Tomamos ahora $\lambda(i) = \lambda / i$ y por el lema 5.4

$$\sum_{1 \leq i \leq y} \text{mín} \left( \frac{\lambda}{i}, \frac{1}{2 \left\| xi \right\|} \right) \ll \left( y + \frac{\lambda}{q} + q \right) \log 2qy,$$

y esto —combinado con (5.8)— demuestra (5.7). □

Otro ingrediente básico que usaremos en prueba de la proposición 5.1 son ciertas formas bilineales.

**Lema 5.6.** *Sea $x \in \mathbb{R}$ verificando*

$$\left| x - \frac{a}{q} \right| \leq \frac{1}{q^2} \qquad (a,q) = 1 \quad q \geq 1.$$

*Para cualesquiera números complejos $\alpha_i, \beta_j$ tales que $|\alpha_i| \le 1$, $|\beta_j| \le 1$ y cualquier número real $\lambda \ge 1$ tenemos*

$$\sum_{\substack{ij\le\lambda\\ i>I,\, j>J}}\sum \alpha_i\,\beta_j\; e\,(xij) \ll \left(\frac{\lambda}{I}+\frac{\lambda}{J}+\frac{\lambda}{q}+q\right)^{1/2}\lambda^{1/2}(\log\lambda)^2. \tag{5.9}$$

*Demostración.* Cuando $q \ge \lambda$ el lema es trivial porque

$$\sum_{ij\le\lambda}\sum 1 = \sum_{1\le i\le\lambda}\;\sum_{1\le j\le\lambda/i} 1 \ll \lambda\log\lambda.$$

Estudiamos a continuación el caso $q < \lambda$.

Cuando $ij \le \lambda$ o bien $i \le \sqrt{\lambda}$ o bien $j \le \sqrt{\lambda}$. Pongamos

$$\mathcal{B} := \sum_{\substack{ij\le\lambda\\ i>I,\, j>J}}\sum \alpha_i\,\beta_j\; e\,(xij) = \sum_{\substack{i\le\sqrt{\lambda}\\ ij\le\lambda\\ i>I,\, j>J}}\sum \cdots + \sum_{\substack{j\le\sqrt{\lambda}\\ ij\le\lambda\\ i>I,\, j>J}}\sum \cdots - \sum_{\substack{i,j\le\sqrt{\lambda}\\ ij\le\lambda\\ i>I,\, j>J}}\sum \cdots .$$

Analizamos la primera de estas tres sumas:

$$\mathcal{B}_1 := \sum_{\substack{i\le\sqrt{\lambda}\\ ij\le\lambda\\ i>I,\, j>J}}\sum \alpha_i\,\beta_j\; e\,(xij)\,.$$

Digamos que $\sqrt{\lambda}$ es de la forma $2^n I$ (siempre se puede suponer completando con coeficientes $\alpha_i = \beta_j = 0$). Entonces

$$(I,\sqrt{\lambda}] = (I,2I]\;\cup(2I,4I]\;\cup\;\ldots\cup\;(2^{n-1}I,2^nI],$$

y tomando, de entre todos estos, al intervalo $(H,2H]$ que aporte la mayor contribución a $\mathcal{B}_1$ tenemos

$$\mathcal{B}_1 \ll (\log\lambda)\,|B(\lambda,H)|\,,$$

con

$$B(\lambda,H) := \sum_{H<i\le 2H}\alpha_i \sum_{ij\le\lambda}\beta_j\; e\,(xij)\,.$$

Si denotamos

$$\omega_i = \sum_{j\le\lambda/i}\beta_j\; e\,(xij)\,,$$

y usamos la desigualdad de Cauchy-Schwarz tenemos

$$\begin{aligned} B(\lambda,H)^2 &\le \sum_{H<i\le 2H} |\alpha_i|^2 \cdot \sum_{H<i\le 2H} |\omega_i|^2 \\ &\le 2H \cdot \sum_{H<i\le 2H} \sum_{1\le j_1\le j_2\le \lambda/i} \beta_{j_2}\,\overline{\beta_{j_1}}\, e\left(x(j_2-j_1)i\right) \\ &\le 2H \sum_{1\le j_1\le j_2\le \lambda/H} \sum \beta_{j_2}\,\overline{\beta_{j_1}} \sum_{\substack{H<i\le 2H \\ j_2-j_1\le \lambda/i}} e\left(x(j_2-j_1)i\right) \\ &\ll 2H \sum_{1\le j_1\le \lambda/H} \left( \sum_{H<i\le 2H} \left| \sum_{\substack{1\le j_2-j_1\le \lambda/H \\ j_2-j_1\le \lambda/i}} e\left(x(j_2-j_1)i\right) \right| \right). \end{aligned}$$

Usando ahora (5.6) avanzamos hasta

$$\begin{aligned} B(\lambda,H)^2 &\ll H\frac{\lambda}{H}\left(\frac{\lambda}{H}+H+\frac{\lambda}{q}+q\right)\log q \\ &\ll \lambda\left(\frac{\lambda}{I}+\frac{\lambda}{q}+q\right)\log\lambda, \end{aligned}$$

donde en este último paso hemos usado que $q<\lambda$ y también que

$$\frac{\lambda}{H}+H \ll \frac{\lambda}{H} \ll \frac{\lambda}{I},$$

porque $I<H\le\sqrt{\lambda}$. Por consiguiente

$$\mathcal{B}_1 \ll (\log\lambda)\,|B(\lambda,H)| \ll \left(\frac{\lambda}{I}+\frac{\lambda}{q}+q\right)^{1/2}\lambda^{1/2}(\log\lambda)^2.$$

Cambiando $i, I$ por $j, J$ obtenemos análogamente

$$\mathcal{B}_2 := \sum_{\substack{j\le\sqrt{\lambda} \\ ij\le\lambda \\ i>I,\, j>J}} \sum \alpha_i\,\beta_j\, e\left(xij\right) \ll \left(\frac{\lambda}{J}+\frac{\lambda}{q}+q\right)^{1/2}\lambda^{1/2}(\log\lambda)^2,$$

y para la tercera suma $\mathcal{B}_3$ se obtiene lo mismo. Finalmente observamos que, para cualquier $A$, se tiene

$$\left(\frac{\lambda}{I}+A\right)^{1/2}+\left(\frac{\lambda}{J}+A\right)^{1/2} \ll \left(\frac{\lambda}{I}+\frac{\lambda}{J}+A\right)^{1/2},$$

y la demostración se completa como sigue

$$\mathcal{B} \ll \mathcal{B}_1+\mathcal{B}_2+\mathcal{B}_3 \ll \left(\frac{\lambda}{I}+\frac{\lambda}{J}+\frac{\lambda}{q}+q\right)^{1/2}\lambda^{1/2}(\log\lambda)^2.$$

□

## 5.2. Arcos menores honrando su apellido

### Acotación de $F_N$ en los arcos menores

Vinogradov demostró en 1934 que cuando $|x - a/q| \leq 1/q^2$ con $(a,q) = 1$ entonces se tiene

$$\sum_{p \leq N} e(px) \ll q^{1/2} N^{1/2} + q^{-1/2} N + N e^{-\frac{1}{2}\sqrt{\log N}},$$

(v. [Vi, pág. 131]). Nosotros continuamos parafraseando a [I-K, §13.4, §13.5] hasta conseguir prácticamente la misma cota para la función $\sum_{n \leq N} \Lambda(n) e(nx)$ (v. proposición 5.1). Después aprovechamos que sabemos acotar la diferencia entre esta última función y $F_N(x) := \sum_{p \leq N} \log p \, e(px)$, como hicimos en (4.9).

### La identidad de Vaughan

Figura 5.2: R.V. Vaughan

En 1977 Vaughan consiguió otra importante simplificación en los instrumentos originales usados por Vinogradov. Para mostrarla empezamos con la ecuación

$$\Lambda(n) = \sum_{b|n} \mu(n) \log \frac{n}{b},$$

que se obtiene usando inversión de Möbius (v. lema 3.1) a partir de (3.7).

Aquí nos quedamos con los términos $b \leq y$ y transformamos el resto de la suma como sigue

$$\sum_{\substack{b|n \\ b>y}} \mu(b) \log \frac{n}{b} = \sum_{\substack{bc|n \\ b>y}} \sum \mu(b)\Lambda(c),$$

porque por (3.7) $\sum_{c|n/b} \Lambda(c) = \log(n/b)$. A continuación dejamos como están a los términos con $c > z$ y transformamos el resto de la suma del modo siguiente

$$\sum_{\substack{bc|n \\ b>y,\, c\leq z}} \sum \mu(b)\Lambda(c) = \sum_{\substack{bc|n \\ c\leq z}} \sum \mu(b)\Lambda(c) - \sum_{\substack{bc|n \\ b\leq y,\, c\leq z}} \sum \mu(b)\Lambda(c).$$

Aquí la suma que aparece tras el signo $=$ sobre todos los $b$ dividiendo a $n/c$ se anula a no ser que $c = n$ (v. 3.3) lo cual no es posible si $n > z (\geq c)$. Sumando todas las expresiones anteriores obtenemos

**Lema 5.7** (Vaughan)**.** *Sean $y, z \geq 1$, para todo $n > z$*

$$\Lambda(n) = \sum_{\substack{b|n \\ b\leq y}} \mu(b) \log \frac{n}{b} - \sum_{\substack{bc|n \\ b\leq y,\, c\leq z}} \sum \mu(b)\Lambda(c) + \sum_{\substack{bc|n \\ b>y,\, c>z}} \sum \mu(b)\Lambda(c). \tag{5.10}$$

Llegados a este punto podemos ir ya al grano de esta sección:

**Proposición 5.1.** *Supongamos que $x$ satisface*

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

*Entonces para todo $N \geq 2$*

$$\boxed{\sum_{n \leq N} \Lambda(n) e(nx) \ll \left(q^{1/2} N^{1/2} + q^{-1/2} N + N^{4/5}\right) (\log N)^3 \qquad \forall\, N \geq 2} \tag{5.11}$$

*Demostración.* Pongamos $S_N(x) = \sum_{n \leq N} \Lambda(n) e(nx)$. Por (5.10) tenemos

$$\begin{aligned} S_N(x) = & \sum_{\substack{li \leq N \\ i \leq I}} \sum \mu(i) (\log l)\, e(xli) \\ & - \sum_{\substack{lij \leq N \\ i \leq I, j \leq J}} \sum \sum \mu(i)\, \Lambda(j)\, e(xlij) \\ & + \sum_{\substack{lij \leq N \\ i \geq I, j \geq J}} \sum \sum \mu(i)\, \Lambda(j)\, e(xlij) \\ & + O(J). \end{aligned}$$

Escogemos $I = J = N^{2/5}$. En la primera y en la segunda suma se aplica (5.7) para obtener $O\left((N^{4/5} + N/q + q)(\log N)^2\right)$.

En la última suma consideramos $lj = r$ como una variable con coeficiente

$$c(r) = \sum_{j | r\,,\, j \geq J} \Lambda(j) \leq \log r,$$

donde la última desigualdad se deduce de (3.7). Entonces utilizando (5.9) obtenemos $O\left((N^{3/5} + N/q + q)^{1/2} N^{1/2} (\log N)^3\right)$. Veamos cómo con algo más de detalle a continuación. En primer lugar

$$S_3 = \sum_{\substack{lij \leq N \\ i \geq I, j \geq J}} \sum \sum \mu(i)\, \Lambda(j)\, e(xlij) = \sum_{\substack{ir \leq N \\ i \geq I, r \geq J}} \sum \mu(i)\, e(xir) \sum_{\substack{j | r \\ j \geq J}} \Lambda(j),$$

y por tanto poniendo $\alpha_i = \mu(i)$ y $\beta_r = c(r)/(\log N)$

$$\frac{1}{\log N} S_3 = \sum_{\substack{ir \leq N \\ i \geq I, r \geq J}} \sum \alpha_i\, \beta_r\, e(xir),$$

estamos en la hipótesis del lema 5.6, ya que $ir \leq N \Rightarrow \beta_r \leq 1$. Finalmente aplicando dicho lema y como $I = J = N^{2/5}$

$$\frac{S_3}{\log N} \ll \left(\frac{N}{I} + \frac{N}{J} + \frac{N}{q} + q\right)^{1/2} N^{1/2}(\log N)^2 \ll (N^{3/5} + N/q + q)^{1/2} N^{1/2}(\log N)^2.$$

Sumando estas estimaciones conseguimos (5.11). □

**Corolario 5.1.** *Para $F_N(x) := \sum_{p\leq N} \log p \; e(px)$ y para cualquier $B > 0$, sobre los arcos menores tenemos que*

$$F_N(x) = O\left(\frac{N}{(\log N)^{(B/2)-3}}\right) \qquad \forall\, x \in \mathfrak{m} = [0,1] \setminus \mathcal{M}, \quad B > 0, \tag{5.12}$$

*donde $\mathcal{M}$ es el conjunto de los arcos mayores (v. su definición en la página 39).*

*Demostración.* Sea $x \in \mathfrak{m}$ y pongamos $Q = (\log N)^B$. En primer lugar aproximamos $x$ por un racional irreducible con denominador mayor que $Q$. Para hacerlo utilizamos el teorema 5.1 (v. página 53) tomando $K = N/Q$. Obtenemos así una fracción $a/q \in [0,1]$ con $1 \leq q \leq N/Q$ y $(a,q) = 1$ tal que

$$\left|x - \frac{a}{q}\right| \leq \frac{Q}{qN} \leq \text{mín}\left(\frac{Q}{N}, \frac{1}{q^2}\right).$$

Si $q \leq Q$ entonces $x$ estaría en el *pequeño gran arco* $\mathcal{M}_{a/q}$, lo que es falso. Por lo tanto tenemos

$$\log N = Q < q \leq \frac{N}{Q} = \frac{N}{(\log N)^B}.$$

Como además se cumple la hipótesis de la proposición 5.1, aplicando (5.11) obtenemos

$$\begin{aligned} F_N(x) &= \sum_{n\leq N} \Lambda(n) e(nx) + O(N) \\ &\ll \left(q^{1/2}N^{1/2} + q^{-1/2}N + N^{4/5}\right)(\log N)^3 \\ &\ll \left(\left(\frac{N}{(\log N)^B}\right)^{1/2} N^{1/2} + \frac{N}{(\log N)^{B/2}} + N^{4/5}\right)(\log N)^3 \\ &\ll \frac{N}{(\log N)^{(B/2)-3}}, \end{aligned}$$

en donde $F_N(x) = \sum_{n\leq N} \Lambda(n) e(nx) + O(N)$ se comprueba de modo análogo a (4.9). □

## 5.3. Fórmula asintótica para las representaciones con más de dos primos

**Proposición 5.2.** *Para $F_N(x) := \sum_{p\leq N} \log p \, e(px)$ y para cualquier $B > 0$ tenemos*

$$\boxed{\int_{\mathfrak{m}} [F_N(x)]^k e(-Nx)\, \mathrm{d}x \;\ll_{B,k}\; \frac{N^{k-1}}{(\log N)^{(B/2)-4}} \qquad \forall\, k > 2,} \tag{5.13}$$

*en donde* $\mathfrak{m} = [0,1] \setminus \mathcal{M}$ *(con los arcos mayores* $\mathcal{M}$ *definidos como en la página 39).*

*Demostración.* En el lema 4.1 ya estimamos asintóticamente la media de $F_N^2$

$$\int_0^1 |F_N(x)|^2 \ll N \log N,$$

y usando ahora esta acotación, además de (5.12) y notando que $k \geq 3$ tenemos

$$\begin{aligned}\int_{\mathfrak{m}} [F_N(x)]^k \, e(-Nx) \, \mathrm{d}x \ll \\ &\ll \sup_{x \in \mathfrak{m}} |F_N(x)|^{k-2} \int_{\mathfrak{m}} |F_N(x)|^2 \\ &\ll \frac{N^{k-2}}{(\log N)^{(B/2)-3}} \int_0^1 |F_N(x)|^2 \\ &\ll \frac{N^{k-1}}{(\log N)^{(B/2)-4}}.\end{aligned}$$

□

La demostración anterior solamente funciona cuando $k \geq 3$. Hemos tropezado con **un escollo que deja descolgado al caso** $k = 2$. Se trata de un hueso que parece duro de roer como comentaremos en el capítulo 6.

Sea un entero $k > 2$ y $\mathcal{P} := \{p \colon p \text{ es primo }\}$. Vamos a culminar todo el trabajo anterior estimando a continuación la función

$$R(N; k, \mathcal{P}) := \sum_{p_1 + \cdots + p_k = N} (\log p_1) \cdots (\log p_k).$$

**Teorema 5.2.** *Cuando* $N$ *y* $k$ *tienen la misma paridad tenemos , para todo* $A > 0$

$$\boxed{R(N; k, \mathcal{P}) = \mathfrak{S}_k(N) \, \frac{N^{k-1}}{(k-1)!} \left(1 + O\left(\frac{1}{(\log N)^A}\right)\right) \quad k > 2 \quad N \equiv k \text{ mód } 2} \tag{5.14}$$

*Demostración.* Utilizamos ahora la contribución de los arcos mayores (4.15) y la de los arcos menores (5.13). En definitiva tenemos que

$$\begin{aligned}R(N; k, \mathcal{P}) &= \int_0^1 [F_N(x)]^k \, e(-Nx) \, \mathrm{d}x \\ &= \int_{\mathcal{M}} [F_N(x)]^k \, e(-Nx) \, \mathrm{d}x + \int_{\mathfrak{m}} [F_N(x)]^k \, e(-Nx) \, \mathrm{d}x \\ &= \mathfrak{S}_k(N) \, \frac{N^{k-1}}{(k-1)!} + O\left(\frac{N^{k-1}}{(\log N)^{B-1}}\right) + \\ &+ O\left(\frac{N^{k-1}}{(\log N)^{(B/2)-4}}\right).\end{aligned}$$

Dado $A > 0$ tomemos $B = 2A + 8$, entonces

$$R(N; k, \mathcal{P}) = \mathfrak{S}_k(N)\, \frac{N^{k-1}}{(k-1)!} + O\left(\frac{N^{k-1}}{(\log N)^A}\right),$$

como queríamos demostrar. □

**Teorema 5.3.** *Sea un entero $k > 2$ y $\mathcal{P} := \{p\colon p \text{ es primo }\}$. Cuando $N$ y $k$ tienen la misma paridad tenemos la estimación*
(5.15)

$$r(N; k, \mathcal{P}) = \mathfrak{S}_k(N)\, \frac{N^{k-1}}{(k-1)!(\log N)^k}\left(1 + O\left(\frac{\log\log N}{\log N}\right)\right) \qquad k > 2 \quad N \equiv k \text{ mód } 2,$$

*y en consecuencia se verifica la estimación asintótica*

(5.16)
$$\boxed{r(N; k, \mathcal{P}) \sim \mathfrak{S}_k(N)\, \frac{N^{k-1}}{(k-1)!(\log N)^k} \qquad \forall\, N \in \mathbb{N},\ k > 2 \quad N \equiv k \text{ mód } 2}$$

*donde $\mathfrak{S}_k(N)$ es la serie singular (v. proposición 4.2).*

*Demostración.* Partimos de la estimación para la función

$$R(N; k, \mathcal{P}) := \sum_{p_1+\cdots+p_k=N} (\log p_1)\cdots(\log p_k),$$

que acabamos de encontrar (v. teorema 5.2):

$$R(N; k, \mathcal{P}) = \mathfrak{S}_k(N)\frac{N^{k-1}}{(k-1)!} + O\left(\frac{N^{k-1}}{(\log N)^A}\right) \qquad \forall\ A > 0 \quad k > 2. \tag{5.17}$$

Sea $\theta \in (1/2, 1)$, tenemos

$$R(N; k, \mathcal{P}) \geq \sum_{\substack{p_1+\cdots+p_k=N \\ \forall\, i\ p_i > N^\theta}} (\log p_1)\cdots(\log p_k) \geq (\theta \log N)^k \left[r(N; k, \mathcal{P}) - \rho_k(N, \theta)\right],$$

donde

$$\rho_k(N, \theta) := \sum_{i=1}^{k} \sum_{\substack{p_1+\cdots+p_k=N \\ \exists\, i\ p_i \leq N^\theta}} 1 = k \sum_{\substack{p_1+\cdots+p_k=N \\ p_1 \leq N^\theta}} 1 = \sum_{p_1 \leq N^\theta} \sum_{p_2+\cdots+p_k=N-p_1} 1$$

$$\leq \sum_{p_1 \leq N^\theta} \sum_{p_3+\cdots+p_k=N-p_1} 1 \leq \left(\sum_{p_1 \leq N^\theta} 1\right)\left(\sum_{p_3+\cdots+p_k<N} 1\right) \leq \pi(N^\theta)[\pi(N)]^{k-2}.$$

Entonces por (3.9)

$$\rho_k(N, \theta) \ll \frac{N^\theta}{\log N}\left(\frac{N}{\log N}\right)^{k-2},$$

de modo que

$$r(N;k,\mathcal{P})(\log N)^k \leq \theta^{-k}\, R(N;k,\mathcal{P}) + O\left(N^{k-2+\theta}\log N\right);$$

como también $R(N;k,\mathcal{P}) \leq r(N;k,\mathcal{P})(\log N)^k$ y además $\theta^{-k} - 1 > \theta - 1$ se obtiene

$$0 \leq r(N;k,\mathcal{P})(\log N)^k - R(N;k,\mathcal{P}) = O\left((1-\theta)R(N;k,\mathcal{P}) + N^{k-1}N^{\theta-1}\log N\right).$$

Escogiendo $\theta$ tal que $N^{\theta-1}\log N = 1$

$$\begin{aligned} &0 \leq r(N;k,\mathcal{P})(\log N)^k - R(N;k,\mathcal{P}) = \\ &= O\left(\frac{\log\log N}{\log N}R(N;k,\mathcal{P}) + N^{k-1}\right) = O\left(\frac{\log\log N}{\log N}N^{k-1}\right), \end{aligned}$$

donde en el último paso hemos usado la estimación (5.17) con $A = 1$ que utilizamos de nuevo, tras despejar en lo anterior, para concluir que

$$\begin{aligned} r(N;k,\mathcal{P}) &= \frac{R(N;k,\mathcal{P})}{(\log N)^k} + O\left(\frac{N^{k-1}\log\log N}{(\log N)^{k+1}}\right) = \\ &= \mathfrak{S}_k(N)\,\frac{N^{k-1}}{(k-1)!(\log N)^k}\left(1 + O\left(\frac{\log\log N}{\log N}\right)\right), \end{aligned}$$

lo que completa la demostración. □

### 5.3.1. El Teorema de Vinogradov

Al comienzo del capítulo X del libro [Vi] se advierte de la notación $r = \log N$. Unas páginas después Vinogradov enuncia los dos siguientes resultados:

**Teorema 5.4.** *El número $I(N)$ de representaciones de un entero positivo impar $N$ como $p_1 + p_2 + p_3$ puede ser expresado por la fórmula*

$$I(N) = \frac{N^2}{2r^3}\mathfrak{S}(N) + O\left(\frac{N^2}{r^{\frac{7}{2}-\epsilon}}\right),$$

*donde $\epsilon > 0$ y*

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

*el primer producto extendido a todos los primos. Además el producto $\mathfrak{S}(N)$ satisface*

$$\mathfrak{S}(N) > \frac{6}{\pi^2}$$

*para todo $N$.*

**Corolario 5.2** (Teorema de Goldbach)**.** *Existe un número $c_0$ tal que todo entero impar $N \geq c_0$ se puede representar como la suma de tres primos.*

El Teorema de Vinogradov con corolario que acabamos de enunciar es un caso particular del teorema 5.3.

Recogemos aquí literalmente el argumento de Vinogradov acerca de la cota inferior de la serie singular:

"Partiendo de

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

que es equivalente a la fórmula enunciada ya que

$$\frac{1-(p-1)^{-2}}{1+(p-1)^{-3}} = 1-\frac{1}{p^3-3p+3},$$

tenemos que

$$\begin{aligned}\mathfrak{S}(N) &> \prod_{p|N}\left(1-\frac{1}{(p-1)^2}\right)\\ &> \prod_{p}\left(1-\frac{1}{p^2}\right) = \frac{6}{\pi^2},\end{aligned}$$

puesto que $N$ es impar y en consecuencia en el primer producto tenemos $p-1 \geq p_1$ donde $p_1$ es el primo más grande menor que $p$."(ref. [Vi, pág. 174])


Figura 5.3: I.M.Vinogradov

Sobre el número $c_0$ que aparece en el corolario antedicho, en [The-P-C-to-Maths, §V.27, pág. 715] se puede leer "¿Cuán grande es «suficientemente grande»? Bueno, hasta hace poco necesitabas que tu número tuviese alrededor de 7 000 000 dígitos, pero en 2002 esto se redujo a 1 500 dígitos".

## 5.4. Casi todo par es la suma de dos primos

Definimos *el número de excepciones* $E(x)$ como el cardinal del conjunto excepcional, formado por todos los números pares menores o iguales que $x$ que no son suma de ninguna pareja de números primos:

$$E(x) := \#\{n \text{ par } \leq N \mid r(n;2,\mathcal{P}) = 0\}.$$

La conjetura de Goldbach se puede reformular como la afirmación $E(x) = 1$ para todo $x \geq 2$. En esta sección mostramos que $E(x) = o(x)$, parafraseando a [Va, §3.2].

Para aligerar algo la escritura ponemos

$$I_A(N,n) := \int_A [F_N(x)]^2 e\,(-nx)\,\mathrm{d}x \qquad n \leq N \text{ enteros positivos.}$$

donde $F_N(x) := \sum_{p\leq N} \log p\, e(px)$, y con esta notación recordamos una vez más que

$$R(n;2,\mathcal{P}) = I_{\mathcal{M}}(N,n) + I_{\mathfrak{m}}(N,n) \qquad n \leq N. \tag{5.18}$$

(v. lema 2.1). Los símbolos $R(n;2,\mathcal{P}), \mathcal{M}, \mathfrak{m}, \mathfrak{S}_2$, corresponden con los conceptos que hemos venido usando en varias ocasiones anteriormente en este trabajo. (para localizar sus definiciones v. tabla en la página XIII)

**Lema 5.8.** *Sea $A > 0$ una constante positiva cualquiera y $N$ cualquier entero positivo. Véase la definición de los arcos mayores para las representaciones con sumas de primos $\mathcal{M}$ (v. página 39). Entonces en los arcos menores $\mathfrak{m} = [0,1] \setminus \mathcal{M}$ tenemos*

$$\sum_{n=1}^{N} |I_{\mathfrak{m}}(N,n)|^2 = O\left(\frac{N^3}{(\log N)^A}\right) \quad \forall\, A > 0, \tag{5.19}$$

*donde*

$$I_{\mathfrak{m}}(N,n) := \int_{\mathfrak{m}} [F_N(x)]^2 e(-nx)\, \mathrm{d}x.$$

*Demostración.* $I_{\mathfrak{m}}(N,n)$ es el $n$-ésimo coeficiente de Fourier de la función $1_{\mathfrak{m}} \cdot [F_N(x)]^2$, donde $1_{\mathfrak{m}}$ es la función característica del conjunto de los arcos menores. Por la identidad de Parseval

$$\sum_{n=1}^{N} |I_{\mathfrak{m}}(N,n)|^2 \leq \sum_{n=-\infty}^{n=+\infty} |I_{\mathfrak{m}}(N,n)|^2 = \int_0^1 \left|1_{\mathfrak{m}} \cdot [F_N(x)]^2\right|^2 \mathrm{d}x = \int_{\mathfrak{m}} |F_N(x)|^4\, \mathrm{d}x.$$

Como en la demostración de la proposición 5.2, para cualquier $B > 0$ con la definición de arcos menores dada por $Q = (\log N)^B$ se cumple que (por el lema 4.1 y el corolario 5.1):

$$\begin{aligned}\sum_{n=1}^{N} |I_{\mathfrak{m}}(N,n)|^2 &\leq \sup_{x\in\mathfrak{m}} |F_N(x)|^2 \int_{\mathfrak{m}} |F_N(x)|^2 \\ &\ll \frac{N^2}{(\log N)^{(B/2)-3}} \int_0^1 |F_N(x)|^2 \\ &\ll \frac{N^3}{(\log N)^{(B/2)-4}}.\end{aligned}$$

Para terminar tomamos $B \geq 2A + 8$. □

**Lema 5.9.** *Sea $A > 0$ una constante positiva cualquiera y $N$ cualquier entero positivo. Véanse las definiciones de los arcos mayores para las representaciones con sumas de primos $\mathcal{M}$ (v. página 39) y de la serie singular $\mathfrak{S}_2$ (v. página 47). Se cumple lo siguiente*

$$\sum_{n=1}^{N} |I_{\mathcal{M}}(N,n) - n\, \mathfrak{S}_2(n)|^2 = O\left(\frac{N^3}{(\log N)^A}\right) \qquad \forall\, A > 0, \tag{5.20}$$

*donde*

$$I_{\mathcal{M}}(N,n) := \int_{\mathcal{M}} [F_N(x)]^2 e(-nx)\, \mathrm{d}x.$$

*Demostración.* Para el $B > 0$ que define a los arcos mayores $\mathcal{M}$, haciendo ajustes triviales a la demostración de la proposición 4.3 se obtiene la siguiente estimación —similar a (4.15)—

$$I_{\mathcal{M}}(N,n) = n\mathfrak{S}_2(n,\log N) + O\left(N(\log N)^{1-B}\right) \qquad \forall\, 1 \le n \le N \quad B > 0. \tag{5.21}$$

donde

$$\mathfrak{S}_2(n,x) := \sum_{q\le x} \frac{\mu^2(q)\, c_q(-n)}{\phi^2(q)} \qquad \text{y} \qquad \mathfrak{S}_2(n) := \mathfrak{S}_2(n,\infty).$$

Pongamos $Q := (\log N)^B$. En primer lugar

$$\begin{aligned}
\mathfrak{S}_2(n,Q) - \mathfrak{S}_2(n) &= \sum_d \sum_{\substack{q'>Q\\(q',n)=d}} \left[\frac{\mu(q')}{\phi(q')}\right]^2 c'_q(-n) \\
&= \sum_d \sum_{\substack{qd>Q\\(q,n)=1}} \left[\frac{\mu(qd)}{\phi(qd)}\right]^2 c_{qd}(-n) \qquad \text{poniendo } q' = qd \\
&= \sum_d \sum_{\substack{q>Q/d\\(q,n)=1}} \left[\frac{\mu(qd)}{\phi(qd)}\right]^2 \mu(q)\frac{\phi(qd)}{\phi(q)} \qquad \text{por (3.8)} \\
&= \sum_{d|n} \frac{\mu(d)^2}{\phi(d)} \sum_{\substack{q>Q/d\\(q,n)=1}} \frac{\mu(q)}{\phi(q)^2} \qquad \text{por el lema 3.3} \\
&\ll \sum_{d|n} \frac{\mu(d)^2}{\phi(d)} \cdot \text{mín}\left(\frac{d}{Q}, 1\right),
\end{aligned}$$

en donde hemos usado que $\mu(q)^3 = \mu(q)$ y, en el último paso, que

$$\sum_{q>x} \frac{1}{\phi(q)^2} \ll \frac{1}{x},$$

(v. la demostración del lema 4.5 en la página 48). En segundo lugar, dando un paso más en la serie anterior de acotaciones y recordando el comportamiento asintótico la función de $\phi$ (en concreto $\phi(d) \gg d/\log d$ que se deduce de (3.6)):

$$\mathfrak{S}_2(n,Q) - \mathfrak{S}_2(n) \ll \sum_{d|n} \frac{\mu(d)^2}{\phi(d)} \ll \sum_{d\le n} \frac{\log d}{d} \le \log n \sum_{d\le n} \frac{1}{d} \ll (\log n)^2.$$

Juntando las dos acotaciones anteriores tenemos

$$\begin{aligned}
\sum_{n=1}^{N} |\mathfrak{S}_2(n,Q) - \mathfrak{S}_2(n)|^2 &\ll \sum_{n=1}^{N} (\log n)^2 \, |\mathfrak{S}_2(n,Q) - \mathfrak{S}_2(n)| \\
&\leq (\log N)^2 \sum_{n=1}^{N} \left| \sum_{q>Q} \left[ \frac{\mu(q)}{\phi(q)} \right]^2 c_q(-n) \right| \\
&\ll (\log N)^2 \sum_{n\leq N} \sum_{d|n} \frac{\mu(d)^2}{\phi(d)} \cdot \text{mín} \left( \frac{d}{Q}, 1 \right) \\
&\ll (\log N)^2 \frac{N}{Q} \sum_{n\leq N} \sum_{d|n} \frac{\mu(d)^2}{\phi(d)} \\
&\ll (\log N)^2 \frac{N}{Q} \sum_{d\leq N} \frac{1}{\phi(d)} \\
&\ll (\log N)^3 \frac{N}{Q}.
\end{aligned}$$

Con esto y usando (5.21), además de $Q = \log N$, comprobamos que

$$\begin{aligned}
\sum_{n=1}^{N} |I_{\mathcal{M}}(N,n) - n\ \mathfrak{S}_2(n)|^2 &= \sum_{n=1}^{N} \left| n\left[\mathfrak{S}_2(n,\log N) - \mathfrak{S}_2(n)\right] + O\left(N(\log N)^{1-B}\right) \right|^2 \\
&= \sum_{n=1}^{N} |n\left[\mathfrak{S}_2(n,\log N) - \mathfrak{S}_2(n)\right]|^2 + \sum_{n=1}^{N} O\left(N(\log N)^{1-B}\right)^2 + \\
&+ \sum_{n=1}^{N} 2\ \left|n\left[\mathfrak{S}_2(n,\log N) - \mathfrak{S}_2(n)\right]\right| \cdot O\left(N(\log N)^{1-B}\right) \\
&\ll N^2(\log N)^3 \frac{N}{(\log N)^B} + N\frac{N^2}{(\log N)^{2(B-1)}} + N(\log N)^2 \frac{N}{(\log N)^{1-B}} \\
&= O\left(\frac{N^3}{(\log N)^{B-3}}\right),
\end{aligned}$$

y escogiendo $B \geq A + 3$ se completa la demostración. □

**Lema 5.10.** *Sea $A > 0$ una constante positiva cualquiera y $N$ cualquier entero positivo. Véanse las definiciones de $R(n;2,\mathcal{P})$ (v. página 36) y de $\mathfrak{S}_2(n)$ (v. página 47). Tenemos*

$$\sum_{n\leq N/2} |R(2n;2,\mathcal{P}) - 2n\ \mathfrak{S}_2(2n)|^2 = O\left(\frac{N^3}{(\log N)^A}\right) \quad \forall\ A > 0.$$

*Demostración.* Combinamos las fórmulas (5.18), (5.19) y (5.20):

$$\sum_{n\leq N/2} |R(2n;2,\mathcal{P}) - 2n\,\mathfrak{S}_2(2n)|^2 \leq \sum_{n=1}^{N} |I_{\mathcal{M}}(n) - n\,\mathfrak{S}_2(n)|^2 + \sum_{n=1}^{N} |I_{\mathfrak{m}}(n)|^2 \ll \frac{N^3}{(\log N)^A}.$$

□

Ahora ya podemos demostrar el

**Teorema 5.5** (Chudakov, van der Corput, Estermann)**.** *Si*

$$E(N) := \#\{2n \leq N \mid r(2n;2,\mathcal{P}) = 0\},$$

*entonces para todo* $A > 0$

$$\boxed{E(N) = O\left(\frac{N}{(\log N)^A}\right) \qquad \forall\ A > 0.}$$

*Demostración.* Para cada excepción $2n$ tenemos que $R(2n;2,\mathcal{P}) = 0$ y por tanto

$$\frac{1}{(2n)^2}\,|R(2n;2,\mathcal{P}) - 2n\,\mathfrak{S}_2(2n)|^2 = \mathfrak{S}_2(2n)^2 \gg 1,$$

por el corolario 4.2. En consecuencia

$$E(N) \ll \sum_{n\leq N/2} |R(2n;2,\mathcal{P}) - 2n\,\mathfrak{S}_2(2n)|^2\,\frac{1}{(2n)^2}.$$

Para concluir la prueba se hace sumación por partes (usando el lema 3.5 con $f(x) = |R(x;2,\mathcal{P}) - x\,\mathfrak{S}_2(x)|^2$ y $g(x) = 1/x^2$) y después se echa mano del resultado del lema 5.10. □

**Corolario 5.3.** *Si* $E(x) := \#\{2n \leq x \mid r(2n;2,\mathcal{P}) = 0\}$ *entonces* $E(x) = o(x)$*, es decir*

$$\lim_{x\to\infty} \frac{E(x)}{x} = 0.$$

Es corolario dice que la densidad del conjunto excepcional tiende a cero, y en este sentido casi todo número par se puede representar como suma de dos primos:

En 1976 Montgomery y Vaughan mejoraron el teorema 5.5 obteniendo el siguiente resultado

**Teorema 5.6** (Montgomery y Vaughan)**.** *Sea* $E(N) := \#\{n\ par\ \leq N \mid r(n;2,\mathcal{P}) = 0\}$. *Existe* $c > 1$ *tal que*

$$\boxed{\exists\ c > 1 \qquad E(x) = O\left(x^{1-c}\right)}$$

# Capítulo 6

# Por qué la conjetura de Goldbach es difícil

Fijado un primo $p$, los valores de $e(px)$ resuenan en las frecuencias $x = a/q$ racionales (v. final del capítulo 2). Imaginemos que, por el contrario, cuando $x$ se mueve entre los irracionales, las oscilaciones de $\{e(px) \mid x \in [0,1] \setminus \mathbb{Q}\}$ son significativamente imprevisibles y que asumimos —con heurístico atrevimiento— modelar la pseudo-aleatoriedad de dichos números usando una misma distribución de probabilidad tanto para su parte real como para su parte imaginaria.

Llamemos $\mathbb{X}_p, \mathbb{Y}_p$ a las funciones definidas sobre los arcos menores $\mathfrak{m}$ como sigue

$$\mathbb{X}_p(x) := \mathrm{Re}\,(e(px)) \qquad \mathbb{Y}_p(x) := \mathrm{Im}\,(e(px))\,.$$

Supongamos también que las $\pi(N)$ *variables aleatorias* $\mathbb{X}_p$, $p \leq N$ son independientes entre sí e igualmente distribuidas con esperanza $\mu = 0$ y varianza $0 < \sigma^2 \leq 1$, puesto que $e(px)$ tiene siempre valor absoluto 1. Con estas hipótesis el Teorema Central del Límite nos indicaría que

$$\mathbb{X}_N := \frac{\sum_{p\leq N} \mathbb{X}_p - \pi(N)\mu}{\sqrt{\pi(N)\sigma^2}} \quad \xrightarrow[N\to\infty]{d.} \quad \mathrm{Normal}(0,1)\,; \tag{6.1}$$

es decir: la *variable aleatoria* $\mathbb{X}_N$ tendría aproximadamente la misma distribución de probabilidad que la normal estándar, para $N$ suficientemente grande. Llamemos $\Phi$ a la función de distribución de la normal estándar. Fijado $0 < \epsilon < 1$ denotemos por $x_\epsilon \in \mathbb{R}$ al valor que satisface

$$\Phi(x_\epsilon) = \mathbb{P}(\mathrm{Normal}(0,1) \leq x_\epsilon) = 1 - \epsilon,$$

y recordemos que cuando $x_\epsilon \geq 2$ crece el valor de $\epsilon$ se acerca rápidamente a 0.
De (6.1) se deduciría que, asintóticamente,

$$\mathbb{P}\left(\frac{\left|\sum_{p\leq N} \mathbb{X}_p\right|}{\sqrt{\pi(N)}} \geq x_\epsilon \sigma\right) \sim 2(1 - \Phi(x_\epsilon)) = 2\epsilon.$$

Este argumento heurístico empuja a conjeturar que, para la mayoría de valores de $x$ sobre los arcos menores, es de esperar que

$$\sum_{p\leq N} \mathbb{X}_p(x) \ll \sqrt{\pi(N)}.$$

Por un razonamiento análogo también $\sum_{p\leq N} \mathbb{Y}_p(x) \ll \sqrt{\pi(N)}$ en dichos valores de $x$. Puesto que

$$f_N(x) := \sum_{p\leq N} e\,(px) = \sum_{p\leq N} \mathbb{X}_p(x) + \sum_{p\leq N} \mathbb{Y}_p(x),$$

podríamos concluir que

$$f_N(x) \ll \sqrt{\pi(N)} \sim \sqrt{\frac{N}{\log N}} \qquad \text{para “la mayoría de” } x \in \mathfrak{m}. \tag{6.2}$$

Otra indicación de que probablemente esta sea una cota difícil de mejorar proviene del hecho de que la medida de Lebesgue del conjunto de los arcos menores se acerca asintóticamente a la medida de Lebesgue de todo el intervalo [0,1]. Para $N$ suficientemente grande podemos esperar que

$$\int_{\mathfrak{m}} f_N(u)^2\,\mathrm{d}u \approx \int_0^1 f_N(u)^2\,\mathrm{d}u = \sum_{p\leq N} 1^2 = \pi(N).$$

La estimación (6.2) resultaría consistente con lo que en ciertas fuentes se denomina la *filosofía de la cancelación de la raíz cuadrada.* [1]

Asumiendo (6.2) y sumando por partes tendríamos

$$F_N(x) := \sum_{p\leq N} \log p\; e\,(px) \ll \sqrt{N \log N} \qquad \text{para “la mayoría de” } x \in \mathfrak{m}, \tag{6.3}$$

como una cota que parece arduo poder rebajar. Ya hemos encontrado otros indicios de (6.3) en el lema 4.1 y en la gráfica que se muestra en la página 39.

Estas reflexiones apuntan a la dificultad de resolver la conjetura de Goldbach por medio del método del círculo. Otra obstrucción que nos apercibió de esta dificultad fue el hecho de que $\mathfrak{S}_3(2n) = 0$ (v. comentario tras el corolario 4.2 en la página 49).

Mientras no se pueda rebajar (6.3), las herramientas que nos han servido para resolver el caso $k \geq 3$ son inútiles para $k = 2$. Al tratar de emular la demostración del teorema 5.2 tendríamos

$$R(N; 2, \mathcal{P}) = \mathfrak{S}_2(N)\; N + Err_1(N) + Err_2(N), \tag{6.4}$$

[1] Se habla de esta *filosofía* varias veces en el en el libro [M-TB]. También en relación con esto podemos recomendar http://blogs.ethz.ch/kowalski/2008/07/07/is-there-a-combinatorial-square-root-cancellation-philosophy/

en donde el candidato a término de error proveniente de los arcos menores estaría acotado, por (6.3), como sigue:

$$\begin{aligned} Err_2(N) = \int_{\mathfrak{m}} [F_N(x)]^2 \, e\,(-Nx)\ \mathrm{d}x \ll \\ \ll \int_{\mathfrak{m}} N \log N \, \mathrm{d}x \\ \leq N \log N. \end{aligned}$$

Lamentablemente con esta cota el candidato a término principal $\mathfrak{S}_2(N)\, N$ **no prevalece asintóticamente sobre** $Err_2(N)$

$$\frac{Err_2(N)}{\mathfrak{S}_2(N)\, N} \ll \frac{\log N}{\mathfrak{S}_2(N)}$$

y la presunta estimación (6.4) resulta inútil: no se puede garantizar que, para $N$ grande, se tenga $R(N; 2, \mathcal{P}) > 0$. Lo único que falla es una potencia de logaritmo: se necesitaría rebajar (6.3) hasta algo como

$$\exists\ \delta > 0 \qquad \sum_{p \leq N} \log p \; e\,(px) \ll \sqrt{N\ (\log N)^{-\delta}} \qquad \text{para “la mayoría de” } x \in \mathfrak{m},$$

lo que implicaría que $Err_2(N) = o\,(\mathfrak{S}_2(N)\, N)$. Pero poder conseguir esta mejora parece muy poco probable. En definitiva lo que necesitamos es acotar

$$\left| \int_{\mathfrak{m}} F_N(x)^2 \, e\,(-Nx)\ \mathrm{d}x \right|.$$

“Sin embargo, demostrar que hay cancelación en la integral anterior es muy difícil. Es mucho más fácil trabajar con valores absolutos. El que no podamos probar que la contribución de los arcos menores es pequeña no significa que el método del círculo no es útil o que no sea capaz un día de probar la Conjetura de Goldbach. Las simulaciones numéricas confirman, para muchos problemas, que los arcos menores no contribuyen para muchos $N$. ”[M-TB, pág. 325]

# Bibliografía y otras referencias


[Ch-1] Chamizo, F.
*Ideas sobre el método del círculo* (2011)
http://web.uam.es/personal_pdi/ciencias/fchamizo/kiosco/kiosco.html

[Ch-2] Chamizo, F.
temario anotado de *Curso avanzado de Teoría de Números* (2006)
http://www.uam.es/personal_pdi/ciencias/fchamizo/asignaturas/to2009/semavanz0506/semavanz0506.html

[Ch-3] Chamizo, F.
*El Teorema de los números primos en progresiones aritméticas* (2011)
http://web.uam.es/personal_pdi/ciencias/fchamizo/kiosco/kiosco.html

[Ch-4] Chamizo, F.
*Rudimentos sobre métodos de criba* (2006)
http://web.uam.es/personal_pdi/ciencias/fchamizo/kiosco/kiosco.html

[Ch-C-U] Chamizo, F., Cristóbal, E. y Ubis, A.
*El método del círculo*
La Gaceta de la RSME Volumen 9, Número 1 (2006)

[Ci] Cilleruelo, J.
*La conjetura de Goldbach*
La Gaceta de la RSME Volumen 3, Número 3 (septiembre-diciembre, 2000)

[C-C] Cilleruelo, J. y Córdoba, A.
*La Teoría de los números*
Mondadori 1992

[Cr] Cristóbal, E.
*El método del círculo* (2003)
http://web.uam.es/personal_pdi/ciencias/fchamizo/posgrado/posgrado.html

[E-M] Ellison, W.J., Mendès. M.
*Les nombres premiers*
Hermann, 1975

[G] Goss, D.
*Some Hints on Mathematical Style*
http://www.math.ohio-state.edu/%7Egoss/hint.pdf

[G-O] Guevara Bravo, J. y Ojeda Uresti, J.
*¿Formuló Goldbach la conjetura de Goldbach?*
*Ciencias*, enero-marzo, número 081 2006
http://redalyc.uaemex.mx/src/inicio/ArtPdfRed.jsp?iCve=64408112

[H-W] Hardy G.H., y Wright, E.M.
*An Introduction to the Theory of Numbers*
Oxford Press, fifth edition 1979

[I-K] Iwaniec, H. y Kowalski, E.
*Analytic number theory*
American Mathematical Society 2004

[M-TB] Miller, S. y Takloo-Bighash, R.
*An invitation to modern number theory*
Princetown University Press 2006

[M-V] Montgomery, H. y Vaughan, R.
*Multiplicative Number Theory. I Classical Theory*
Cambridge University Press, 2007

[N] Nathanson, M.B.
*Additive Number Theory. The Classical Bases*
Springer 1996

[R] Raboso, D.
*Caracteres* (2010)
http://web.uam.es/personal_pdi/ciencias/fchamizo/posgrado/posgrado.html

[T] Tao, T.
*On writing*
http://terrytao.wordpress.com/advice-on-writing-papers/

[Te] Tesoro, R.
*Una demostración analítica del Teorema de los Números Primos* (2011)
http://web.uam.es/personal_pdi/ciencias/fchamizo/posgrado/posgrado.html

[Va] Vaughan, R.C.
*The Hardy-Littlewood method*
Cambridge University Press 1981

[Vi] Vinogradov, I.M.
*The Method of Trigonometrical Sums in the Theory of Numbers*
Dover Publications, Inc. 2004

[The-P-C-to-Maths] *The Princeton Companion to Mathematics*
Edited by Timothy Gowers
Princetown University Press 2008

[mathworld] *Goldbach conjecture*
`http://mathworld.wolfram.com/GoldbachConjecture.html`

[mathoverflow] *Translation of Goldbach's 1742 letter to Euler*
`http://mathoverflow.net/questions/23349/translation-of-goldbachs-1742-letter-to-euler`

[T-P-Glossary] *The Prime Glossary - Goldbach's conjecture*
`http://primes.utm.edu/glossary/page.php?sort=GoldbachConjecture`

## Créditos

Este documento se terminó de componer en septiembre de 2011 con LaTeX escribiendo en el editor Texmaker con oscilaciones entre las dos distribuciones TeX Live para Mac OS y MiKTeX para Windows.

La autoría/procedencia de las figuras es: fig. 1.1 y 5.2 imágenes descargadas desde Wikipedia, fig. 2.1, 3.1 y 3.4 imágenes tomadas de The MacTutor History of Mathematics archive. Los créditos de la imagen en la fig. 5.3 son para RIA NOVOSTI/SCIENCE PHOTO LIBRARY y fue descargada desde el cibersitio de Science Photo Library. L. Martínez dibujó la fig. 5.1 y F. Chamizo preparó la gráfica fig. 1.2; el resto de figuras fueron preparadas por R. Tesoro.

Creemos que las imágenes copiadas en este trabajo son de dominio público. Si usted cree que posee derechos de autor sobre alguna de estas imágenes, por favor contacte al autor o al tutor y o bien la quitaremos o añadiremos el correspondiente reconocimiento.

El  termina aquí esta etapa del camino pensando QUID ULTRA FACIAM.