Universidad Nacional Autónoma de México

Facultad de Ciencias

Primos en progresiones aritméticas de Dirichlet como sumas de potencias

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

MATEMATICO

PRESENTA:

Raúl Rodríguez Barrera

TUTOR

Mat. Julio César Guevara Bravo

Ciudad de México 2019

1. Datos del alumno
Rodríguez
Barrera
Raúl
Universidad Nacional Autónoma de
México
Facultad de Ciencias
Matemáticas
311331831

2. Datos del tutor
Mat.
Julio Cesar
Guevara
Bravo

3. Datos del sinodal 1
Dra.
Diana
Avella
Alaminos

4. Datos del sinodal 2
Dr. Juan José
Alba
González

5. Datos del sinodal 3
M. en C.
Oscar Alberto
Garrido
Jiménez

6. Datos del sinodal 4
Dr.
Alejandro
Alvarado
García

7. Datos del trabajo escrito
Primos en progresiones aritméticas de
Dirichlet como sumas
de potencias
108 p
2019

La matemática es la reina
de las ciencias
y la teoría de números es
la reina de las matemáticas.
Gauss

Este trabajo está dedicado
con un profundo amor a mi madre.

Agradecimientos

A mis padres por su apoyo incondicional, sin ellos este trabajo no hubiera sido posible, a mis hermanos en especial a Tere por convertirse en mi enfermera particular, a mi tío Cipriano, mi tía Alvara, mi abuela María y mis primos Elias, Gaby y Luz por abrirme las puertas de su casa en esta etapa tan difícil de mi vida.

A César Guevara por toda su dedicación y paciencia, por todas sus enseñanzas desde mi primer día en la Facultad, y por guiarme en la realización esta tesis hasta el final.

A Oscar Garrido por darme la oportunidad de iniciar mi carrera como académico en la facultad, por todo su apoyo incondicional ante todo y más allá de los aspectos académicos gracias por tu amistad.

A Raúl D. Morales por ayudarme cuando lo necesité.

A Cristina por nunca dejarme solo y apoyarme en todo

A todos mis amigos que a pesar de todo nunca dejaron de apoyarme, a "la oficina" en especial Ale, Caro, Diego, Hugo, Joseph y Naty, con ellos compartí momentos maravillosos durante la carrera.

A Bere porque siempre que te necesito estás para apoyarme, gracias.

Índice general

0.1. Introducción

Los números primos son aún un objeto de estudio de gran interés, lo han sido desde la época dorada de la antigua Grecia y Euclides demostró por primera vez que existe una infinidad de ellos.

En los cursos actuales de introducción a la Teoría de Números aún se estudia la infinitud de los primos y ya no sólo desde la visión euclidiana, también lo hacemos para algunos casos particulares de progresiones que contienen entre sus términos una infinidad de primos. Podemos clasificar a los primos de acuerdo con el residuo que dejan cuando son divididos por un entero n. Es en este contexto que considaremos a los primos de la forma $p = h + nk$, y con base en esto, definimos una progresión aritmética como una sucesión de la forma $\{h + nk\}_{n\in\mathbb{N}}$, que simplemente denotaremos como $\{h + nk\}$.

En esta dirección generalmente nos surge el cuestionamiento de ¿cómo abordamos la infinidad de primos de manera general en la progresión aritmética $\{h + kn\}$ (donde h y k son primos relativos)?

Este trabajo de tesis se centrará en el estudio de las progresiones señaladas. Por un lado, se presenta la manera como se puede afrontar la demostración de la infinitud de los primos en estas progresiones. Por otra parte, nos interesa conoces algunas características de la representación como suma de potencias de los primos en sus diferentes clases residuales.

La tesis está presentada en tres capítulos, como se menciona enseguida.

En el **capítulo 1** se definen los conceptos necesarios, tanto algebraicos como del análisis complejo, para abordar el teorema de Dirichlet, el cual establece que: dada una progresión aritmética $\{h+nk\}$, en ella existen una infinidad de primos siempre que $(h, k) = 1$. La prueba que aquí presentamos está basada en la de Harold N. Shapiro publicada en 1950. En la última sección de este capítulo presentamos un bosquejo de las pruebas originales del teorema de Dirichlet.

El **capítulo 2** está dedicado al estudio de las progresiones con un enfoque totalmente aditivo. Partimos del teorema de Waring que enuncia que todo entero es una suma de k-ésimas potencias, y en particular abordaremos los

casos de cuadrados y cubos que son de utilidad para estudiar la imagen de las progresiones aritméticas de Dirichlet en $\mathbb{Z}_4$ y $\mathbb{Z}_6$ bajo la función "cantidad de representaciones" como suma de cuatro cuadrados y nueve cubos respectivamente.

Finalmente, el **capítulo 3** consta de tres apéndices dedicados a un estudio más profundo de la anatomía de la gráfica de la función "cantidad de representaciones" como suma de cuatro cuadrados, nueve cubos, y el caso general para $k-$ésimas potencias. Particularmente estudiamos en que casos existe una infinidad de enteros con una única representación como suma de estas potencias.

Capítulo 1

El teorema de Dirichlet

A partir de una clasificación de los enteros con base en $\mathbb{Z}_k$ sabemos que los primos se encuentran en las clases de equivalencia que contienen enteros impares. Así, podemos identificar de manera natural en $\mathbb{Z}_2$ que los primos están en la clase de los enteros de la forma $2k+1$, y como los primos son de cardinalidad infinita, entonces la progresión $\{2k+1\}$ contiene una infinidad de primos. El primer caso fue inmediato.

Veamos qué sucede con $\mathbb{Z}_3$. Sabemos que las clases que contienen a los primos son $3k+1$ y $3k+2$, pero éstas tienen la característica de que no contienen sólo números impares y por simple auscultación podemos constatar que ambas contienen primos. Entonces ¿Cómo saber que ambas progresiones contienen una infinidad de primos? Pensemos de manera euclidiana y veamos a qué conclusiones podemos llegar.

Supongamos que sólo tenemos una cantidad finita de los primos de la forma $3k+2$, que son: $q_1, q_2, q_3, \ldots, q_r$. Ahora consideremos el número siguiente, $N = 3(q_1 q_2 q_3 \cdots q_r) + 2$, si éste es primo entonces no puede ser uno de los conocidos, por lo tanto hay uno más. Si es compuesto, entonces tiene un factor primo, pero éste puede ser de la forma $3k+1$ ó $3k+2$, pero sucede que para generar a N como producto de primos, necesitamos entre sus factores a un primo de la forma $3k+2$, porque de no existir, entonces no es posible generar a N sólo con primos de la forma $3k+1$. Por lo tanto requerimos por lo menos un primo de la forma $3k+2$, que tiene que ser distinto de cualquiera de los q_i, por lo tanto existe uno más de los conocidos. Así, bajo este proceso podemos concluir que hay una infinidad de primos de esta clase.

De la misma forma, supongamos que tenemos una cantidad finita de los primos de la forma $3k+1$, que son: $p_1, p_2, p_3, \ldots, p_t$. Ahora construimos el número, $N = 3(p_1 p_2 q_3 \cdots q_t) + 1$, si éste es primo entonces no puede ser uno de los conocidos, por lo tanto hay uno más. Si es compuesto, entonces tiene un factor primo, y este puede ser de la forma $3k+1$ ó $3k+2$, pero en este caso sí es posible formar al entero N sólo con primos de la forma $3k+2$. Por lo tanto nada nos garantiza que se tenga en la factorización de N un primo de la forma $3k+1$. Entonces, para este caso y con esta metodología, no podemos llegar a la conclusión de la infinitud de primos de la forma $3k+1$.

Veamos un caso más, para $\mathbb{Z}_4$. Las clases que contienen a los primos son $4k+1$ y $4k+3$, la segunda, equivalente a la clase $4k-1$. Como en $\mathbb{Z}_3$ veamos los casos.

Primero analicemos la infinidad de primos de la forma $4k-1$. Supongamos que existe una cantidad finita de primos $p_1, p_2, \ldots, p_n$ de la forma $4k-1$. Sea $N = 4p_1 p_2 \cdots p_n - 1$ y tenemos dos casos para analizar

Caso 1: Que N sea primo. Como N tiene la forma $4k-1$ y además $N > p_i$ $\forall i \in \{1, 2, \cdots, n\}$ entonces tendríamos una contradicción, pues z sería un número primo de la forma $4k-1$ y distinto a los antes mencionados. Por lo tanto existe uno más.

Caso 2: Que N sea compuesto. Por el teorema fundamental de la aritmética se puede descomponer como producto de primos. Si todos estos primos son de la forma $4m+1$, entonces el producto de números de esta forma tiene esta misma, así N sería de la forma $4k+1$, lo cual es absurdo. Dicho de otra manera, alguno de los divisores primos de N es de la forma $4k-1$, digamos que p_j es dicho primo, entonces $p_j \mid N$ y como $p_j \mid 4p_1 p_2 \cdots p_n$ entonces $p_j \mid (N - 4p_1 p_2 \cdots p_n) = -1$, lo cual es una contradicción. Por lo tanto existe otro primo de la forma $4k-1$ y así podemos concluir que hay una infinidad de primos de la forma $4k-1$.

Ya sabemos que, por lo menos, una de las dos progresiones contiene una infinidad de primos, ¿pero qué sucede con la otra progresión? para dar respuesta a esta interrogante analicemos los primos de la forma $4k+1$.

Supongamos que existe una cantidad finita de primos en la progresión aritmética $4k+1$, y retomemos la idea de la demostración anterior. Consideremos que

$$p_1 = 4k_1 + 1, p_2 = 4k_2 + 1, \ldots, p_n = 4k_n + 1$$

son todos los primos de la forma $4k + 1$. Ahora, sea $M = 4(p_1 \cdot p_2 \cdots p_n) + 1$ y tenemos nuevamente los dos casos.

Caso 1:
Si M es primo y como $M > p_k$ para toda k, entonces M es un primo de la forma $4k + 1$, pero diferente de todas las p_k y por lo tanto existe uno más.

Caso 2:
Si M es compuesto entonces el razonamiento aplicado en la prueba anterior no funciona, pues si M está formado por una cantidad par de factores primos de la forma $4k-1$, no obtendríamos un nuevo factor primo de la forma $4k+1$.

De acuerdo con lo anterior podríamos pensar que la única progresión aritmética que tiene una infinidad de primos es la de la forma $4k - 1$, sin embargo en un artículo de 1795 Euler demostró que hay una infinidad de primos de la forma $4k + 1$ utilizando las series que tanto le apasionaron. Veamos la demostración.

Euler consideró la serie

$$\frac{1}{3} - \frac{1}{5} + \frac{1}{7} + \frac{1}{11} - \frac{1}{13} - \frac{1}{17} + \frac{1}{19} + \frac{1}{23} - \frac{1}{29} + \cdots,$$

donde los recíprocos de los primos de la forma $4k + 1$ vienen precedidos por un signo negativo y para los primos de la forma $4k - 1$ por un signo positivo. Acto seguido Euler presenta una aproximación de esta serie[1] que es 0.3349816, y con estos elementos construye la demostración de la infinidad

[1] La aproximación que presenta Euler posiblemente es generada a partir de un resultado de Leibniz sobre series alternantes convergentes.
Entonces la serie

$$\frac{1}{3} - \frac{1}{5} + \frac{1}{7} + \frac{1}{11} - \frac{1}{13} - \frac{1}{17} + \frac{1}{19} + \frac{1}{23} - \frac{1}{29} + \cdots$$

se puede relacionar con el teorema de Leibniz que enuncia esto:
"Dada una sucesión decreciente $a_n > 0$ y si a_n tiende a cero cuando $n \longrightarrow \infty$, entonces la

de primos de la forma $4k+1$. Lo hace así:

Sean S y T tales que

$$S = \frac{1}{5} + \frac{1}{13} + \frac{1}{17} + \frac{1}{29} + \frac{1}{37} + \cdots \quad y \quad T = \frac{1}{3} + \frac{1}{7} + \frac{1}{11} + \frac{1}{19} + \frac{1}{23} + \frac{1}{31} + \cdots,$$

y como $T = S + (T - S)$, por lo tanto

$$T = S + \left(\frac{1}{3} - \frac{1}{5} + \frac{1}{7} + \frac{1}{11} - \frac{1}{13} - \frac{1}{17} + \frac{1}{19} + \cdots \right) \approx S + 0.3349816.$$

Al retomar la serie de los recíprocos de los primos se tiene que

$$\sum_{p \ primo} \frac{1}{p} = \frac{1}{2} + T + S \approx \frac{1}{2} + 2S + 0.3349816,$$

y como la suma de la izquierda es divergente, entonces

$$S = \frac{1}{5} + \frac{1}{13} + \frac{1}{17} + \frac{1}{29} + \frac{1}{37} + \cdots$$

debe ser divergente, lo cual sucederá sólo si existe una infinidad de primos de la forma $4k+1$.

Ahora surge de manera natural la siguiente pregunta:
¿Qué deben cumplir las progresiones $\{h + nk\}$ para que contengan una infinidad de primos?

Supongamos que la progresión $\{h + nk\}$ contiene un primo p, es decir $p = h + n_0 k$ si h y k tienen un divisor en común $d > 1$, tenemos que

$$p = h + n_0 k = d(h_1 + n_0 k_1),$$

---

serie

$$\sum_{n=1}^{\infty} (-1)^{n+1} a_n$$

converge"
Con este teorema Euler ya sabría que su serie converge, entonces su aproximación 0.3349816 ya no tiene problema si ésta es imprecisa.
Para ver la demostración con las características de Leibniz se puede consultar el libro de Ferraro [2008].

es decir, p es divisible por d. De esta manera tenemos que $(h,k) = 1$ es una condición necesaria para que existan primos en la progresión aritmética $\{h + kn\}$.

Gauss conjeturó que si $(h,k) = 1$ entonces existe una infinidad de primos en la progresión aritmética $\{h + kn\}$, en notación moderna, si $(h,k) = 1$ entonces existe una infinidad de primos p tal que $p \equiv h \ (mod\ k)$. Aunque fue Dirichlet, en 1837, quien demostró por primera vez este hecho, que en la actualidad es conocido como el teorema de Dirichlet.

Lo que se expondrá en las secciones siguientes es la demostración del Teorema de Dirichlet, trataremos de exponer una demostración con las bases algebraicas requeridas y que generalmente no se exponen en los libros conocidos.

1.1. Plan de la demostración

Ya abordamos los antecedentes que dieron lugar a plantear la interrogante de los primos que se encuentran en las progresiones aritméticas. A continuación construiremos el marco teórico necesario, para que sea posible demostrar el teorema de los primos en las progresiones aritméticas de Dirichlet.

A partir de este punto es evidente que las técnicas empleadas para conocer la infinidad de números primos contenidos en progresiones aritméticas son muy distintas. Tratar de generalizar esto utilizando solamente resultados elementales de la teoría de números resultaría muy complicado, por eso nos vemos en la necesidad de desarrollar una teoría más rica con el propósito de generalizar los resultados antes mencionados.

Para terminar esta sección presentamos la ruta de la demostración del teorema de Dirichlet, lo hacemos porque en la siguiente sección se desarrolla todo el proceso de la demostración, que es muy extenso.

Definición 1.1 (notacion de Landau)**.** *Dadas dos funciones f, g decimos que f es de orden g, y lo denotamos por $f = \mathcal{O}(g)$ o $f \ll g$. Si existen $M > 0$ y x_0 tal que para todo $x \geqslant x_0$ se cumple que*

$$|f(x)| \leqslant M|g(x)|.$$

Una manera de demostrar que existe una infinidad de primos es mostrando que la serie

$$\sum_{p \ primo} \frac{log\ p}{p}$$

diverge. Para ello se puede usar la siguiente fórmula asintótica

$$\sum_{p \leqslant x} \frac{log\ p}{p} = log\ x + \mathcal{O}(1). \tag{1.1}$$

Obtendremos el teorema de Dirichlet como consecuencia del siguiente lema, que es el análogo a (1.1), pero restringido a todos los primos de la forma $h + kn$ donde $(h, k) = 1$.

Lema 2.9 Si $k > 0$ y $(h, k) = 1$, entonces para toda $x > 1$

$$\sum_{\substack{p \leqslant x \\ p \equiv h (mod\ k)}} \frac{log\ p}{p} = \frac{1}{\varphi(k)} log\ x + \mathcal{O}(1). \tag{1.2}$$

Donde $\varphi(k) = \Big|\{n \in \mathbb{N} \ : n < k \ y \ (n, k) = 1\}\Big|$, conocida como la función indicatriz de Euler. Notemos que (1.2) implica que $\displaystyle\sum_{\substack{p \leqslant x \\ p \equiv h (mod\ k)}} \frac{log\ p}{p}$ diverge y así existe una infinidad de primos p de la forma $h + nk$.

Para demostrar (1.2) es necesario introducir los llamados caracteres de Dirichlet *mod* k, los cuales designaremos por

$$\chi_1, \chi_2, \ldots, \chi_{\varphi(k)}.$$

La prueba de (1.2) es consecuencia del siguiente lema en el que dichos caracteres juegan un papel importante.

Lema 2.8 Para $x > 1$ tenemos que:

$$\sum_{\substack{p \leqslant x \\ p \equiv h (mod\ k)}} \frac{log\ p}{p} = \frac{1}{\varphi(k)} log\ x \ + \ \frac{1}{\varphi(k)} \sum_{r=2}^{\varphi(k)} \overline{\chi}_r(h) \sum_{p \leqslant x} \frac{\chi_r(p) log\ p}{p} + \mathcal{O}(1)$$

Como el término $\frac{1}{\varphi(k)}\sum_{r=2}^{\varphi(k)}\overline{\chi}_r(h) = \mathcal{O}(1)$, entonces es claro que el *lema* 2.8 implica el *lema* 2.9, si probamos lo siguiente.

Lema 2.7 Para $x > 1$ y $\chi_1 \neq \chi$ tenemos que

$$\sum_{p\leqslant x}\frac{\chi(p)log\ p}{p} = \mathcal{O}(1) \tag{1.3}$$

Para probar el lema anterior usaremos el siguiente lema que expresa la suma anterior como otra suma que se encuentra extendida a todos los naturales $n \leqslant x$.

Lema 2.6 Para cada $x > 1$ y $\chi \neq \chi_1$ tenemos

$$\sum_{p\leqslant x}\frac{\chi(p)log\ p}{p} = -\mathcal{L}'(\chi,1)\sum_{n\leqslant x}\frac{\mu(n)\chi(n)}{n}\ +\ \mathcal{O}(1)$$

donde $\mathcal{L}'(\chi,1) = -\sum_{n=1}^{\infty}\frac{\chi(n)log\ n}{n}$, la convergencia de esta serie será estudiada con detalle.

Es claro que el *lema* 2.6 implica el *lema* 2.7 si demostramos lo siguiente

Lema 2.5 Para $x > 1$ y $\chi \neq \chi_1$

$$\sum_{n\leqslant x}\frac{\mu(n)\chi(n)}{n} = \mathcal{O}(1) \tag{1.4}$$

Esta igualdad se deduce del siguiente lema y del hecho que $\mathcal{L}(\chi,1) \neq 0$, donde
$\mathcal{L}(\chi,1) = \sum_{n=1}^{\infty}\frac{\chi(n)}{n}$ (la convergencia de esta serie se estudiará con detalle).

Lema 2.4 Para $x > 1$ y $\chi \neq \chi_1$ tenemos que

$$\mathcal{L}(\chi,1)\sum_{n\leqslant x}\frac{\mu(n)\chi(n)}{n} = \mathcal{O}(1) \tag{1.5}$$

Así, como $\mathcal{L}(\chi, 1) \neq 0$ podemos eliminar $\mathcal{L}(\chi, 1)$ en (1.5) para obtener (1.4).

Para probar que $\mathcal{L}(\chi, 1) \neq 0$, usaremos la descomposición como producto de Euler de dicha serie.

Dicha descomposición establece que bajo ciertas condiciones (que los caracteres de Dirichlet satisfacen) se tiene que $\forall s \in \mathbb{C}$ tal que $Re(s) > 1$

$$\sum_{n=1}^{\infty} \frac{\mathcal{F}(n)}{n^s} = \prod_{p \ primo} \frac{1}{1 - \mathcal{F}(p)p^{-s}}.$$

1.2. Demostración del teorema de Dirichlet

En este punto tenemos trazada la ruta a seguir para demostrar el teorema de Dirichlet. Iniciamos introduciendo un poco de teoría de grupos necesaria para poder desarrollar los conceptos necesarios que involucran caracteres de Dirichlet.

Se puede plantear que la teoría de grupos es joven, ésta tiene su origen en los trabajos de Galois que corresponden a encontrar soluciones por radicales de la ecuación $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$. Cabe señalar que el concepto de grupo que empleó Galois en su trabajo es el que ahora conocemos como grupo de permutaciones de n elementos.

Definición 1.2. *Un grupo es una pareja $(G, *)$, donde G es un conjunto no vacío y $* : G \times G \longrightarrow G$ es una operación binaria*
que satisface lo siguiente:

a) $*$ es asociativa, es decir

$$a * (b * c) = (a * b) * c \ \forall a, b, c \in G$$

b) Existe un elemento e en G, llamado neutro que satisface

$$a * e = e * a = a \ \forall a \in G$$

c) Para cada $a \in G$ existe un elemento a' en G tal que

$$a' * a = a * a' = e$$

Ejemplo 1.1. *Si $G = GL(n, \mathbb{C})$ las matrices de $n \times n$ con entradas en los complejos cuyo determinante es distinto de cero y $*$ denota el producto usual de matrices entonces $(G, *)$ es un grupo.*

Note que no todos los grupos son conmutativos, por ejemplo, dado que el producto de matrices no conmuta el *Ejemplo* 1.1 muestra un grupo que no es conmutativo. Cuando $*$ es una operación conmutativa, decimos que el grupo es conmutativo o abeliano.

Definición 1.3. *Sea $f : \mathbb{Z} \longrightarrow \mathbb{C}$, decimos que f es multiplicativa si para cada $a, b \in \mathbb{Z}$ tales que $(a, b) = 1$ se tiene que $f(ab) = f(a)f(b)$, si esto se cumple para cualquier entero, diremos que f es completamente multiplicativa.*

Ejemplo 1.2. *Denotemos con $\mathbb{M}$ al conjunto de funciones multiplicativas. Dadas dos funciones multiplicativas f y g, definimos la siguiente operación*

$$(f * g)(n) = \sum_{d|n} f(d)g\Big(\frac{n}{d}\Big)$$

la operación $*$ es conocida como producto o convolución de Dirichlet.

Teorema 1.1. *$(\mathbb{M}, *)$ es un grupo conmutativo*[2]

Demostración. Primero veamos que se cumple la conmutatividad, para esto necesitamos notar que

$$(f * g)(n) = \sum_{d|n} f(d)g\Big(\frac{n}{d}\Big) = \sum_{ab=n} f(a)g(b)$$

donde a y b recorren todos los números enteros positivos tales que su producto es n. De esta forma tenemos que $f * g = g * f$.

Veamos que se cumplen las propiedades restantes, sean f, g y h funciones multiplicativas y $(n, m) = 1$.

[2]Con la suma usual de funciones $(\mathbb{M}, +, *)$ es un anillo conmutativo.

1. Cerradura:
   Cada divisor d de mn puede ser expresado de la forma $d = ab$.
   Además, $(a, b) = 1$ y $(\frac{m}{a}, \frac{n}{b}) = 1$. Por lo tanto

$$\begin{aligned}(f * g)(nm) &= \sum_{d|nm} f(d)g\Big(\frac{nm}{d}\Big) \\ &= \sum_{ab|nm} f(ab)g\Big(\frac{nm}{ab}\Big) \\ &= \sum_{\substack{a|m \\ b|n}} f(a)f(b)g\Big(\frac{m}{a}\Big)g\Big(\frac{n}{b}\Big) \\ &= \sum_{a|m} f(a)g\Big(\frac{m}{a}\Big) \sum_{b|n} f(b)g\Big(\frac{n}{b}\Big) \\ &= (f * g)(m)(f * g)(n)\end{aligned}$$

   Así, la convolución de funciones multiplicativas es también una función multiplicativa.

2. Neutro:
   Definimos la siguiente función

$$I(n) = \Big[\frac{1}{n}\Big] = \begin{cases} 1 & si \quad n = 1 \\ 0 & si \quad n > 1 \end{cases}$$

   entonces I es completamente multiplicativa y además

$$(f * I)(n) = \sum_{d|n} f(d)I\Big(\frac{n}{d}\Big) = \sum_{d|n} f(d)\Big[\frac{n}{d}\Big] = f(n).$$

3. Inversos:
   Si f es una función aritmética no nula[3] entonces existe una única función aritmética f^{-1}, que se conoce como inverso de Dirichlet tal que

$$f * f^{-1} = f^{-1} * f = I,$$

[3]Se sigue que $f(1) \neq 0$, pues si $f(1) = 0$, entones para cada $n \in \mathbb{N}$ se tendría que $f(n) = f(1 \cdot n) = f(1)f(n) = 0$. Y así $f \equiv 0$, lo cual es absurdo.

además, f^{-1} se obtiene por medio de la siguiente relación de recurrencia

$$f^{-1}(1) = \frac{1}{f(1)},\ f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\Big(\frac{n}{d}\Big) f^{-1}(d) \ para\ n > 1$$

Veamos por inducción fuerte que la ecuación $(f * f^{-1})(n) = I(n)$ tiene una única solución para $f(n)$.

Si $n = 1$ entonces $f(1)f^{-1}(1) = (f * f^{-1})(1) = I(1) = 1$ y como $f(1) \neq 0$ entonces $f^{-1}(1) = \dfrac{1}{f(1)}$, como se quería.

Supongamos que la ecuación es valida para toda $k < n$, entonces queremos resolver la ecuación $(f * f^{-1})(n) = I(n)$ para $n > 1$, o dicho de otra forma

$$\begin{aligned} 0 = \Big[\tfrac{1}{n}\Big] &= \sum_{d|n} f\Big(\frac{n}{d}\Big) f^{-1}(d) \\ &= f(1)f^{-1}(n) + \sum_{\substack{d|n \\ d<n}} f\Big(\frac{n}{d}\Big) f^{-1}(d) \end{aligned}$$

así despejando $f^{-1}(n)$ de la última expresión tenemos que

$$f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\Big(\frac{n}{d}\Big) f^{-1}(d).$$

4. Asociatividad:
   Sea $\psi = g * h$. entonces

$$\begin{aligned} (f * (\psi))(n) &= \sum_{ad=n} f(a)\psi(d) \\ &= \sum_{ad=n} f(a) \sum_{bc=d} g(b)h(c) = \sum_{abc=n} f(a)g(b)h(c). \end{aligned}$$

Por otro lado si $\varphi = f * g$, entonces tenemos que

$$\begin{aligned}((\varphi) * h)(n) &= \sum_{dc=n} \varphi(d)h(c) \\ &= \sum_{dc=n} \sum_{ab=d} f(a)g(b)h(c) = \sum_{abc=n} f(a)g(b)h(c)\end{aligned}$$

lo que concluye la demostración.

□

Definición 1.4. *Si $(G, *)$ es un grupo, su orden es la cardinalidad del conjunto subyacente $|G|$.*

Definición 1.5. *Si $(G, *)$ es un grupo, un subgrupo de G es un subconjunto $H \subseteq G$ tal que la operación restringida a H es cerrada y H es un grupo con esa operación.*

Definición 1.6. *Si $(G, *)$ es un grupo, dado un elemento $g \in G$ definimos sus potencias enteras de esta manera:*

1. *Si k=0, se define $g^0 = e$.*
2. *Si $k \geqslant 1$, se definen las potencias enteras de g como sigue*

$$\begin{aligned} g^1 &= g \\ g^2 &= g * g \\ g^3 &= g^2 * g \\ &\vdots \\ g^{k+1} &= g^k * g. \end{aligned}$$

3. *Si $-k < 0$, entonces definimos*

$$g^{-k} = (g^{-1})^k.$$

Teorema 1.2. *Si $(G, *)$ es un grupo y g es un elemento cualquiera de G, entonces el conjunto*

$$(g) = \{g^n \ : \ n \in \mathbb{Z}\}$$

es un subgrupo conmutativo de G.

Demostración. Sean $a, b \in (g)$, entonces existen $r, s \in \mathbb{Z}$ tal que $a = g^r$ y $b = g^s$, note también que

$$a * b = g^r * g^s = g^{r+s}$$

con lo que $a*b$ es un elemento de (g), es decir (g) es cerrado bajo la operación. Además

$$a * b = g^r * g^s = g^{r+s} = g^{s+r} = g^s * g^r = b * a$$

lo cual muestra que la operación es conmutativa. Por otro lado, $g^0 = e$, de esta manera $e \in (g)$.

Finalmente notemos que si $g^m \in (g)$ entonces g^{-m} es un elemento de (g) que cumple $g^m * g^{-m} = g^{m-m} = g^0 = e$. □

El grupo (g) es conocido como el subgrupo cíclico generado por g. Por otro lado, si existe un elemento $a \in G$ tal que $G = (a)$, diremos que G es un grupo cíclico generado por a.

Definición 1.7. *Una función $\varphi : G_1 \longrightarrow G_2$ entre dos grupos $(G_1, *_1)$ y $(G_2, *_2)$ se dice que es un homomorfismo o morfismo de grupos si*

$$\varphi(g_1 *_1 g_2) = \varphi(g_1) *_2 \varphi(g_2), \ \forall g_1, g_2 \in G_1.$$

Ejemplo 1.3. *Consideremos los siguientes grupos multiplicativos $GL(2, \mathbb{R})$ y $\mathbb{R}\backslash\{0\}$, entonces la función $det : GL(2, \mathbb{R}) \longrightarrow \mathbb{R}\backslash\{0\}$, llamada determinante, es un morfismo entre estos grupos ya que*

$$det(A \cdot B) = det(A) \cdot det(B).$$

Teorema 1.3. *Sean G_1 y G_2 dos grupos con e_1 y e_2 sus respectivos neutros y $\varepsilon : G_1 \longrightarrow G_2$ un morfismo, entonces:*

$$\begin{aligned} i) \quad & \varepsilon(e_1) && = e_2 \\ ii) \quad & \varepsilon(a)^{-1} && = \varepsilon(a^{-1}) \\ iii) \quad & \varepsilon(a)^n && = \varepsilon(a^n). \ \forall n \in \mathbb{Z}. \end{aligned}$$

Demostración. Para la primera parte tenemos que

$$\varepsilon(e_1) = \varepsilon(e_1 e_1) = \varepsilon(e_1)\varepsilon(e_1)$$

entonces cancelando $\varepsilon(e_1) = e_2$.

Para la segunda parte sea $a \in G_1$ entonces

$$e_2 = \varepsilon(aa^{-1}) = \varepsilon(a)\varepsilon(a^{-1}),$$

y tendremos que

$$\varepsilon(a)^{-1} = \varepsilon(a)^{-1}e_2 = \varepsilon(a)^{-1}\varepsilon(a)\varepsilon(a^{-1}) = \varepsilon(a^{-1}).$$

La parte tres se deduce inmediatamente de uno, dos y de la definición de potencias enteras de un elemento. □

Definición 1.8. *Un morfismo es un epimorfismo si es suprayectivo; es un monomorfismo si es inyectivo y finalmente diremos que es un isomorfismo si es biyectivo.*

En este último caso decimos que G_1 es isomorfo a G_2 y lo denotamos por $G_1 \simeq G_2$

Definición 1.9. *Si $(H, *_1)$ y $(K, *_2)$ son dos grupos, entonces su producto cartesiano*

$$H \times K = \{(h, k) \ : \ h \in H, k \in K\}$$

es un grupo con la operación definida en cada entrada, es decir si (h, k) y (h', k') son elementos de $H \times K$, definimos

$$(h, k) * (h', k') = (h *_1 h', k *_2 k').$$

El neutro de $H \times K$ es el elemento (e_H, e_K), y el inverso de (h, k) es (h^{-1}, k^{-1}). El grupo $H \times K$ es conocido como el producto directo externo de los grupos H y K.

Teorema 1.4. *Todo grupo abeliano finito G se puede descomponer como producto directo de grupos cíclicos*

$$G \simeq C(m_1) \times C(m_2) \times \ldots \times C(m_s)$$

donde cada $C(m_j)$ es un grupo cíclico de orden m_j y cada $m_j \mid m_{j+1}$ para $j \in \{1, 2, \ldots, s-1\}$.

Demostración. La prueba de este resultado será omitida pero puede ser encontrada en cualquier texto clásico de teoría de grupos, por ejemplo en [Zaldivar 2006, p. 90] □

1.2.1. Caracteres de grupos abelianos finitos

Definición 1.10. *Sea G un grupo conmutativo finito de orden k y con elemento neutro e. Un carácter sobre G es una función $\chi : G \longrightarrow \mathbb{C}$ compleja no nula tal que $\chi(u)\chi(v) = \chi(uv)$, $\forall u, v \in G$.*

Teorema 1.5. *Si χ es carácter de un grupo finito G con elemento identidad e, entonces $\chi(e) = 1$ y cada valor de la función $\chi(a)$ es una raíz k-ésima de la unidad, de hecho si $a^k = 1$ entonces $\chi(a)^k = 1$.*

Demostración. Sea c en G tal que $\chi(c) \neq 0$. Como $ce = c$ tenemos que $\chi(c) = \chi(ce) = \chi(c)\chi(e)$ y dado que $\chi(c) \neq 0$, entonces $\chi(e) = 1$. Por otra parte si $a^n = 1$ entonces

$$\chi(a)^n = \chi(a^n) = \chi(e) = 1$$

□

Ejemplo 1.4. *Cada grupo G tiene al menos un carácter , que la función idénticamente 1, llamada el carácter principal, la cual denotaremos por χ_1. Así, tenemos que $\chi_1(g) = 1$ para toda $g \in G$.*

Teorema 1.6. *El conjunto de caracteres de un grupo abeliano G, $HOM(G, \mathbb{S}^1)$ donde $\mathbb{S}^1 = \{z \in \mathbb{C} : |z| = 1\}$ forman un grupo abeliano bajo la siguiente operación. Si χ_1, χ_2 son dos caracteres, definimos*

$$(\chi_1 * \chi_2)(g) = \chi_2(g)\chi_2(g).$$

Demostración. La operación es conmutativa pues el producto de números complejos conmuta. Dado $\chi \in HOM(G, \mathbb{S}^1)$ definimos $\overline{\chi} \in HOM(G, \mathbb{S}^1)$ por $\overline{\chi}(g) = \overline{\chi(g)}$ $\forall g \in G$, notemos que

$$(\chi\overline{\chi})(g) = \chi(g)\overline{\chi(g)} = |\chi(g)|^2 = 1,$$

$\forall \chi \in HOM(G, \mathbb{S}^1)$, es decir $\bar{\chi}$ es el inverso de χ. Finalmente tenemos que

$$(\chi_1\chi)(g) = \chi_1(g)\chi(g) = 1\chi(g) = \chi(g),$$

es decir, χ_1 es el neutro bajo la multiplicación. □

Dicho grupo se conoce como el grupo dual de G y se denota por $\widehat{G}$.

Teorema 1.7. *Sea G un grupo abeliano finito. Entonces, para toda $g \in G$, $g \neq e$ existe $\chi \in \widehat{G}$ tal que $\chi(g) \neq 1$.*

Demostración. Consideremos la descomposición del grupo G como producto directo de subgrupos cíclicos $G = G_1 \times G_2 \times \cdots \times G_s$ de órdenes $n_1, n_2, \ldots, n_s$ respectivamente. Sea $(a_i) = G_i$, ahora si $g \in G$, g se puede escribir como $g = ({a_1}^{b_1}, {a_2}^{b_2}, \ldots, {a_s}^{b_s})$ con $0 \leqslant b_i < n_i$, donde únicamente para el elemento unidad del grupo todos los b_i son nulos.

Por otro lado si $\chi \in G$ es un carácter de G entonces el valor $\chi(g)$ queda totalmente determinado por los valores de χ en los generadores de los G_i, es decir

$$\chi(g) = \chi(a_1)^{b_1}\chi(a_2)^{b_2} \ldots \chi(a_s)^{b_s}$$

si $g \neq e$ entonces existe un j tal que $b_j \neq 0$ y así podemos definir el siguiente carácter

$$\chi(a_m) = \begin{cases} 1 & si \quad m \neq j \\ exp\left(\frac{2\pi i}{n_j}\right) & si \quad m = j \end{cases}$$

que cumple que $\chi(g) = exp\left(\frac{2\pi i b_j}{n_j}\right) = cos\left(\frac{b_j}{n_j}2\pi\right) + isen\left(\frac{b_j}{n_j}2\pi\right)$ y como $0 < b_j < n_j$ tenemos que $0 < \frac{b_j}{n_j} < 1$. De esta manera $\chi(g) \neq 1$. □

1.2.2. Relaciones de ortogonalidad

Teorema 1.8. *Se cumplen los siguientes resultados.*

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & si \quad \chi = \chi_1 \\ 0 & si \quad \chi \neq \chi_1 \end{cases} \tag{1.6}$$

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |\widehat{G}| & si \quad g = e \\ 0 & si \quad g \neq e \end{cases} \tag{1.7}$$

Demostración. Si $\chi = \chi_1$ entonces $\sum_{g \in G} \chi(g) = \sum_{g \in G} \chi_1(g) = \sum_{g \in G} 1 = |G|$. Por otro lado, si $\chi \neq \chi_1$ y $y \in G$ es tal que $\chi(y) \neq 1$, entonces

$$\sum_{g\in G}\chi(g)=\sum_{g\in G}\chi(gy)=\Big[\sum_{g\in G}\chi(g)\Big]\chi(y),$$

de esta manera

$$0=(\chi(y)-1)\sum_{g\in G}\chi(g)$$

y como $\chi(y)\neq 1$ entonces $\sum_{g\in G}\chi(g)=0$, lo cual concluye la prueba de la parte (1.6).

Para la parte (1.7), si $g=e$ tenemos que

$$\sum_{\chi\in\widehat{G}}\chi(g)=\sum_{\chi\in\widehat{G}}\chi(e)=\sum_{\chi\in\widehat{G}}1=|\widehat{G}|$$

como se quería. Ahora si $g\neq e$ y por el Teorema 1.7 tenemos que existe un carácter χ' tal que $\chi'(g)\neq 1$, entonces

$$\chi'(g)\sum_{\chi\in\widehat{G}}\chi(g)=\sum_{\chi\in\widehat{G}}\chi'(g)\chi(g)=\sum_{\chi\in\widehat{G}}(\chi'\chi)(g)=\sum_{\chi\in\widehat{G}}\chi(g)$$

de aquí se obtiene que

$$(\chi'(g)-1)\sum_{\chi\in\widehat{G}}\chi(g)=0$$

y como $\chi'(g)\neq 1$ tenemos que $\sum_{\chi\in\widehat{G}}\chi(g)=0$, con lo cual concluye la demostración. □

Corolario 1.9. *En todo grupo conmutativo finito el número de caracteres es igual al orden del grupo.*[4]

[4]Más aún se cumple que $G\simeq\widehat{G}\simeq\widehat{\widehat{G}}$.

Demostración. Tenemos que

$$
\begin{aligned}
|G| &= \sum_{g\in G} \chi_1(g) && (\textit{por } (1.6) \textit{ dado que } \chi = \chi_1)\\
&= \sum_{g\in G} \chi_1(g) + \sum_{\substack{\chi\in\widehat{G}\\ \chi\neq\chi_1}} \sum_{g\in G} \chi(g) && (\textit{pues si } \chi \neq \chi_1 \textit{ tenemos que} \sum_{g\in G} \chi(g) = 0)\\
&= \sum_{\chi\in\widehat{G}} \sum_{g\in G} \chi(g)\\
&= \sum_{g\in G} \sum_{\chi\in\widehat{G}} \chi(g)\\
&= \sum_{\substack{g\in G\\ g\neq e}} \sum_{\chi\in\widehat{G}} \chi(g) + \sum_{\chi\in\widehat{G}} \chi(e) && (\textit{separando el sumando cuando } g = e)\\
&= \sum_{\chi\in\widehat{G}} \chi(e) && (\textit{pues } \sum_{\chi\in\widehat{G}} \chi(g) = 0 \textit{ dado que } g \neq e)\\
&= \sum_{\chi\in\widehat{G}} 1 = |\widehat{G}|
\end{aligned}
$$

así tenemos que $|G| = |\widehat{G}|$. □

De esta manera podemos reescribir el *Teorema* 1.8 de la siguiente manera

Teorema 1.10. *Sea G un grupo abeliano finito, entonces*

$$\sum_{g\in G} \chi(g) = \begin{cases} |G| & si \quad \chi = \chi_1 \\ 0 & si \quad \chi \neq \chi_1 \end{cases} \tag{1.8}$$

$$\sum_{\chi\in\widehat{G}} \chi(g) = \begin{cases} |G| & si \quad g = e \\ 0 & si \quad g \neq e \end{cases} \tag{1.9}$$

Demostración. Por el Corolario anterior tenemos que $|G| = |\widehat{G}|$, sustituyendo esto en (1.7) concluimos la demostración. □

De este teorema se desprenden los siguientes dos corolarios que resultan ser importantes

Corolario 1.11. ***(ortogonalidad por columnas)*** *Para cualquier par de caracteres χ y ψ se tiene que*

$$\frac{1}{|G|}\sum_{g\in G}\frac{\chi(g)}{\psi(g)}=\begin{cases}1 & si \quad \chi=\psi\\ 0 & si \quad \chi\neq\psi\end{cases} \tag{1.10}$$

Demostración. Tenemos que

$$\begin{aligned}\sum_{g\in G}\frac{\chi(g)}{\psi(g)}&=\sum_{g\in G}\chi(g)\psi^{-1}(g)\\ &=\sum_{g\in G}(\chi\psi^{-1})(g)=\begin{cases}|G| & si \quad \chi=\psi\\ 0 & si \quad \chi\neq\psi\end{cases} \quad \text{(por (1.8))}\end{aligned}$$

o equivalentemente al dividir entre $|G|$ tenemos que

$$\frac{1}{|G|}\sum_{g\in G}\frac{\chi(g)}{\psi(g)}=\begin{cases}1 & si \quad \chi=\psi\\ 0 & si \quad \chi\neq\psi\end{cases}$$

lo cual concluye la demostración. □

Corolario 1.12. ***(ortogonalidad por renglones)*** *Para todo $u\in G$ y $v\in G$ se cumple*

$$\frac{1}{|G|}\sum_{\chi\in\widehat{G}}\frac{\chi(u)}{\chi(v)}=\begin{cases}1 & si \quad u=v\\ 0 & si \quad u\neq v\end{cases} \tag{1.11}$$

Demostración. Tenemos que

$$\begin{aligned}\sum_{\chi\in\widehat{G}}\frac{\chi(u)}{\chi(v)}&=\sum_{\chi\in\widehat{G}}\chi(u)\chi^{-1}(v)=\sum_{\chi\in\widehat{G}}\chi(u)\chi(v^{-1})\\ &=\sum_{\chi\in\widehat{G}}\chi(uv^{-1})=\begin{cases}|G| & si \quad uv^{-1}=e\\ 0 & si \quad uv^{-1}\neq e\end{cases} \quad \text{(por (1.9))}\end{aligned}$$

o equivalentemente al dividir entre $|G|$ tenemos que

$$\frac{1}{|G|}\sum_{\chi\in\widehat{G}}\frac{\chi(u)}{\chi(v)}=\begin{cases}1 & si \quad u=v\\ 0 & si \quad u\neq v\end{cases}$$

como se quería demostrar. □

1.2.3. Caracteres de Dirichlet

Todos los resultados anteriores son válidos para grupos conmutativos finitos en general. Ahora nos enfocaremos a estudiar los caracteres asociados a un grupo en particular.

Definición 1.11. *Para cada entero a su correspondiente clase residual $[a]$ es el conjunto de todos los enteros congruentes con a módulo k*

$$[a] = \{x : x \equiv a \ (mod\ k)\}.$$

La multiplicación de clases residuales está definida por la relación

$$[a][b] = [ab]. \tag{1.12}$$

Veamos que este producto está bien definido, primero notemos que

$$[a] = \{x \in \mathbb{Z} \ : x = km + r \ m \in \mathbb{Z}\},$$

sean $a, b, a', b' \in \mathbb{Z}$ tal que $a \equiv a' \ (mod\ k)$ y $b \equiv b' \ (mod\ k)$, así tenemos que

$$ab = (q_1k + r)(q_2k + s) = (q_1q_2 + sq_1 + rq_2)k + rs$$

y

$$a'b' = (q_1'k + r)(q_2'k + s) = (q_1'q_2' + sq_1' + rq_2')k + rs$$

luego $ab \equiv rs \ (mod\ k)$ y $a'b' \equiv rs \ (mod\ k)$, y por transitividad se tiene que $ab \equiv a'b' \ (mod\ k)$, es decir $[ab] = [a'b']$.

Lema 1.1. *m es invertible módulo k sí y solo sí $(m, k) = 1$.*

Demostración. Supongamos que m es invertible $(mod\ k)$ y d es un divisor común de m y k. Entonces $m = da$ y $k = db$ para algunos enteros a y b, donde $1 \leqslant b \leqslant k$. Ahora $mb = dab = ka \equiv 0 \ (mod\ k)$, luego como m es invertible, obtenemos que $b \equiv 0 \ (mod\ k)$, pero como $1 \leqslant b \leqslant k$, esto paso solamente si $b = k$, así que $d = 1$.

Para el regreso, supongamos que k y m no tienen un divisor común mayor que 1, y consideremos los $m - 1$ números

$$m, 2m, 3m, \ldots, (k-1)m.$$

Veamos que alguno de estos números es congruente a 1 $(mod\ k)$. Para esto, es suficiente ver que estos $k-1$ números representan $k-1$ clases de congruencias distintas. Es decir, si dos de estos números son congruentes entre sí, digamos $ma \equiv mb\ (mod\ k)$, $1 \leqslant a < b \leqslant k-1$ tenemos que k divide a la diferencia, es decir $k \mid m(b-a)$ luego como k no tiene factor común con m, $k \mid (b-a)$, pero esto es imposible porque $1 \leqslant b-a \leqslant k-1$. □

Teorema 1.13. *Con la multiplicación definida en* (1.12) *el conjunto de clases residuales módulo k es un grupo abeliano de orden $\varphi(k)$ el cual denotaremos por $\mathbb{Z}_k^*$.*

Demostración. Primero notemos que claramente el producto de clases conmuta, la propiedad de ser cerrado se cumple automáticamente por la manera como está definido el producto de las clases. Por otro lado notemos que [1] funciona como neutro, pues

$$[a][1] = [a1] = [a].$$

Ahora sean $[a], [b], [c] \in \mathbb{Z}_k^*$ entonces

$$[a]([b][c]) = [a]([bc]) = [abc] = ([ab])[c],$$

y así se cumple la asociatividad. Finalmente sabemos que un elemento a es invertible módulo k si y sólo si $(a,k) = 1$, lo cual implica que $|\mathbb{Z}_k^*| = \varphi(k)$. □

Definición 1.12. *Consideremos los caracteres $\{\psi_1, \psi_2, \ldots, \psi_{\varphi(k)}\}$ asociados a este grupo los cuales usaremos para obtener funciones extendidas que toman valores en todo $\mathbb{Z}$ de la siguiente manera*

$$\chi_i(n) = \begin{cases} \psi_i([n]) & si \quad (n,k) = 1 \\ 0 & si \quad (n,k) > 1 \end{cases}$$

Las funciones χ_i son conocidas como los caracteres de Dirichlet módulo k. Como el número de caracteres de un grupo es igual a su orden y el orden de $|\mathbb{Z}_k^*| = \varphi(k)$ entonces existen $\varphi(k)$ caracteres de este tipo, de los cuales denominaremos carácter principal de Dirichlet a la función

$$\chi_1(n) = \begin{cases} 1 & si \quad (n,k) = 1 \\ 0 & si \quad (n,k) > 1 \end{cases}$$

Teorema 1.14. *De las propiedades demostradas para los caracteres de un grupo se deducen inmediatamente las siguientes propiedades para el grupo* $\mathbb{Z}_k^*$.

$$\sum_{[q]\in\mathbb{Z}_k^*} \chi([q]) = \begin{cases} \varphi(k) & si \quad \chi = \chi_1 \\ 0 & si \quad \chi \neq \chi_1 \end{cases} \tag{1.13}$$

$$\sum_{i=1}^{\varphi(k)} \chi_i(u) = \begin{cases} \varphi(k) & si \quad u \equiv 1 \ (mod\ k) \\ 0 & si \quad u \not\equiv 1 (mod\ k) \end{cases} \tag{1.14}$$

$$\sum_{i=1}^{\varphi(k)} \frac{\chi_i(u)}{\chi_i(a)} = \begin{cases} \varphi(k) & si \quad u \equiv a \ (mod\ k) \\ 0 & si \quad u \not\equiv a (mod\ k) \end{cases} \qquad siempre\ que\ (a,k) = 1 \tag{1.15}$$

Demostración. La prueba es inmediata dado que el orden de $\mathbb{Z}_k^* = \varphi(k)$ $\square$

Teorema 1.15. *Hay* $\varphi(k)$ *caracteres de Dirichlet módulo* k, *cada uno es completamente multiplicativo y periódico (de periodo* k*), es decir se tiene lo siguiente*

$$\chi(ab) = \chi(a)\chi(b) \qquad \forall a, b \in \mathbb{Z} \tag{1.16}$$

$$\chi(a+k) = \chi(a) \qquad \forall a \in \mathbb{Z}. \tag{1.17}$$

Demostración. La primera parte es clara, para probar que son completamente multiplicativos necesitamos los siguientes resultados básicos sobre el máximo común divisor

$$\begin{array}{llllll} i) & si & (ab,k) > 1 & entonces & (a,k) > 1 \quad o & (b,k) > 1 \\ ii) & si & (ab,k) = 1 & entonces & (a,k) = 1 \quad y & (b,k) = 1. \end{array}$$

Regresando a la prueba del teorema primero veamos que se cumple (1.16). Sean

$$\{\psi_1, \psi_2, \ldots, \psi_{\varphi(k)}\}$$

los caracteres asociados al grupo $\mathbb{Z}_k^*$ y $\{\chi_1, \chi_2, \ldots, \chi_{\varphi(k)}\}$ sus respectivos caracteres de Dirichlet. Así, tenemos los siguientes dos casos para $i \in \{1, 2, \ldots, \varphi(k)\}$ fijo

Caso 1: si $(ab,k)=1$ entonces

$$\begin{aligned}\chi_i(ab) &= \psi_i(ab) \quad \text{(pues (ab,k)=1)} \\ &= \psi_i(a)\psi_i(b) \quad \text{(dado que } \psi_i \text{ es un carácter)} \\ &= \chi_i(a)\chi_i(b) \quad \text{(por } i\text{) tenemos que } (a,k)=1 \text{ y } (b,k)=1).\end{aligned}$$

Caso 2: si $(ab,k)>1$ por $ii)$ podemos suponer sin perdida de generalidad que $(a,k)>1$, así

$$\chi_i(ab)=0=0\chi_i(b)=\chi_i(a)\chi_i(b) \quad \text{(la última igualdad se da pues } (a,k)>1).$$

Finalmente veamos que son funciones periódicas de periodo k, para esto necesitaremos el siguiente resultado

$$iii) \text{ Si } a\equiv b \ (mod\ k), \text{ entonces } (a,k)=(b,k)$$

Ahora sea $a\in\mathbb{Z}$, entonces como $a+k\equiv a\ (mod\ k)$ y por $iii)$ tenemos que $(a+k,k)=(a,k)$. De esta forma tenemos lo siguiente

$$\begin{aligned}\chi_i(a+k) &= \begin{cases}\psi_i([a+k]) & si \quad (a+k,k)=1 \\ 0 & si \quad (a+k,k)>1\end{cases} \\ &= \begin{cases}\psi_i([a]) & si \quad (a,k)=1 \\ 0 & si \quad (a,k)>1\end{cases} \quad \text{(pues } a+k\equiv a\ (mod\ k)) \\ &= \chi_i(a).\end{aligned}$$

□

Recíprocamente tenemos el siguiente resultado

Teorema 1.16. *Si f es multiplicativa, $f(q)=0$ siempre que $(k,q)>1$ y f es de periodo k, entonces f es un carácter de Dirichlet módulo k.*

Demostración. Es suficiente mostrar que f es completamente multiplicativa, si $(ab,k)>1$ supongamos sin pérdida de generalidad que $(a,k)>1$, entonces

$$f(ab)=0=0\cdot f(b)=f(a)f(b).$$

Ahora supongamos que $(ab,k)=1$ en particular tenemos que $(a,k)=1$. Consideremos ahora el siguiente mapeo $n\longmapsto b+nk\ (mod\ a)$, dicho mapeo

permuta las clases residuales módulo a, así hay un n_0 para el cual $b + n_0 k \equiv 1 \ (mod\ a)$ de esta manera tenemos que $(b + n_0 k, a) = (1, a) = 1$, entonces

$$\begin{aligned} f(ab) &= f(a(b + n_0 k)) && (por\ periodicidad) \\ &= f(a)f(b + n_0 k) && (por\ ser\ multiplicativa) \\ &= f(a)f(b) && (por\ periodicidad) \end{aligned}$$

□

1.2.4. Tablas de caracteres

En esta sección nos interesa mostrar explícitamente la regla de correspondencia de los caracteres asociados al grupo $\mathbb{Z}_k^*$, particularmente para los casos $k = 1, 2, 3, 4, 5$. Además de ilustrar las relaciones (1.10) y (1.11).

1. $k = 1\ o\ k = 2,\ \varphi(k) = 1$

   En ambos casos el único carácter es el carácter principal χ_1 y no hay nada que hacer.

2. $k = 3,\ \varphi(k) = 2$

   Por definición $\chi_1(1) = \chi_1(2) = 1$ y $\chi_1(3) = 0$, además

   $$1 = \chi_2(2)^{\varphi(3)} = \chi_2(2)^2$$

   Así, $\chi_2(2) = 1$ o $\chi_2(2) = -1$, pero $\chi_2 \neq \chi_1$ lo cual implica que $\chi_2(2) = -1$ y así podemos completar la tabla de caracteres módulo 3 (ver *Figura* 1.1).

n	1	2	3
$\chi_1(n)$	1	1	0
$\chi_2(n)$	1	-1	0

Figura 1.1: Tabla de caracteres módulo 3

3. $k = 4$, $\varphi(k) = 2$

   Entonces $\chi_1(1) = \chi_1(3) = 1$ y $\chi_1(2) = \chi_1(4) = 0$, por otra parte $\chi_2(1) = 1$ y $\chi_2(2) = \chi_2(4) = 0$, sólo nos resta determinar el valor $\chi_2(3)$, para esto sabemos que

$$1 = \chi_2(3)^{\varphi(4)} = \chi_2(3)^2$$

   Así, $\chi_2(3) = 1$ o $\chi_2(3) = -1$, pero $\chi_2 \neq \chi_1$ lo cual implica que $\chi_2(3) = -1$ que es el último dato requerido para completar la tabla de caracteres módulo 4 (ver *Figura* 1.2).

n	1	2	3	4
$\chi_1(n)$	1	0	1	0
$\chi_2(n)$	1	0	-1	0

Figura 1.2: Tabla de caracteres módulo 4

4. $k = 5$, $\varphi(k) = 4$

   En este caso $\chi_1(r) = 1$ para $1 \leq r \leq 4$ y $\chi_i(5) = 0$, al igual que los casos anteriores tenemos que

$$1 = \chi_i(2)^{\varphi(5)} = \chi_i(2)^4.$$

   De esta manera tenemos que $\chi_i(2) \in \{1, -1, i, -i\}$, como $\chi_1(2) = 1$, hagamos $\chi_2(2) = -1, \chi_3(2) = i, \chi_4(2) = -i$, por otro lado $\chi_i(4) = \chi_i(2^2) = \chi_i(2)^2$, entonces

$$\begin{aligned} \chi_2(4) &= \chi_2(2)^2 = (-1)^2 = 1 \\ \chi_3(4) &= \chi_3(2)^2 = i^2 = -1 \\ \chi_4(4) &= \chi_4(2)^2 = (-i)^2 = -1. \end{aligned}$$

   Finalmente tenemos que

$$\chi_i(2)\chi_i(3) = \chi_i(6) = \chi_i(1) = 1,$$

es decir $\chi_i(3) = \chi_i(2)^{-1}$, con esto tenemos que $\chi_2(3) = -1$, $\chi_3(3) = -1$, $\chi_4(3) = -1$ y así la tabla de caracteres módulo 5 es la siguiente (ver *Figura* 1.3).

n	1	2	3	4	5
$\chi_1(n)$	1	1	1	1	0
$\chi_2(n)$	1	-1	-1	1	0
$\chi_3(n)$	1	i	-i	-1	0
$\chi_4(n)$	1	-i	i	-1	0

Figura 1.3: Tabla de caracteres módulo 5

Enfocándonos en esta última tabla, si consideramos las columnas de dicha tabla como vectores en $\mathbb{C}^4$, y considerando como producto interno (1.10), tenemos que bajo este producto interno dichos vectores forman una base ortonormal; de manera análoga si consideramos las columnas de dicha tabla como vectores en $\mathbb{C}^4$, y según (1.11) como producto interno, dichos vectores son nuevamente una base ortonormal.[5]

1.2.5. Productos de Euler

Teorema 1.17 (Euler). *Si $s \in \mathbb{C}$ y además $Re(s) > 1$, entonces*

$$\zeta(s) = \prod_{p \ primo} \frac{1}{1 - p^{-s}}$$

donde $\zeta(s)$ es la función zeta de Riemann.

Demostración. Sea $f(z) = \dfrac{1}{1-z}$, sabemos por el teorema de Taylor que $f(z) = \displaystyle\sum_{n=0}^{\infty} z^n$ para toda $z \in \mathbb{C}$ tal que $Re(s) > 1$. En particular para cada primo p y $s > 1$ tenemos que

$$\frac{1}{1 - p^{-s}} = 1 + p^{-s} + p^{-2s} + p^{-3s} + \cdots \tag{1.18}$$

[5]Esta interpretación de las tablas de caracteres le da el nombre a (1.10) y (1.11).

Si $\{p_1, p_2, p_3, \ldots, p_r\}$ son los primeros r números primos, entonces por (1.18) tenemos que:

$$\begin{aligned}
\frac{1}{1-p_2^{-s}} &= 1 + p_2^{-s} + p_2^{-2s} + p_2^{-3s} + \cdots \\
\frac{1}{1-p_3^{-s}} &= 1 + p_3^{-s} + p_3^{-2s} + p_3^{-3s} + \cdots \\
&\vdots \\
\frac{1}{1-p_r^{-s}} &= 1 + p_r^{-s} + p_r^{-2s} + p_r^{-3s} + \cdots
\end{aligned}$$

Consideramos el siguiente producto

$$\prod_{i=1}^{r} \frac{1}{1-p_i^{-s}} = (1 + p_1^{-s} + p_1^{-2s} + p_1^{-3s} + \cdots)(1 + p_2^{-s} + p_2^{-2s} + p_2^{-3s} + \cdots)\cdots$$

notemos que el término general del producto de la derecha es de la forma $n^{-s} = p_1^{-sm_1} \cdot p_2^{-sm_2} \cdots p_r^{-sm_r}$, para algunos m_j, $j \in \{1, 2, \ldots, r\}$, o dicho de otra forma $n = p_1^{m_1} \cdot p_2^{m_2} \cdots p_r^{m_r}$.

Notemos que un número n es de esta forma si y sólo si sus divisores primos son algunos de los primeros r números primos, además por el teorema fundamental de la aritmética sabemos que dicha descomposición como producto de números primos es única, es decir dicho número n aparece sólo una vez. Entonces tenemos la siguiente igualdad

$$\prod_{p \leqslant p_r} \frac{1}{1-p^{-s}} = \sum_{\substack{p|n \\ p \leqslant p_r}} n^{-s}.$$

De esta manera tenemos que

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \lim_{r\to\infty} \sum_{\substack{p|n \\ p \leqslant p_r}} n^{-s} = \lim_{r\to\infty} \prod_{p \leqslant p_r} \frac{1}{1-p^{-s}} = \prod_{p \ primo} \frac{1}{1-p^{-s}}.$$

□

Este hecho puede ser establecido de manera más general de la siguiente forma.

Teorema 1.18. *Si $\mathcal{F}$ es una función multiplicativa tal que la serie $\sum_{n=1}^{\infty} \left|\mathcal{F}(n)\right|$ converge, entonces para cada $s \in \mathbb{C}$ tal que $Re(s) > 1$, la serie $\sum_{n=1}^{\infty} \left|\frac{\mathcal{F}(n)}{n^s}\right|$ converge y en su dominio de convergencia tiene una descomposición como producto infinito*

$$\sum_{n=1}^{\infty} \frac{\mathcal{F}(n)}{n^s} = \prod_{p \ primo} \Big(1 + \frac{\varphi(p)}{p^s} + \frac{\varphi(p^2)}{p^{2s}} + \frac{\varphi(p^3)}{p^{3s}} + \cdots\Big).$$

Demostración. Primero veamos la convergencia absoluta de la serie. Tenemos que

$$\begin{aligned} 0 < \sum_{n=1}^{\infty} \Big|\frac{\mathcal{F}(n)}{n^s}\Big| \ &= \sum_{n=1}^{\infty} \frac{|\mathcal{F}(n)|}{|n^s|} \leqslant \sum_{n=1}^{\infty} \frac{\mathcal{M}}{|n^s|} \quad \text{(ya que } \mathcal{F} \text{ está acotada)} \\ &= \mathcal{M} \sum_{n=1}^{\infty} \frac{1}{|n^s|} \end{aligned}$$

Pero la serie $\sum_{n=1}^{\infty} \frac{1}{|n^s|}$ converge para $Re(s) > 1$, de esta manera $\sum_{n=1}^{\infty} \left|\frac{\mathcal{F}(n)}{n^s}\right|$ converge.

Por otra parte, para la descomposición como producto infinito, para un $N \in \mathbb{N}$ fijo, consideremos el producto parcial

$$\prod_{p<N} \Big(1 + \frac{\mathcal{F}(p)}{p^s} + \frac{\mathcal{F}(p^2)}{p^{2s}} + \frac{\mathcal{F}(p^3)}{p^{3s}} + \cdots\Big).$$

De otra forma, si $\{p_1, p_2, \ldots, p_k\}$ son los primos menores o iguales que N, entonces dicho producto se puede expresar de la siguiente forma

$$\prod_{j=1}^{k} \Big(1 + \frac{\mathcal{F}(p_j)}{p_j^s} + \frac{\mathcal{F}(p_j^2)}{p_j^{2s}} + \frac{\mathcal{F}(p_j^3)}{p_j^{3s}} + \cdots\Big)$$

donde el término general de dicho producto es a la vez el producto de algunas potencias de los $\dfrac{\mathcal{F}(p_j)}{p_j^s}$, variando dichas potencias, es decir

$$\prod_{j=1}^{k}\left(1+\frac{\mathcal{F}(p_j)}{p_j^s}+\frac{\mathcal{F}(p_j^2)}{p_j^{2s}}+\frac{\mathcal{F}(p_j^3)}{p_j^{3s}}+\cdots\right)=\sum_{m_1,m_2,\ldots,m_k}\frac{\mathcal{F}(p_1^{m_1})\cdot\mathcal{F}(p_2^{m_2})\cdots\mathcal{F}(p_k^{m_k})}{p_1^{sm_1}\cdot p_2^{sm_2}\cdots p_k^{sm_k}}$$

donde los $m_j\in\{1,2,\ldots,k\}$, pero $\mathcal{F}$ es multiplicativa, entonces esa última suma se puede expresar como sigue

$$\sum_{m_1,m_2,\ldots,m_k}\frac{\mathcal{F}(p_1^{m_1}\cdot_2^{m_2}\cdots p_k^{m_k})}{p_1^{m_1}\cdot_2^{m_2}\cdots p_k^{m_k}}=\sum_{p(n)<N}\frac{\mathcal{F}(n)}{n^s}$$

si $n=p_1^{m_1}\cdot_2^{m_2}\cdots p_k^{m_k}$, y donde $p(n)$ es el factor primo mayor que aparece en la descomposición de n como producto de primos.
Como cualquier natural menor que N no tiene factores primos mayores que N, entonces tenemos que

$$\left|\sum_{n=1}^{\infty}\frac{\mathcal{F}(n)}{n^s}-\sum_{p(n)<N}\frac{\mathcal{F}(n)}{n^s}\right|\leqslant\sum_{n=N}^{\infty}\left|\frac{\mathcal{F}(n)}{n^s}\right|$$

y dicha suma tiende a cero cuando N tiende a infinito. □

Corolario 1.19. *Si $\mathcal{F}:\mathbb{N}\longrightarrow\mathbb{C}$ es una función acotada y completamente multiplicativa, entonces $\forall s\in\mathbb{C}$ tal que $Re(s)>1$*

$$\sum_{n=1}^{\infty}\frac{\mathcal{F}(n)}{n^s}=\prod_{p\ primo}\frac{1}{1-\mathcal{F}(p)p^{-s}}$$

El producto de la derecha es conocido como producto de Euler asociado a la serie de la izquierda.

Demostración. Como

$$\frac{1}{1-\mathcal{F}(p)p^{-s}}=1+p^{-s}\mathcal{F}(p)+p^{-2s}\mathcal{F}(p)^2+p^{-3s}\mathcal{F}(p)^3+\cdots$$

y además $\mathcal{F}$ es completamente multiplicativa, entonces se tiene que para cada

primo p, $\mathcal{F}(p^k) = \mathcal{F}(p)^k$.
Por lo anterior tenemos que

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{\mathcal{F}(n)}{n^s} &= \prod_{p\ primo} \left(1 + p^{-s}\mathcal{F}(p) + p^{-2s}\mathcal{F}(p^2) + p^{-3s}\mathcal{F}(p^3) + \cdots\right) \\ &= \prod_{p\ primo} \left(1 + p^{-s}\mathcal{F}(p) + p^{-2s}\mathcal{F}(p)^2 + p^{-3s}\mathcal{F}(p)^3 + \cdots\right) \\ &= \prod_{p\ primo} \frac{1}{1 - \mathcal{F}(p)p^{-s}}.\end{aligned}$$

□

Definición 1.13. *Dado un carácter de Dirichlet, se define su $\mathcal{L}-$ serie de Dirichlet de la siguiente manera*

$$\mathcal{L}(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

para un complejo s tal que $Re(s) > 1$.

Teorema 1.20. *Dado $\chi \neq \chi_1$ un carácter de Dirichlet módulo k, entonces su $\mathcal{L}-$serie de Dirichlet es una función analítica en el semiplano $Re(s) > 0$.*

Demostración. Definimos

$$S_\chi(x) = \sum_{n \leqslant x} \chi(n)$$

ésta es una función periódica, de periodo k y también $S_\chi(n) = 0$ si

$$n \equiv 0\ (mod\ k).$$

Por otro lado como $|\chi| = 1$, se tiene que $|S_\chi(n)| \leqslant k$.

Recordemos que la fórmula de Abel establece que si $\{a_n\}$ es una sucesión de números complejos, $\mathcal{A}(x) = \sum_{1 \leqslant n \leqslant x} a_n$ y Φ es una función de clase C^1 en $[1, x]$, entonces

$$\sum_{1 \leqslant n \leqslant x} a_n \Phi(n) = \mathcal{A}(x)\Phi(x) - \int_1^x \mathcal{A}(t)\Phi'(t)dt.^6$$

[6] La prueba es simplemente una aplicacion de la fórmula de integración por partes para integrales de Riemann-Stieltjes.

Si se aplica la fórmula de Abel a $a_n = \chi(n), \mathcal{A}(x) = S_\chi(x)$ y $\Phi(n) = n^{-s}$, tenemos que

$$\sum_{1 \leqslant n \leqslant x} \frac{\chi(n)}{n^s} = \frac{S_\chi(x)}{x^s} + s\int_1^x S_\chi(t)t^{-s-1}dt$$

y si $x \longrightarrow \infty$, tenemos que

$$\mathcal{L}(\chi, s) = s\int_1^\infty S_\chi(t)t^{-s-1}dt$$

y posteriormente pasa que

$$\left| s\int_1^\infty S_\chi(t)t^{-s-1}dt \right| \leqslant |s|\int_1^\infty |S_\chi(t)|t^{-Re(s)-1}dt \leqslant |s|\int_1^\infty k \cdot t^{-Re(s)-1}dt,$$

y esta última integral resulta ser

$$|s|k\frac{t^{-Re(s)}}{-Re(s)}\Big|_1^\infty = \lim_{x\to\infty} \frac{k|s|}{Re(s)}\big(1 - x^{-Re(s)}\big) = \frac{k|s|}{Re(s)}.$$

Así $\mathcal{L}(\chi, s)$ es analítica en $Re(s) > 0$ y $|\mathcal{L}(\chi, s)| \leqslant \dfrac{k|s|}{Re(s)}$. □

Teorema 1.21. *Para un complejo s tal que $Re(s) > 1$, $\mathcal{L}(\chi, s)$ converge y admite una descomposición como producto de Euler.*

Demostración. Sabemos que cualquier carácter χ cumple $|\chi| = 1$ y son funciones completamente multiplicativas. Entonces para $Re(s) > 1$, $\mathcal{L}(\chi, s)$ converge y además

$$\mathcal{L}(\chi, s) = \prod_{p\ primo} \frac{1}{1 - \chi(p)p^{-s}}.$$

□

Notemos que si $\chi = \chi_1$, entonces $\chi(p) = 0$, además si $p \mid k$, $\chi_1(p) = 1$ y si $(P, k) = 1$, entonces de esta manera el producto de Euler para $\mathcal{L}(\chi_1, s)$ está dado por

$$\mathcal{L}(\chi_1, s) = \prod_{\substack{p\ primo \\ (p,k)=1}} \frac{1}{1 - p^{-s}} = \prod_{p\ primo} \frac{1}{1 - p^{-s}} \cdot \prod_{p|k}(1 - p^{-s}) = \zeta(s)\prod_{p|k}(1 - p^{-s}).$$

Así, estudiar los ceros de esta $\mathcal{L}-$serie de Dirichlet, es equivalente a estudiar los ceros de la función ζ de Riemann.

1.2.6. La no anulación de $\mathcal{L}(\chi, 1)$ para $\chi \neq \chi_1$

Teorema 1.22. *Sea χ un carácter no principal módulo k y f una función no negativa , con derivada continua no negativa para todo $x \geqslant x_0$, entonces si $x_0 \leqslant x \leqslant y$, tenemos*

$$\sum_{x<n\leqslant y} \chi(n)f(n) = \mathcal{O}(f(x)). \tag{1.19}$$

Si además $\lim_{x\to\infty} f(x) = 0$ *entonces la serie* $\sum_{n=1}^{\infty} \chi(n)f(n)$ *converge y tenemos, para $x \geqslant x_0$ que*

$$\sum_{n\leqslant x} \chi(n)f(n) = \sum_{n=1}^{\infty} \chi(n)f(n) + \mathcal{O}(f(x)). \tag{1.20}$$

Demostración. Sea $\mathcal{A}(x) = \sum_{n\leqslant x} \chi(n)$, como $\chi \neq \chi_1$ tenemos que

$$\mathcal{A}(k) = \sum_{n=1}^{k} \chi(n) = 0$$

además, como χ es una función de periodo k, entonces tenemos que $\mathcal{A}(nk) = 0$ para $n = 1, 2, 3 \ldots$. Así, para todo x se tiene que

$$|\mathcal{A}(x)| = \Big| \sum_{n=1}^{k} \chi(n) \Big| \leqslant \sum_{n=1}^{k} |\chi(n)| \leqslant \varphi(k),$$

dicho de otra manera $\mathcal{A}(x) = \mathcal{O}(1)$. Por otro lado se utiliza la identidad de Abel para expresar la suma de (1.19) en forma de integral, de la siguiente manera

$$\begin{aligned}
\sum_{x<n\leqslant y} \chi(n)f(n) &= f(y)\mathcal{A}(y) - f(x)\mathcal{A}(x) - \int_x^y \mathcal{A}(t)f'(t)dt \\
&= f(y)\mathcal{O}(1) + f(x)\mathcal{O}(1) - \int_x^y \mathcal{O}(1)f'(t)dt \\
&= \mathcal{O}(f(y)) + \mathcal{O}(f(x)) + \mathcal{O}\left(\int_x^y (-f'(t))dt \right) = \mathcal{O}(f(x)).
\end{aligned}$$

Con esto queda demostrada la identidad (1.19). Ahora si $\lim_{x\to\infty} f(x) = 0$, tenemos que

$$\lim_{x\to\infty} \sum_{x<n\leqslant y} \chi(n)f(n) = \lim_{x\to\infty} \mathcal{O}(f(x)) = 0,$$

y entonces por el criterio de convergencia de Cauchy, la serie $\sum_{n=1}^{\infty} \chi(n)f(n)$ converge.

Finalmente para probar (1.20) notemos que

$$\begin{aligned}\sum_{n=1}^{\infty} \chi(n)f(n) &= \sum_{n\leqslant x} \chi(n)f(n) + \lim_{y\to\infty} \sum_{x<n\leqslant y} \chi(n)f(n) \\ &= \sum_{n\leqslant x} \chi(n)f(n) + \lim_{y\to\infty} \mathcal{O}(f(x)) \quad \text{(por (1.19))} \\ &= \sum_{n\leqslant x} \chi(n)f(n) + \mathcal{O}(f(x)).\end{aligned}$$

Lo que da lugar a concluir la demostración. □

Consideremos ahora las siguientes funciones

$$f(x) = \frac{1}{x}, f(x) = \frac{log\ x}{x}, f(x) = \frac{1}{\sqrt{x}}$$

para $x \geqslant 1$, claramente dichas funciones cumplen las hipótesis del teorema anterior. Con base en esto tenemos lo siguiente.

Corolario 1.23. *Si χ es un carácter no principal módulo k y si $x \geqslant 1$, entonces:*

$$\sum_{n\leqslant x} \frac{\chi(n)}{n} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} + \mathcal{O}\Big(\frac{1}{x}\Big), \tag{1.21}$$

$$\sum_{n\leqslant x} \frac{\chi(n)log\ n}{n} = \sum_{n=1}^{\infty} \frac{\chi(n)log\ n}{n} + \mathcal{O}\Big(\frac{log\ x}{x}\Big), \tag{1.22}$$

$$\sum_{n\leqslant x}\frac{\chi(n)}{\sqrt{n}}=\sum_{n=1}^{\infty}\frac{\chi(n)}{\sqrt{n}}+\mathcal{O}\Big(\frac{1}{\sqrt{x}}\Big) \tag{1.23}$$

Demostración. □

Finalmente designaremos a la serie que aparece en (1.21) como $\mathcal{L}(\chi,1)$, y la serie que aparece en (1.22) por $-\mathcal{L}'(\chi,1)$.

Teorema 1.24 (**El método de la hipérbola de Dirichlet**). *Sean* $f,g:\mathbb{N}\longrightarrow\mathbb{C}$ *funciones aritméticas. Si* $h=f*g$,

$$\mathcal{F}(x)=\sum_{n\leqslant x}f(n),\quad \mathcal{G}(x)=\sum_{n\leqslant x}g(n),\quad \mathcal{H}(x)=\sum_{n\leqslant x}h(n)$$

y a,b *son números positivos tales que* $ab=x$, *entonces*

$$\mathcal{H}(x)=\sum_{\substack{q,d\\ qd\leqslant x}}f(d)g(q)=\sum_{n\leqslant a}f(n)\mathcal{G}\Big(\frac{x}{n}\Big)+\sum_{n\leqslant b}g(n)\mathcal{F}\Big(\frac{x}{n}\Big)-\mathcal{F}(a)\mathcal{G}(b) \tag{1.24}$$

Demostración. Notemos que podemos escribir $\mathcal{H}(x)$ de la siguiente manera

$$\mathcal{H}(x)=\sum_{n\leqslant x}f*g=\sum_{n\leqslant x}\sum_{d|n}f(d)g\Big(\frac{n}{d}\Big)=\sum_{\substack{q,d\\ qd\leqslant x}}f(d)g(q)\quad(\text{donde } n=qd)$$

por otra parte la suma $\mathcal{H}(x)=\sum_{\substack{q,d\\ qd\leqslant x}}f(d)g(q)$ se encuentra extendida en todas las parejas de puntos reticulares (q,d) que están comprendidos en el primer cuadrante del plano, por debajo de la gráfica de la hipérbola $qd=x$ (denotaremos esta región por Γ).

Consideremos las siguientes regiones (ver *Figura* 1.4)

$$\mathbf{A}=\{(q,d)\in\mathbb{N}\times\mathbb{N}:qd\leqslant x\ y\ d\leqslant a\}$$
$$\mathbf{B}=\{(q,d)\in\mathbb{N}\times\mathbb{N}:qd\leqslant x\ y\ q\leqslant b\}$$

y finalmente $\mathbf{C}=\mathbf{A}\cap\mathbf{B}$.

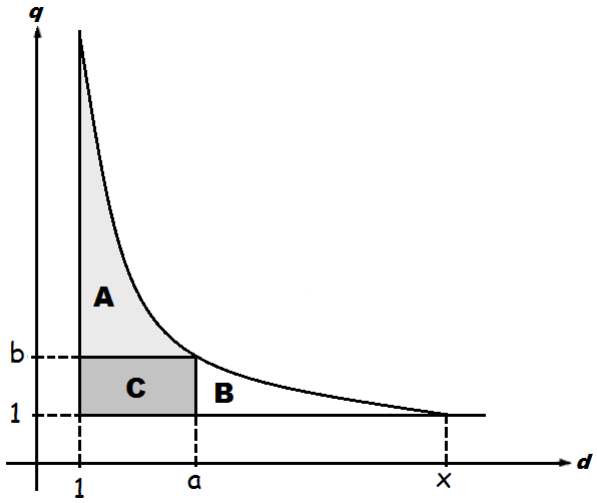

Figura 1.4: Regiones de puntos reticulares

Notemos que

$$\sum_{(q,d)\in\Gamma} f(d)g(q) = \sum_{(q,d)\in\mathbf{A}} f(d)g(q) + \sum_{(q,d)\in\mathbf{B}} f(d)g(q) - \sum_{(q,d)\in\mathbf{C}} f(d)g(q) \quad (1.25)$$

Calculemos por separado las sumas que aparecen en (1.25)

a) $$\sum_{(q,d)\in\mathbf{A}} f(d)g(q) = \sum_{d\leqslant a} f(d) \sum_{q\leqslant \frac{x}{d}} g(q) = \sum_{d\leqslant a} \sum_{q\leqslant \frac{x}{d}} f(d)g(q) = \sum_{n\leqslant a} f(n)\mathcal{G}\Big(\frac{x}{n}\Big)$$

b) $$\sum_{(q,d)\in\mathbf{B}} f(d)g(q) = \sum_{q\leqslant b} g(q) \sum_{d\leqslant \frac{x}{q}} f(d) = \sum_{q\leqslant b} \sum_{d\leqslant \frac{x}{q}} f(d)g(q) = \sum_{n\leqslant b} g(n)\mathcal{F}\Big(\frac{x}{n}\Big)$$

c) $$\sum_{(q,d)\in\mathbf{C}} f(d)g(q) = \mathcal{F}(a)\mathcal{G}(b).$$

Así, sustituyendo en (1.25) tenemos el resultado deseado. □

Lema 1.2. *Sea χ un carácter real módulo k y sea*

$$\mathcal{A}(n) = \sum_{d|n} \chi(d)$$

entonces $\mathcal{A}(n) \geqslant 0$ *para toda* n*, si además* n *es un cuadrado por lo tanto*

$$\mathcal{A}(n) \geqslant 1.$$

Demostración. La prueba se divide en dos casos, partiremos por el más sencillo de ellos.

Caso 1: Si n es una potencia de un primo, es decir $n = p^a$, entonces tenemos que

$$\mathcal{A}(p^a) = \sum_{t=0}^{a} \chi(p^t) = 1 + \sum_{t=1}^{a} \chi(p^t) = 1 + \sum_{t=1}^{a} \chi(p)^t,$$

como χ es un carácter real solo se pueden tomar los valores $0, -1, 1$.

Si $\chi(p) = 0$, entonces $\mathcal{A}(p^a) = 1$. Si $\chi(p) = 1$, entonces

$$\mathcal{A}(p^a) = 1 + \sum_{t=1}^{a} \chi(p^t) = 1 + \sum_{t=1}^{a} 1 = 1 + a.$$

Finalmente si $\chi(p) = -1$ se tendrá

$$\mathcal{A}(p^a) = \begin{cases} 0 & si \quad a \quad impar \\ 1 & si \quad a \quad par. \end{cases}$$

Así, si $n = p^\alpha$ entonces $\mathcal{A}(p^a) \geqslant 0$.

Caso 2: Si n es compuesto, es decir $n = \prod_{i=1}^{k} {p_i}^{a_i}$, se puede probar que

$$\mathcal{A}(n) = \mathcal{A}({p_1}^{a_1}) \cdot \mathcal{A}({p_2}^{a_2}) \cdots \mathcal{A}({p_k}^{a_k}),$$

luego por el caso anterior tenemos que $\mathcal{A}(p_i^{a_i}) \geqslant 0$, $\forall i \in \{1, 2, \ldots, k\}$. Y así

$$\mathcal{A}(n) = \mathcal{A}({p_1}^{a_1}) \cdot \mathcal{A}({p_2}^{a_2}) \cdots \mathcal{A}({p_k}^{a_k}) \geqslant 0.$$

Finalmente, si n es un cuadrado, tenemos que a_i es par $\forall i \in \{1, 2, \ldots, k\}$. De esta manera tenemos por el Caso 1 que $\mathcal{A}({p_i}^{a_i}) \geqslant 1$, es decir

$$\mathcal{A}(n) = \mathcal{A}({p_1}^{a_1}) \cdot \mathcal{A}({p_2}^{a_2}) \cdots \mathcal{A}({p_k}^{a_k}) \geqslant 1.$$

como se quería demostrar. □

Teorema 1.25. *Para todo carácter no principal real χ módulo k consideremos*

$$\mathcal{A}(n) = \sum_{d|n} \chi(d) \text{ y } \mathcal{B}(x) = \sum_{n\leqslant x} \frac{\mathcal{A}(n)}{\sqrt{n}}$$

entonces tenemos:

a) $\mathcal{B}(x) \longrightarrow \infty$ *cuando* $x \longrightarrow \infty$

b) $\mathcal{B}(x) = 2\sqrt{x}\mathcal{L}(\chi, 1) + \mathcal{O}(1)$ *para todo* $x \geqslant 1$.

Demostración. Para probar la parte a) tenemos por el *lema* 2.1 que

$$\mathcal{B}(x) = \sum_{n\leqslant x} \frac{\mathcal{A}(n)}{\sqrt{n}} \geqslant \sum_{\substack{n\leqslant x \\ n=m^2}} \frac{1}{\sqrt{n}} = \sum_{m\leqslant\sqrt{x}} \frac{1}{m}.$$

Entonces, tenemos la siguiente desigualdad

$$\lim_{x\to\infty} \mathcal{B}(x) \geqslant \lim_{x\to\infty} \sum_{m\leqslant\sqrt{x}} \frac{1}{m} = \infty \quad \text{(pues la serie armónica diverge)}$$

Para probar la parte b) escribimos

$$\mathcal{B}(x) = \sum_{n\leqslant x} \frac{\mathcal{A}(n)}{\sqrt{n}} = \sum_{n\leqslant x} \frac{1}{\sqrt{n}} \sum_{d|n} \chi(d) = \sum_{\substack{q,d \\ qd\leqslant x}} \frac{\chi(d)}{\sqrt{qd}} = \sum_{\substack{q,d \\ qd\leqslant x}} \frac{\chi(d)}{\sqrt{d}} \cdot \frac{1}{\sqrt{q}}$$

donde $n = qd$.
Consideremos $a = b = \sqrt{x}$ y $f(n) = \dfrac{\chi(n)}{\sqrt{n}}$, $g(n) = \dfrac{1}{\sqrt{n}}$, y por (1.24) tenemos que

$$\begin{aligned} \mathcal{B}(x) &= \sum_{\substack{q,d \\ qd\leqslant x}} \frac{\chi(d)}{\sqrt{qd}} \\ &= \sum_{n\leqslant\sqrt{x}} \frac{\chi(n)}{\sqrt{n}} \mathcal{G}\Big(\frac{x}{n}\Big) + \sum_{n\leqslant\sqrt{x}} \frac{1}{\sqrt{n}} \mathcal{F}\Big(\frac{x}{n}\Big) - \mathcal{F}(\sqrt{x})\mathcal{G}(\sqrt{x}). \end{aligned} \tag{1.26}$$

Recordemos que $\mathcal{G}(x) = \sum_{n\leqslant x} \frac{1}{\sqrt{n}} = 2\sqrt{x} + A + \mathcal{O}\Big(\frac{1}{x}\Big)$[7] en donde A es una constante. Por otro lado, por (1.23) tenemos que $\sum_{n\leqslant x} \frac{\chi(n)}{\sqrt{n}} = B + \mathcal{O}\Big(\frac{1}{x}\Big)$, donde $B = \sum_{n=1}^{\infty} \frac{\chi(n)}{\sqrt{n}}$. Notemos además que

$$\begin{aligned}
\mathcal{F}(\sqrt{x})\mathcal{G}(\sqrt{x}) &= \Big(B + \mathcal{O}\Big(\frac{1}{\sqrt{x}}\Big)\Big)\Big(2x^{1/4} + A + \mathcal{O}\Big(\frac{1}{\sqrt{x}}\Big)\Big) \\
&= 2Bx^{1/4} + \mathcal{O}\Big(\frac{2}{x^{1/4}}\Big) + AB + \mathcal{O}\Big(\frac{A}{\sqrt{x}}\Big) + \mathcal{O}\Big(\frac{B}{\sqrt{x}}\Big) + \mathcal{O}\Big(\frac{1}{x}\Big) \\
&= 2Bx^{1/4} + \mathcal{O}(1).
\end{aligned}$$

Al sustituir lo anterior en (1.26) tenemos que:

$$\begin{aligned}
\mathcal{B}(x) = &\sum_{n\leqslant\sqrt{x}} \frac{\chi(n)}{\sqrt{n}}\left(2\sqrt{\tfrac{x}{n}} + A + \mathcal{O}\Big(\sqrt{\tfrac{n}{x}}\Big)\right) + \sum_{n\leqslant\sqrt{x}} \frac{1}{\sqrt{n}}\left(B + \mathcal{O}\Big(\sqrt{\tfrac{n}{x}}\Big)\right) \\
&- 2Bx^{1/4} + \mathcal{O}(1) \\
&= 2\sqrt{x}\sum_{n\leqslant\sqrt{x}} \frac{\chi(n)}{n} + A\sum_{n\leqslant\sqrt{x}} \frac{\chi(n)}{\sqrt{n}} + \mathcal{O}\left(\frac{1}{\sqrt{x}}\sum_{n\leqslant\sqrt{x}} |\chi(n)|\right) + B\sum_{n\leqslant\sqrt{x}} \frac{1}{\sqrt{n}} \\
&+ \mathcal{O}\left(\frac{1}{\sqrt{x}}\sum_{n\leqslant\sqrt{x}} 1\right) - 2Bx^{1/4} + \mathcal{O}(1) \quad \text{(distribuyendo)} \\
&= 2\sqrt{x}\mathcal{L}(\chi, 1) + \mathcal{O}(1).
\end{aligned}$$

□

Corolario 1.26. *Para todo carácter no principal real χ módulo k tenemos que $\mathcal{L}(\chi, 1) \neq 0$.*

Demostración. Inmediata por el teorema anterior. □

Lema 1.3. *En el semiplano complejo $Re(s) > 1$, se tiene que $\big|\mathcal{L}(\chi, s)\big| > 0$.*

[7] La prueba es una aplicación de la fórmula de sumación de Euler.

Demostración. Sabemos que

$$|\mathcal{L}(\chi, s)| = \prod_{p \ primo} \left| \frac{1}{1 - \chi(p)p^{-s}} \right|,$$

además, como $\chi(p) = 0$ siempre que $(p, k) > 1$ y $\chi(p) = \psi(p)$ si $(p, k) = 1$, entonces podemos reescribir el producto anterior de la siguiente manera

$$\prod_{p \nmid k} \left| \frac{1}{1 - \chi(p)p^{-s}} \right| \geqslant \prod_{p \nmid k} \frac{1}{1 + |\chi(p)|p^{-Re(s)}} = \prod_{p \nmid k} \frac{1}{1 + p^{-Re(s)}} > 0.$$

□

Lema 1.4. *Para $Re(s) > 1$ y χ un carácter de Dirichlet módulo k tenemos que:*

$$log\big(\mathcal{L}(\chi, s)\big) = \sum_{p \ primo} \sum_{m=1}^{\infty} \frac{(\chi(p))^m}{mp^{ms}} \tag{1.27}$$

Demostración.

$$\begin{aligned} log\big(\mathcal{L}(\chi, s)\big) &= log\left(\prod_{p \ primo} \frac{1}{1 - \chi(p)p^{-s}} \right) \\ &= \sum_{p \ primo} log\left(\frac{1}{1 - \chi(p)p^{-s}} \right) && \text{(por propiedades de logaritmos)} \\ &= \sum_{p \ primo} -log\Big(1 - \frac{\chi(p)}{p^s}\Big) && \text{(por propiedades de logaritmos)} \\ &= \sum_{p \ primo} \sum_{m=1}^{\infty} \frac{\chi(p)^m}{mp^{ms}} && \text{(pues } -log(1-z) = \sum_{m=1}^{\infty} \frac{z^m}{m}.\text{)} \end{aligned}$$

□

Podemos considerar que a partir de este punto damos inicio a la prueba del teorema de Dirichlet. Seguiremos la ruta trazada en la introducción e iniciamos demostrando que $\mathcal{L}(\chi, 1) \neq 0$ para los caracteres de Dirichlet no principales.

Teorema 1.27. *Si χ es un carácter de Dirichlet módulo k con $\chi \neq \chi_1$, entonces $\mathcal{L}(\chi, 1) \neq 0$.*

Demostración. Dividiremos la prueba en dos casos.

Caso 1: Si χ es un carácter real, entonces por el *Corolario* 1.26 el caso está concluido.
Caso 2:
Sea χ un carácter complejo y $s > 1$. Tenemos que

$$\begin{aligned}
\sum_{i=1}^{\varphi(k)} log\big(\mathcal{L}(\chi_i, s)\big) &= \sum_{i=1}^{\varphi(k)} \left(\sum_{p \ primo} \left(\sum_{m=1}^{\infty} \frac{1}{m} \frac{(\chi_i(p))^m}{p^{ms}} \right) \right) \qquad \text{(por (1.27))} \\
&= \sum_{p \ primo} \left(\sum_{m=1}^{\infty} \frac{1}{m} \frac{\sum_{i=1}^{\varphi(k)} \chi_i(p^m)}{p^{ms}} \right) \\
&= \sum_{p \ primo} \left(\sum_{\substack{m=1 \\ p^m \equiv 1 \ (mod \ k)}}^{\infty} \frac{\varphi(k)}{mp^{ms}} \right) \qquad \text{(Por (1.14))} \\
&= \varphi(k) \sum_{p \ primo} \left(\sum_{\substack{m=1 \\ p^m \equiv 1 \ (mod \ k)}}^{\infty} \frac{1}{mp^{ms}} \right) \geqslant 0,
\end{aligned}$$

por lo que

$$\left| \prod_{i=1}^{\varphi(k)} \mathcal{L}(\chi_i, s) \right| = exp\left(\sum_{i=1}^{\varphi(k)} log\big(\mathcal{L}(\chi_i, s)\big) \right) \geqslant exp(0) = 1. \qquad (1.28)$$

Supongamos que para un carácter complejo χ se tiene que $\mathcal{L}(\chi, 1) = 0$, como $\chi \neq \overline{\chi}$ y $\mathcal{L}(\overline{\chi}, 1) = \overline{\mathcal{L}(\chi, 1)} = 0$, se tiene que en el producto $\prod_{i=1}^{\varphi(k)} \mathcal{L}(\chi_i, s)$ hay al menos dos ceros cuando $s \longrightarrow 1^+$, que son suficientes para cancelar el único polo simple correspondiente a $\mathcal{L}(\chi_1, 1)$, por lo que:

$$\lim_{s \to 1^+} \left| \prod_{i=1}^{\varphi(k)} \mathcal{L}(\chi_i, s) \right| = 0$$

lo cual contradice (1.28). □

1.2.7. Sumas con caracteres de Dirichlet

Lema 1.5. *Para $x > 1$ y $\chi \neq \chi_1$, tenemos que*

$$\mathcal{L}(\chi, 1) \sum_{n \leqslant x} \frac{\mu(n)\chi(n)}{n} = \mathcal{O}(1) \tag{1.29}$$

Demostración. Primero recordemos que la fórmula de inversión de Möbius generalizada establece que si $\alpha : \mathbb{N} \longrightarrow \mathbb{C}$ es una función completamente multiplicativa, entonces

$$G(x) = \sum_{n \leqslant x} \alpha(n) F\Big(\frac{x}{n}\Big) \text{ si y sólo si } F(x) = \sum_{n \leqslant x} \mu(n)\alpha(n) G\Big(\frac{x}{n}\Big).$$

Ahora, consideremos que si $\alpha(n) = \chi(n)$ y $F(x) = x$, entonces al aplicar la fórmula de inversión de Möbius generalizada tenemos que

$$x = \sum_{n \leqslant x} \mu(n)\chi(n) G\Big(\frac{x}{n}\Big) \tag{1.30}$$

de donde

$$G(x) = \sum_{n \leqslant x} \chi(n)\frac{x}{n} = x \sum_{n \leqslant x} \frac{\chi(n)}{n} = x\left(\sum_{n=1}^{\infty} \frac{\chi(n)}{n} + \mathcal{O}\Big(\frac{1}{x}\Big) \right) = x\mathcal{L}(\chi, 1) + \mathcal{O}(1).$$

Al sustituir en (1.30) tenemos que

$$\begin{aligned} x &= \sum_{n \leqslant x} \mu(n)\chi(n) G\Big(\frac{x}{n}\Big) \\ &= \sum_{n \leqslant x} \mu(n)\chi(n)\Big(\frac{x}{n}\mathcal{L}(\chi, 1) + \mathcal{O}(1)\Big) \\ &= x\mathcal{L}(\chi, 1) \sum_{n \leqslant x} \frac{\mu(n)\chi(n)}{n} + \sum_{n \leqslant x} \mu(n)\chi(n)\mathcal{O}(1). \end{aligned}$$

Enfocándonos en la suma de la derecha tenemos que

$$\begin{aligned} \sum_{n \leqslant x} \mu(n)\chi(n)\mathcal{O}(1) = \mathcal{O}(1) \sum_{n \leqslant x} \mu(n)\chi(n) &\leqslant \mathcal{O}(1) \sum_{n \leqslant x} \chi(n) \\ &\leqslant \mathcal{O}(1)\varphi(k) = \mathcal{O}(1). \end{aligned}$$

Así, podemos escribir

$$x = x\mathcal{L}(\chi, 1) \sum_{n \leqslant x} \frac{\mu(n)\chi(n)}{n} + \mathcal{O}(x).$$

Es decir, tenemos que

$$\mathcal{O}(x) = x\mathcal{L}(\chi, 1) \sum_{n \leqslant x} \frac{\mu(n)\chi(n)}{n},$$

y al dividir entre x obtenemos el resultado deseado. □

Por el lema anterior y usando el hecho de que $\mathcal{L}(\chi, 1) \neq 0$ obtenemos el siguiente resultado.

Lema 1.6. *Para $x > 1$ y $\chi \neq \chi_1$ tenemos*

$$\sum_{n \leqslant x} \frac{\mu(n)\chi(n)}{n} = \mathcal{O}(1) \tag{1.31}$$

Demostración. Por (1.21) sabemos que $\mathcal{L}(\chi, 1)$ es convergente y no nula, entonces por el lema anterior tenemos que

$$\sum_{n \leqslant x} \frac{\mu(n)\chi(n)}{n} = \frac{\mathcal{O}(1)}{\mathcal{L}(\chi, 1)} = \mathcal{O}(1).$$

□

A continuación estudiaremos una suma similar a la anterior pero ahora extendida únicamente sobre los primos, para esto es necesario introducir una nueva función y probar algunas de sus propiedades.

Definición 1.14. *Para cada $n \in \mathbb{N}$ definimos la función de Mangoldt como sigue*

$$\Lambda(n) = \begin{cases} \log p & si \quad n = p^{\alpha} \quad para \quad p \quad primo \quad y \quad \alpha \geqslant 1 \\ 0 & en \quad otro \quad caso \end{cases}$$

Esta función debe su nombre al matemático Alemán Hans von Mangoldt. Expondremos algunas propiedades importantes de la función de Mangoldt.

Teorema 1.28. *Si $n \geqslant 1$ entonces*

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

Demostración. Si $n = 1$ entonces $0 = log(1) = \sum_{d|1} \Lambda(d)$. Supongamos entonces que $n > 1$. Si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ tenemos que

$$log(n) = log\Big(\prod_{i=1}^{r} p_i^{\alpha_i}\Big) = \sum_{i=1}^{r} log(p_i^{\alpha_i}) = \sum_{i=1}^{r} \alpha_i log(p_i).$$

Por otra parte tenemos lo siguiente

$$\sum_{d|n} \Lambda(d) = \sum_{i=1}^{r} \sum_{m=1}^{\alpha_i} \Lambda(p_i^m) = \sum_{i=1}^{r} \sum_{m=1}^{\alpha_i} log\ p_i = \sum_{i=1}^{r} \alpha_i log\ p_i = log(n).$$

□

Corolario 1.29. *Para $n \geqslant 1$ tenemos que $\Lambda(n) = \sum_{d|n} \mu(d) log\Big(\frac{n}{d}\Big)$.*

Demostración. Recordemos que la fórmula de inversión de Möbius establece que si $g(n)$ y $f(n)$ son funciones aritméticas que satisfacen $g(n) = \sum_{d|n} f(d)$ para todo entero $n \geqslant 1$, entonces

$$f(n) = \sum_{d|n} g(d)\mu\Big(\frac{n}{d}\Big) = \sum_{d|n} \mu(d) f\Big(\frac{n}{d}\Big),$$

para toda $n \geqslant 1$. De esta manera si hacemos $g(n) = log\ n$ y $f(n) = \Lambda(n)$ y con la fórmula de inversión de Möbius tenemos el resultado deseado. □

Lema 1.7. *Para $x > 1$ y $\chi \neq \chi_1$ se tiene que*

$$\sum_{p \leqslant x} \frac{\chi(p) log\ p}{p} = -\mathcal{L}'(\chi, 1) \sum_{n \leqslant x} \frac{\mu(n)\chi(n)}{n} + \mathcal{O}(1). \tag{1.32}$$

Demostración. tenemos que

$$\sum_{n\leqslant x}\frac{\chi(n)\Lambda(n)}{n}=\sum_{p\leqslant x}\sum_{a=1}^{\infty}\frac{\chi(p^a)log\ p}{p^a}\qquad\text{(donde } p^a\leqslant x)$$
$$=\sum_{p\leqslant x}\frac{\chi(p)log\ p}{p}+\sum_{p\leqslant x}\sum_{a=2}^{\infty}\frac{\chi(p^a)log\ p}{p^a}\qquad\text{(donde } p^a\leqslant x)$$

y como la segunda suma está acotada superiormente por

$$\sum_{p\ primo}log\ p\sum_{a=2}^{\infty}\frac{1}{p^a}=\sum_{p\ primo}\frac{log\ p}{p(p-1)}<\sum_{n=2}^{\infty}\frac{log\ n}{n(n-1)}=\mathcal{O}(1)$$

entonces podemos escribir

$$\sum_{p\leqslant x}\frac{\chi(p)log\ p}{p}=\sum_{n\leqslant x}\frac{\chi(n)\Lambda(n)}{n}+\mathcal{O}(1).\tag{1.33}$$

Por otro lado, del *corolario* 1.29 tenemos que:

$$\sum_{n\leqslant x}\frac{\chi(n)\Lambda(n)}{n}=\sum_{n\leqslant x}\frac{\chi(n)}{n}\sum_{d|n}\mu(d)log\Big(\frac{n}{d}\Big),$$

y si escribimos $n=cd$, aunado con que usemos la propiedad multiplicativa de χ, entonces podemos escribir la igualdad anterior de la siguiente manera

$$\sum_{n\leqslant x}\frac{\chi(n)\Lambda(n)}{n}=\sum_{d\leqslant x}\frac{\mu(d)\chi(d)}{d}\sum_{c\leqslant x/d}\frac{\chi(c)log\ c}{c}.\tag{1.34}$$

Como $x/d\geqslant 1$, en la suma con respecto a c podemos utilizar (1.22) y así se tiene que:

$$\sum_{c\leqslant x/d}\frac{\chi(c)log\ c}{c}=-\mathcal{L}(1,\chi)+\mathcal{O}\left(\frac{log\big(x/d\big)}{x/d}\right)$$

y al sustituir en (1.34), tenemos que:

$$\sum_{n\leqslant x}\frac{\chi(n)\Lambda(n)}{n}=\left(\sum_{d\leqslant x}\frac{\mu(d)\chi(d)}{d}\right)\left(-\mathcal{L}(1,\chi)+\mathcal{O}\left(\frac{log\big(x/d\big)}{x/d}\right)\right)$$
$$=-\mathcal{L}'(1,\chi)\sum_{d\leqslant x}\frac{\mu(d)\chi(d)}{d}+\mathcal{O}\left(\sum_{d\leqslant x}\frac{1}{d}\frac{log\big(x/d\big)}{x/d}.\right)$$

ahora, note que

$$\begin{aligned}\sum_{d\leqslant x}\frac{1}{d}\frac{log\big(x/d\big)}{x/d} &= \sum_{d\leqslant x}\frac{1}{d}\frac{log\ x - log\ d}{x/d}\\ &= \frac{1}{x}\sum_{d\leqslant x}\big(log\ x - log\ d\big)\\ &= \frac{[x]log\ x}{x} - \frac{1}{x}\sum_{d\leqslant x} log\ d\\ &= \frac{1}{x}([x]log\ x - xlog\ x + \mathcal{O}(x)) = \mathcal{O}(1).\end{aligned}$$

Por lo tanto

$$\sum_{n\leqslant x}\frac{\chi(n)\Lambda(n)}{n} = -\mathcal{L}'(1,\chi)\sum_{d\leqslant x}\frac{\mu(d)\chi(d)}{d} + \mathcal{O}(1). \tag{1.35}$$

Por (1.33) y (1.35) llegamos al resultado deseado. □

Así por el *lema* 1.6 y dado que $-\mathcal{L}'(\chi,1)$ es convergente obtenemos el siguiente resultado.

Lema 1.8. *Para $x>1$ y $\chi\neq\chi_1$ se tiene que*

$$\sum_{p\leqslant x}\frac{\chi(p)log\ p}{p} = \mathcal{O}(1) \tag{1.36}$$

Demostración. Se sigue de (1.31), (1.32) y de la convergencia de $\mathcal{L}'(\chi,1)$. □

Acto seguido pasamos a probar la identidad que podemos considerar es la identidad fundamental para la prueba del teorema de Dirichlet.

Lema 1.9. *Para cada $x>1$ tenemos*

$$\sum_{\substack{p\leqslant x\\ p\equiv h\ (mod\ k)}}\frac{log\ p}{p} = \frac{1}{\varphi(k)}log\ x\ +\ \frac{1}{\varphi(k)}\sum_{r=2}^{\varphi(k)}\overline{\chi}_r(h)\sum_{p\leqslant x}\frac{\chi_r(p)log\ p}{p} + \mathcal{O}(1)$$

Demostración. Sabemos que

$$\sum_{r=1}^{\varphi(k)} \chi_r(p)\overline{\chi}_r(h) = \begin{cases} \varphi(k) & si \quad p \equiv h \ (mod\ k) \\ 0 & si \quad p \not\equiv h \ (mod\ k) \end{cases} \quad \text{siempre que } (p,k)=1$$

además, si $p \equiv h \ (mod\ k)$, y si multiplicamos ambos lados de la igualdad por $\dfrac{log\ p}{p}$, entonces obtenemos la siguiente expresión

$$\sum_{r=1}^{\varphi(k)} \chi_r(p)\overline{\chi}_r(h)\frac{log\ p}{p} = \varphi(k)\frac{log\ p}{p} \quad \text{si } p \equiv h \ (mod\ k).$$

Ahora, se suma para todos los primos menores o iguales que x y se obtiene lo siguiente

$$\begin{aligned} &\sum_{p\leqslant x}\sum_{r=1}^{\varphi(k)} \chi_r(p)\overline{\chi}_r(h)\frac{log\ p}{p} \\ &= \varphi(k) \sum_{\substack{p\leqslant x \\ p\equiv h \ (mod\ k)}} \frac{log\ p}{p} \\ &= \sum_{r=1}^{\varphi(k)} \chi_r(p)\overline{\chi}_r(h) \sum_{p\leqslant x} \frac{log\ p}{p} \\ &= \overline{\chi}_1(h) \sum_{p\leqslant x} \frac{\chi_1(p) log\ p}{p} + \sum_{r=2}^{\varphi(k)} \overline{\chi}_r(h) \sum_{p\leqslant x} \frac{\chi_r(p) log\ p}{p}. \end{aligned}$$

Notemos que $\overline{\chi}_1(h) = 1$ y $\chi_1(p) = 1$ siempre que $(p,k) = 1$ y cero en otro caso.
Por lo que

$$\begin{aligned} \overline{\chi}_1(h) \sum_{p\leqslant x} \frac{\chi_1(p) log\ p}{p} &= \sum_{\substack{p\leqslant x \\ (p,k)=1}} \frac{log\ p}{p} \\ &= \sum_{p\leqslant x} \frac{log\ p}{p} - \sum_{\substack{p\leqslant x \\ p|k}} \frac{log\ p}{p} \\ &= \sum_{p\leqslant x} \frac{log\ p}{p} + \mathcal{O}(1) \end{aligned}$$

pues la cantidad de primos que dividen a k es finita.

Recordemos que el primer teorema de Mertens establece que

$$\sum_{p\leqslant x}\frac{log\ p}{p}=log\ x+\mathcal{O}(1),$$

entonces tenemos que:

$$\begin{aligned}\varphi(k)\sum_{\substack{p\leqslant x\\ p\equiv h\ (mod\ k)}}\frac{log\ p}{p}&=\overline{\chi}_1(h)\sum_{p\leqslant x}\frac{\chi_1(p)log\ p}{p}+\sum_{r=2}^{\varphi(k)}\overline{\chi}_r(h)\sum_{p\leqslant x}\frac{\chi_r(p)log\ p}{p}\\&=\sum_{p\leqslant x}\frac{log\ p}{p}+\sum_{r=2}^{\varphi(k)}\overline{\chi}_r(h)\sum_{p\leqslant x}\frac{\chi_r(p)log\ p}{p}+\mathcal{O}(1)\\&=log\ x+\mathcal{O}(1)+\sum_{r=2}^{\varphi(k)}\overline{\chi}_r(h)\sum_{p\leqslant x}\frac{\chi_r(p)log\ p}{p}+\mathcal{O}(1)\\&=log\ x+\sum_{r=2}^{\varphi(k)}\overline{\chi}_r(h)\sum_{p\leqslant x}\frac{\chi_r(p)log\ p}{p}+\mathcal{O}(1),\end{aligned}$$

y al dividir entre $\varphi(k)$ tenemos el resultado deseado. □

Finalmente, conjuntado los lemas anteriores obtenemos el siguiente resultado.

Lema 1.10. *Si $k>0$ y $(h,k)=1$, entonces para toda $x>1$*

$$\sum_{\substack{p\leqslant x\\ p\equiv h\ (mod\ k)}}\frac{log\ p}{p}=\frac{1}{\varphi(k)}log\ x+\mathcal{O}(1)\tag{1.37}$$

Demostración. Por el *lema* 1.9 tenemos que

$$\begin{aligned}\sum_{\substack{p\leqslant x\\ p\equiv h\ (mod\ k)}}\frac{log\ p}{p}&=\frac{1}{\varphi(k)}log\ x\ +\ \frac{1}{\varphi(k)}\sum_{r=2}^{\varphi(k)}\overline{\chi}_r(h)\sum_{p\leqslant x}\frac{\chi_r(p)log\ p}{p}+\mathcal{O}(1)\\&=\frac{1}{\varphi(k)}log\ x+\frac{1}{\varphi(k)}\sum_{r=2}^{\varphi(k)}\overline{\chi}_r(h)\mathcal{O}(1)+\mathcal{O}(1)\quad(\text{por }(1.36))\\&=\frac{1}{\varphi(k)}log\ x+\mathcal{O}(1).\end{aligned}$$

□

Teorema 1.30. *Si $k > 0$ y $(h,k) = 1$, la serie* $\sum_{\substack{p \text{ primo} \\ p \equiv h \pmod{k}}} \frac{log\ p}{p}$ *diverge.*

Demostración. Por (1.37) tenemos que

$$\sum_{\substack{p \text{ primo} \\ p \equiv h \pmod{k}}} \frac{log\ p}{p} = \lim_{x \to \infty} \sum_{\substack{p \leqslant x \\ p \equiv h \pmod{k}}} \frac{log\ p}{p} = \lim_{x \to \infty} \frac{1}{\varphi(k)} log\ x + \mathcal{O}(1) = \infty.$$

□

Corolario 1.31 (**Dirichlet 1837**). *Si $(h,k) = 1$ existe una infinidad de primos en la progresión aritmética $h + nk$ para $n = 0, 1, 2, 3, \ldots$*

Demostración. Inmediata por el teorema anterior. □

1.3. Un bosquejo de las pruebas originales

En esta sección presentamos sólo un bosquejo de los planteamientos y demostraciones que conocemos de Dirichlet y Dedekind. Se conoce un libro [Dirichlet 1999] sobre teoría de números que contiene aportaciones de ambos y en él Dedekind demuestra el teorema de las progresiones de Dirichlet. No presentamos todo el análisis de los trabajos de ambos porque se requiere una extensión considerable y un análisis de corte histórico que sobrepasa el objetivo de esta tesis.

1.3.1. Dirichlet

Figura 1.5: Johann Peter Gustav Lejeune Dirichlet (1805-1859)

Se debe de considerar que en la demostración de Dirichlet lo que ahora conocemos como caracteres -y que llevan su nombre- no aparecen de manera explícita, no obstante sí podemos reconocer algunas de las propiedades que actualmente conocemos de los caracteres. Por lo señalado no esperemos encontrar una lista de propiedades de éstos en el trabajo original.

Dirichlet plantea su análisis a partir de que la diferencia entre dos elementos consecutivos de la progresión aritmética $a + tp$ es un primo p. Ahora, dado el primo p ya era posible para Dirichlet encontrar lo que conocemos como una raíz primitiva módulo p, es decir, encontrar un entero c tal que los $p-1$

residuos de $c^0, c^1, \ldots, c^{p-2}$ módulo p generen al conjunto $\{0, 1, 2, \ldots, p-1\}$ en algún orden.

Para Dirichlet estaba clara la idea de que para todo entero n, existe un entero γ_n tal que

$$c^{\gamma_n} \equiv n \ (mod\ p).$$

Sabemos que si χ es un carácter de Dirichlet módulo p, entonces $\chi(c)$ es una raíz p-ésima de la unidad, digamos ω. Con lo anterior sabemos que χ se puede determinar mediante ω, esto es, que para todo n primo relativo con p se tiene que

$$\chi(n) = \omega^{\gamma_n}.$$

En esta igualdad se encuentra la notación que usa Dirichlet para lo que actualmente usamos como $\chi(n)$.

Se tiene que considerar que cuando la diferencia no es p (primo), sino un k compuesto entonces se escribirá de la forma $k = 2^{\lambda} p_1^{\pi_1} p_2^{\pi_2} \cdots p_j^{\pi_j}$ que es producto de potencias de primos y ya no será tan manejable este caso como el primero. Dirichlet ya sabía por Gauss que si p es un primo impar y π es un entero mayor o igual que uno entonces se puede encontrar una raíz primitiva c módulo p^{π}. Esto se puede interpretar como que para todo entero n primo con p existe un γ_n tal que

$$c^{\gamma_n} \equiv n \ (mod\ p^{\pi}).$$

De esta manera se pueden elegir raíces primitivas $c_1, c_2, \ldots, c_j$ asociadas con $p_1^{\pi_1} p_2^{\pi_2} \cdots p_j^{\pi_j}$. Pero, para el caso que $\lambda \geqslant 3$ no hay raíz primitiva módulo 2^{λ}, y lo que se tiene es que $\left(\mathbb{Z}/2^{\lambda}\mathbb{Z}\right)^*$ es un producto de dos grupos cíclicos, y para todo entero n primo con 2^{λ} existen α_n y β_n tales que

$$(-1)^{\alpha_n} 5^{\beta_n} \equiv m \ (mod\ 2^{\lambda}).$$

Así, para todo n primo con k se puede escribir que

$$n \equiv (-1)^{\alpha_n} 5^{\beta_n} c_1^{\gamma_{1,m}} c_2^{\gamma_{2,m}} \cdots c_j^{\gamma_{j,m}} \ (mod\ k),$$

donde $\gamma_{i,n}$ es el índice de n relacionado con $p_i^{\pi_i}$.

Con las raíces adecuadas de la unidad $\theta, \varphi, \omega_1, \omega_2, \ldots, \omega_j$ se llega a que

$$\chi(n) = \theta^{\alpha_n} \varphi^{\beta_n} \omega_1^{\gamma_{1,m}} \omega_2^{\gamma_{2,m}} \cdots \omega_j^{\gamma_{j,m}}.$$

Se puede recapitular todo lo anterior de esta manera: cuando se tiene un módulo primo p Dirichlet fija un elemento primitivo módulo c y representa cada carácter χ en términos de una raíz p-ésima ω de la unidad, y en ese caso el valor del carácter es $\chi(n) = \omega^{(\gamma)}$. En el caso en que el módulo k sea compuesto entonces Dirichlet fija unos elementos primitivos módulo los términos primos de la factorización de k, y cada carácter χ queda representado en términos de la sucesión $\theta, \varphi, \pi, \pi', \ldots$ que son las raíces de la unidad.

En este contexto actualmente identificamos a los caracteres como argumentos de las L-funciones, es decir, $L(s, \chi)$ que estarán vinculadas con las sumas sobre los caracteres. Ahora demos lugar a la manera como lo abordó Dirichlet.

Dirichlet -nuevamente- tratará en primer lugar el caso cuando la diferencia de los elementos de la progresión es un primo p, y recordemos que para este caso cada carácter χ corresponde a una raíz Ω p-ésima de la unidad. Dirichlet usó el producto de Euler de esta manera:

$$\prod \frac{1}{1 - \omega^{\gamma} \frac{1}{q^s}} = \sum \omega^{\gamma} \frac{1}{n^s} = L$$

donde el producto se evalúa en los primos (menos p) y la suma sobre los naturales que son primos con p. Además, γ se refiere a γ_p en el producto y γ_n en la suma.

Como hay $p-1$ raíces diferentes $(p-1)$-ésimas de la unidad, Dirichlet menciona lo que sigue: El producto de Euler construido en la igualdad anterior representa $(p-1)$ ecuaciones diferentes, que se pueden obtener reemplazando ω con los $(p-1)$ valores. Se sabe que los $p-1$ valores diferentes pueden ser representados por una de las potencias de Ω, elegida adecuadamente, de entre estas $\Omega^0, \Omega^1, \ldots, \Omega^{p-2}$. En correspondencia con estas potencias podemos escribir los diferentes valores de L, correspondientes a las sumas y productos como

$$L_0, L_1, \ldots, L_{p-2}.$$

Para el caso general cuando la diferencia entre los términos de la progresión es un compuesto k, el proceso que Dirichlet presenta es semejante, esto es

$$\prod \frac{1}{1-\theta^{\alpha}\varphi^{\beta}\omega^{\gamma}\omega'^{\gamma'}\frac{1}{q^s}} = \sum \theta^{\alpha}\varphi^{\beta}\omega^{\gamma}\omega'^{\gamma'}\frac{1}{n^s} = L,$$

el sistema de índices $\alpha, \beta, \gamma, \gamma', \ldots$ en el producto corresponden con q, y los de la suma con n.

De la ecuación general las raíces diferentes $\theta, \varphi, \omega, \omega', \ldots$ pueden ser combinadas entre sí y se obtienen k ecuaciones.

Dirichlet hace notar que podemos escoger las raíces primitivas de la unidad $\Theta, \Phi, \Omega, \Omega', \ldots$ de tal manera que $\theta, \varphi, \omega, \omega', \ldots$ pueden ser expresadas como potencias de ellas, entonces

$$\theta = \Theta^a, \varphi = \Phi^b, \omega = \Omega^c, \omega' = \Omega'^{c'} \ldots$$

y esto queda como en el primer caso. Dirichlet señaló que nos podemos referir a la L-serie de una manera adecuada como $L_{a,b,c,c'}$ donde los subíndices son los exponentes de las raíces primitivas elegidas.
Para el caso donde la diferencia común es un primo p, Dirichlet desarrolla una ecuación, que en nuestra notación sería

$$log\ L(s,\chi) = -\sum_{q\nmid k} log\big(1-\frac{\chi(q)}{q^s}\big)$$

y al hacerlo obtiene que

$$\sum \frac{1}{q^{1+\rho}} + \frac{1}{2}\sum \frac{1}{q^{2+2\rho}} + \frac{1}{3}\sum \frac{1}{q^{3+3\rho}} + \cdots$$
$$= \frac{1}{p-1}(logL_0 + \Omega^{-\gamma_m} logL_1 + \Omega^{-2\gamma_m} logL_2 + \cdots + \Omega^{-(p-1)\gamma_m} logL_{p-2}).$$

Y el fin es llegar a algo de la forma

$$\sum_{\chi\in\widehat{\mathbb{Z}_k^*}} \overline{\chi(m)} log\ L(s,\chi) = \varphi(k) \sum_{q\equiv m\ (mod\ k)} \frac{1}{q^s} + \mathcal{O}(1).$$

Aquí hacemos una pausa para retomar la fórmula de Euler

$$\sum_{n=1}^{\infty} n^{-s} = \prod_{q} \left(1 - \frac{1}{q^s}\right)^{-1}$$

que es equivalente a

$$log \sum_{n=1}^{\infty} n^{-s} = \sum_{q} -log\left(1 - \frac{1}{q^s}\right),$$

y como

$$log\ (1-x) = -x - \frac{x^2}{2} - \frac{x^3}{3} - \cdots$$

entonces se tiene que

$$log \sum_{n=1}^{\infty} n^{-s} = \sum_{q} \frac{1}{q^s} + \sum_{n=2}^{\infty} \frac{1}{n} \sum_{q} \frac{1}{q^{ns}}$$

y por lo tanto

$$log \sum_{n=1}^{\infty} n^{-s} = \sum_{q} \frac{1}{q^s} + \mathcal{O}(1).$$

Finalmente Dirichlet deduce que cuando $s \longrightarrow 1$ el término de la Derecha diverge y por lo tanto la suma de la izquierda diverge, lo cual ocurre solamente cuando hay una infinidad de primos q, lo que concluye la demostración.

1.3.2. Dedekind

En 1863 Dedekind publicó el libro "*Vorlesungen Über Zahlentheorie*" (Lectures on number theory), éste estaba hecho con base en sus notas tomadas de un curso de teoría de números impartido por Dirichlet en la Universidad de Göttingen. Dedekind añadió nueve suplementos con material propio, en particular el suplemento VI contenía una presentación del teorema de Dirichlet.

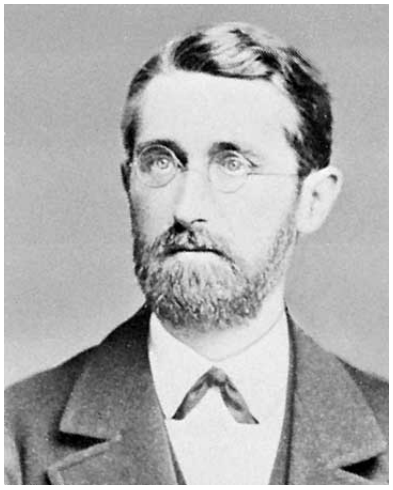

Figura 1.6: Julius Wilhelm Richard Dedekind (1831-1916)

Dedekind comenzó considerando series infinitas de la forma

$$L = \sum \psi(n)$$

donde n recorre todos los enteros positivos y la función real o compleja $\psi(n)$ satisface la condición

$$\psi(n)\psi(n') = \psi(nn'),$$

además suponemos que $\psi(1) = 1$.[8] (Dirichlet 1863)

[8] "Der allgemeine Beweis dieses Satzes... stützt sich auf die Betrachtung einer Classe von unendlichen Reihen von der Form

$$L = \sum \psi(n),$$

wo der Buchstabe n alle ganzen positiven Zahlen durchlaufen muss, und die reelle oder complexe Function $\psi(n)$ der Bedingung

$$\psi(n)\psi(n') = \psi(nn')$$

genügt ... so nehmen wir immer an, dass $\psi(1) = 1$ ist."

Él escribió las letras

$$a, b, c, c', \ldots$$

y consideró que

$$\theta, \eta, \omega, \omega', \ldots$$

denotan alguna raíz de las ecuaciones

$$\theta^a = 1,\ \eta^b = 1,\ \omega^c = 1,\ \omega'^{c'} = 1, \ldots$$

Si n es un entero positivo cooprimo con k y si sus índices son

$$\alpha\ (mod\ a),\ \beta\ (mod\ b),\ \gamma\ (mod\ c),\ \gamma'\ (mod\ c'), \ldots$$

Dedekind dice "es fácil ver que la expresión

$$\psi(n) = \frac{\theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \cdots}{n^s}$$

satisface la condición

$$\psi(n)\psi(n') = \psi(nn')".$$

Dedekind no se refirió a las expresiones importantes como "caracteres" sino que solo introdujo la notación $\chi(n)$ para denotar el numerador de $\psi(n)$, dicho de otra manera $\chi(n) = \theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \cdots$ y señalo que tiene la propiedad $\chi(n)\chi(n') = \chi(nn')$ (Dirichlet 1863).[9]

Luego Dedekind probó el producto de Euler

$$\prod \frac{1}{1 - \psi(q)} = \sum \psi(n) \tag{1.38}$$

donde el producto se encuentra extendido sobre todos los primos.

Dedekind continuó haciendo notar que las L series pueden tener un comportamiento bastante diferente dependiendo de las raíces de la unidad $\theta, \eta, \omega, \omega', \ldots$ que aparecen como factores de $\psi(n)$, y dado que estas raíces pueden tomar $a, b, c, c', \ldots$ valores distintos, entonces tenemos que hay

$$abcc' \cdots = \varphi(k)$$

[9]"Der Zähler $\chi(n) = \theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \cdots$ besitzt die charakteristischen Eigenschaften $\chi(n)\chi(n') = \chi(nn')$..."

distintas L series (Dirichlet 1863)[10]

A éstas Dedekind las clasificó en tres tipos

1. Las raíces de la unidad que se involucran en la construcción del carácter que aparece en L son todas 1, solo hay una serie de este tipo denotada por L_1.

2. Las raíces de la unidad que se involucran en la construcción del carácter que aparece en L son todas reales, es decir son todas ± 1, las L-funciones que aparecen en esta categoría se escriben como L_2.

3. Al menos una raíz de la unidad que aparece en la construcción del carácter que aparece en la L serie es compleja, las series de este tipo se escriben como L_3, más aún cada serie que cae en esta categoría tiene un conjugado L_3' correspondiente a la misma categoría.

Después, de (1.38) y de la expansión en series del logaritmo cuando $|z| < 1$

$$z + \frac{1}{2}z^2 + \frac{1}{3}z^3 + \cdots = log\left(\frac{1}{1-z}\right)$$

donde la parte imaginaria del lado derecho se considera siempre entre $-\frac{1}{2}\pi i$ y $+\frac{1}{2}\pi i$, Dedekind prueba la siguiente ecuación

$$\sum \psi(q) + \frac{1}{2}\sum \psi(q^2) + \frac{1}{3}\sum \psi(q^3) + \cdots = log\ L, \tag{1.39}$$

y hace las siguientes observaciones. Primero, si $\psi(n)$ es real entonces $log\ L$ es real, más aún L es positiva y distinto de cero.

---

[10]"Wir bemerken zunächst, dass diese Reihen je nach der Wahl der in dem Ausdrucke $\psi(n)$ vorkommenden Einheits-Wurzeln $\theta, \eta, \omega, \omega', \ldots$ ein ganz verschiedenes Verhalten zeigen; da dieseWurzeln resp.
$a, b, c, c', \ldots$verschiedene Werthe haben können, so sind in der Form L im Ganzen

$$abcc' \cdots = \varphi(k)$$

verschiedene besondere Reihen enthalten . . . "

Si $\psi(n)$ es complejo y $\psi'(n)$ denota su conjugado, tenemos $\psi(n)\psi(n') = \psi(nn')$ y la suma $L' = \sum \psi'(n)$ es el conjugado de $L = \sum \psi(n)$, de hecho $log\ L'$ es el conjugado de $log\ L$ por lo que la suma $log\ L + log\ \ L' = log(LL')$ es real.

Posteriormente Dedekind prueba resultados clave necesarios para la demostración del teorema de Dirichlet. Primero demuestra que la serie $log\ L_1$ no es convergente, mientras que las series $log\ L$ son convergentes, con esto estamos en posición para trazar la demostración que Dedekind dio. Comienza considerando m un entero positivo primo relativo con k y multiplicando las $\varphi(k)$ series distintas de la forma

$$\sum \psi(q) + \frac{1}{2}\sum \psi(q^2) + \frac{1}{3}\sum \psi(q^3) + \cdots = log\ L,$$

que corresponden al sistema particular de raíces de la unidad

$$\theta, \eta, \omega, \omega', \ldots$$

por el correspondiente valor

$$\theta^{-\alpha_1}\eta^{-\beta_1}\omega^{-\gamma_1}\omega'^{-\gamma_1'}\cdots = \chi$$

donde $\alpha_1, \beta_1, \gamma_1, \gamma_1', \ldots$ son los índices del número m, entonces el término

$$\frac{1}{\mu}\frac{1}{q^{\mu s}}$$

adquiere el coeficiente

$$\sum \theta^{\alpha\mu-\alpha_1}\eta^{\beta\mu-\beta_1}\omega^{\gamma\mu-\gamma_1}\omega'^{\gamma'\mu-\gamma_1'}\ldots$$

donde $\alpha, \beta, \gamma, \gamma', \ldots$ son los índices del primo q y la suma está indicada sobre los $\varphi(k)$ sistemas de raíces. Dicho de otra manera este coeficiente es el producto de las sumas individuales

$$\sum \theta^{\alpha\mu-\alpha_1}, \sum \eta^{\beta\mu-\beta_1}, \sum \omega^{\gamma\mu-\gamma_1}, \sum \omega'^{\gamma'\mu-\gamma_1'}\ldots$$

donde $\theta, \eta, \omega, \omega', \ldots$ pueden tomar respectivamente $a, b, c, c', \ldots$ valores distintos. Así Dedekind dice "este coeficiente es por lo tanto no cero y de hecho es igual a

$$abcc' \cdots = \varphi(k)$$

solo si $\alpha\mu - \alpha_1, \beta\mu - \beta_1, \gamma\mu - \gamma_1, \gamma'\mu - \gamma_1', \ldots$ son divisibles por $a, b, c, c', \ldots$". Es decir, como

$$q^{\mu} \equiv m \ (mod\ k)$$

la suma de todos los productos de la forma $\chi log\ L$ da el resultado

$$\varphi(k)\left(\sum \frac{1}{q^s} + \frac{1}{2}\sum \frac{1}{q^2 s} + \frac{1}{3}\sum \frac{1}{q^3 s} + \cdots\right) = \sum \chi log\ L \qquad (1.40)$$

donde las sumas del lado izquierdo están extendidas sobre todos los primos que satisfacen las siguientes condiciones respectivamente

$$q \equiv m,\ q^2 \equiv m,\ q^3 \equiv m \ \ldots\ (mod\ k).$$

La suma del lado derecho de la ecuación (1.40) es sobre todos los $\varphi(k)$ sistemas de raices

$$\theta, \eta, \omega, \omega' \ldots .$$ [11]

A continuación Dedekind hace la sustitución

$$Q = \frac{1}{2}\sum \frac{1}{q^{2s}} + \frac{1}{3}\sum \frac{1}{q^{3s}} + \frac{1}{4}\sum \frac{1}{q^{4s}} + \cdots$$

y z es algún entero positivo mayor que 1, entonces se tiene la siguiente ecuación.

$$Q < \frac{1}{2}\sum \frac{1}{z^2} + \frac{1}{2}\sum \frac{1}{z^3} + \frac{1}{2}\sum \frac{1}{z^4} + \cdots .$$

[11] Die Summation aller Producte $\chi log\ L$ giebt daher das Resultat

$$\varphi(k)\left(\sum \frac{1}{q^s} + \frac{1}{2}\sum \frac{1}{q^2 s} + \frac{1}{3}\sum \frac{1}{q^3 s} + \cdots\right) = \sum \chi log\ L$$

wo auf der linken Seite das erste, zweite, dritte Summenzeichen u.s.f. sich auf alle Primzahlen q bezieht, welche resp. den Bedingungen $q \equiv m,\ q^2 \equiv m,\ q^3 \equiv m \ \ldots\ (mod\ k)$ u.s.f. genügen, während das Summenzeichen auf der rechten Seite sich auf die sämmtlichen $\varphi(k)$ verschiedenen Wurzel-Systeme $\theta, \eta, \omega, \omega', \ldots$

Luego, si $z \geqslant 2$ tenemos las siguientes condiciones sucesivas

$$\frac{1}{z^3} \leqslant \frac{1}{2}\frac{1}{z^2}, \quad \frac{1}{z^4} \leqslant \frac{1}{4}\frac{1}{z^2}, \quad \frac{1}{z^5} \leqslant \frac{1}{8}\frac{1}{z^2}, \ldots$$

sumando cada una de estas desigualdades tenemos que

$$Q < \sum \frac{1}{z^2}.$$

Así, cuando $s \longrightarrow 1$, Q permanece acotado y también dado que todos los términos de la forma $\chi logL$ que intervienen en la ecuación

$$\varphi(k)\left(\sum \frac{1}{q^s} + Q\right) = \sum \chi logL$$

son finitos, excepto el término $logL_1$, entonces la suma

$$\sum \frac{1}{q^s}$$

no puede ser acotada, lo cual sólo es posible si existe una cantidad infinita de términos en la suma, por lo que existen una infinidad de primos $q \equiv m \ (mod\ k)$, lo que concluye la prueba del teorema de los primos en progresiones aritméticas.

Capítulo 2

Progresiones y sumas de $k-$ésimas potencias

2.1. Sumas de cuadrados

Uno de nuestros objetivos es estudiar diversas características de las progresiones aritméticas de Dirichlet, y para esto hemos considerado que es apropiado adentrarnos en las representaciones de enteros como suma de $k-$ésimas potencias, que es lo que conocemos como problemas de Waring. Entrar a esta área de la teoría de los números resulta, por decirlo de alguna manera, cómodo, ya que está demostrado por Hilbert que todo entero es una suma de $k-$ésimas potencias.

Así, como nuestro interés son las progresiones aritméticas de Dirichlet entonces podemos preguntarnos ¿qué características tienen estas progresiones cuando se analiza en cada uno de sus términos la cantidad de representaciones como suma de $k-$ésimas potencias? Pero de aquí tendríamos varias preguntas paralelas ¿Cómo se comporta la cantidad de las representaciones de los términos de las progresiones en las bases mínimas?[1] Pero antes que las bases mínimas nos podemos preguntar algo semejante con la cantidad de representaciones para las bases asintóticas[2], es decir, ¿qué característi-

[1] Entendemos como base mínima a la cantidad menor de enteros que pueden representar a todo entero como suma de $k-$ésimas potencias, por ejemplo, todo entero es una suma de cuatro cuadrados; es una suma de nueve cubos, diecinueve cuartas potencias y así sucesivamente.

[2] Consideraremos que una base es asintótica cuando todo entero se puede representar

cas encontramos en los elementos de las progresiones aritméticas de Dirichlet después que analizamos su cantidad de representaciones en términos de bases asintóticas?

Como no es posible estudiar todos las casos para las representaciones como suma de $k-$ésimas potencias entonces en este capítulo sólo estudiaremos las sumas de cuadrados y cubos. Primero mostraremos propiedades de progresiones como suma de dos cuadrados; acto seguido, que todo entero es suma de cuatro cuadrados; después exhibiremos que las representaciones para cada entero no son únicas, y en particular analizaremos las progresiones aritméticas de Dirichlet dentro del conjunto general de las representaciones como suma de cuadrados. Por otro lado, ya sabemos que la suma con tres cuadrados no es una base asintótica para todos los enteros positivos, pero es posible exhibir progresiones aritméticas de Dirichlet que sí son representables como suma de tres cuadrados.

De manera semejante trabajaremos con la suma de cubos y su cantidad de representaciones.

2.1.1. Progresiones como suma de dos cuadrados

Los elementos de ciertas progresiones aritméticas se pueden representar como suma de dos cuadrados, pero no puede ser cualquier progresión. Podemos constatar que en $\mathbb{Z}_4$ una de las dos progresiones de Dirichlet no es representable como suma de dos cuadrados. Tenemos que la progresión $\{4k+3\}$ no lo es. El teorema que sigue lo puede justificar.

Teorema 2.1. *Los elementos de la progresión aritmética de Dirichlet* $\{4k+3\}$ *no se pueden expresar como suma de dos cuadrados.*

Demostración. Sea n un elemento de la progresión $\{4k+3\}$, dicho de otra manera, $n \equiv 3 \ (mod\ 4)$. Además supongamos que $n = x^2+y^2$ para $x, y \in \mathbb{Z}^+$. Por otro lado, sabemos que el cuadrado de cualquier entero m módulo 4 cumple con $m^2 \equiv 0, 1 (mod\ 4)$, y se debe a que si m es par, entonces m^2 es múltiplo de 4, y por tanto deja resto 0 módulo 4; si m es impar, entonces m^2

como suma de $k-$ésimas potencias salvo una cantidad finita de excepciones. Por ejemplo, todo entero es suma de $8, 7$ y 6 cubos salvo una cantidad finita de excepciones, entonces decimos que las bases asintóticas para los cubos son con $8, 7$ o 6 cubos.

es impar y deja resto 1 módulo 4. Así, llegamos a que $n = x^2 + y^2 \equiv 0, 1$ ó 2 $(mod\ 4)$ pero no puede pasar que deje resto 3, es decir, n no es congruente con 3 módulo 4 y esto contradice la hipótesis. □

Entonces concluimos que ningún entero en la progresión $\{4k+3\}$ puede ser representado como suma de dos cuadrados y en particular ningún primo de esta forma.

Ahora veremos que en $\mathbb{Z}_4$ los primos en la progresión aritmética de Dirichlet $\{4k+1\}$ sí se pueden escribir como suma de dos cuadrados. Para demostrar este resultado requerimos identificar algunas características de los enteros compuestos positivos que sí pueden ser representados como suma de dos cuadrados.

Lema 2.1. *Sea p un número primo en la progresión $\{4k+1\}$. Entonces existen $x, y \in \mathbb{Z}^+$ tal que*

$$x^2 + y^2 = mp,$$

para algún $m \in \mathbb{Z}^+$ y $m < p$.

Demostración. Por hipótesis p es un primo en la progresión $\{4k+1\}$, entonces $p \equiv 1\ (mod\ 4)$, así el símbolo de Legendre[3] nos indica que[4] $\left(-1/p\right) = 1$, es decir, -1 es residuo cuadrático módulo p. Entonces existe un entero $\alpha < p$ tal que

$$\alpha^2 \equiv -1\ (mod\ p),$$

donde α es un elemento del sistema completo de residuos módulo p. Así de la congruencia anterior se obtiene que $\alpha^2 + 1 = mp$, para alguna $m \in \mathbb{Z}^+$ y si nombramos $x = \alpha$ y $y = 1$, entonces $x^2 + y^2 = mp$.

---

[3]Sea $a \in \mathbb{Z}$ y sea p un primo impar tal que $(a, p) = 1$. Se define el símbolo de Legendre igual a 1, y se denota como $\left(\frac{a}{p}\right)$ si a es un residuo cuadrático módulo p, y se define igual a -1 en cualquier otro caso.

[4]Se usa el resultado que dice que si $p \equiv 1\ (mod\ 4)$ entonces existe x tal que

$$x^2 \equiv -1\ (mod\ p),$$

y en consecuencia $\left(-1/p\right) = 1$

Sólo falta ver que $m < p$. Para esto, como tenemos que $\alpha < p$ entonces $\alpha \leqslant p-1$ y por otro lado como $mp = \alpha^2 + 1 \leqslant (p-1)^2 + 1$, entonces

$$mp \leqslant (p-1)^2 + 1 = p^2 - 2(p-1) < p^2,$$

es decir $mp < p^2$, por lo cual $m < p$. □

El siguiente resultado muestra que podemos ir más lejos respecto a que $m < p$, es decir podemos demostrar que m es exactamente 1. Y con ello demostraremos que todo primo en la progresión aritmética de Dirichlet $\{4k+1\}$ es suma de dos cuadrados.

Teorema 2.2. *Si p es un primo en la progresión $\{4k+1\}$, es decir que $p \equiv 1 \ (mod\ 4)$, entonces p puede ser expresado como suma de dos cuadrados.*

Demostración. Por el lema anterior, existe un entero positivo m tal que $mp = x^2 + y^2$, para $x, y \in \mathbb{Z}^+$. Probaremos por contradicción que $m = 1$.

Supongamos que $m > 1$, es el menor entero tal que mp puede ser expresado como suma de dos cuadrados y consideremos un sistema completo de residuos (nos referiremos a él como SCR) módulo m, donde dado cualquier z en el SCR cumple que

$$\frac{-m}{2} < z \leqslant \frac{m}{2}.$$

Entonces existen a y b en el SCR tal que

$$a \equiv x \ (mod\ m) \ y \ b \equiv y \ (mod\ m) \tag{2.1}$$

y

$$\frac{-m}{2} < a, b \leqslant \frac{m}{2}. \tag{2.2}$$

Entonces

$$a^2 + b^2 \equiv x^2 + y^2 \equiv mp \equiv 0 \ (mod\ m),$$

y en consecuencia $a^2 + b^2 \equiv 0 \ (mod\ m)$, es decir $a^2 + b^2 = mk$, para algún $k \in \mathbb{Z}^+$. Ahora, tenemos que

$$(a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2 \tag{2.3}$$

y además

$$(a^2+b^2)(x^2+y^2) = (mk)(mp) = m^2kp. \tag{2.4}$$

A partir de (2.3) y (2.4) se tiene que $(ax+by)^2 + (ay-bx)^2 = m^2kp$.

Como $a \equiv x \ (mod\ m)$, entonces $ay \equiv xy \ (mod\ m)$ y como $b \equiv y \ (mod\ m)$ entonces $bx \equiv yx \ (mod\ m)$, por lo tanto $ay - bx \equiv xy - xy \equiv 0 \ (mod\ m)$. Así tenemos que $(ax+by)$ y $ay-bx$ son múltiplos de m, y en consecuencia

$$\left(\frac{ax+by}{m}\right), \left(\frac{ay-bx}{m}\right) \in \mathbb{Z}.$$

Ahora, como $(ax+by)^2 + (ay-bx)^2 = m^2kp$, entonces

$$\left(\frac{ax+by}{m}\right)^2 + \left(\frac{ay-bx}{m}\right)^2 = kp.$$

Lo que obtenemos es que kp es suma de dos cuadrados enteros. Ya teníamos que m es el menor entero positivo tal que mp es suma de dos cuadrados y por (2.2) $a, b \leqslant \frac{m}{2}$, entonces

$$a^2 + b^2 \leqslant \tfrac{m^2}{4} + \tfrac{m^2}{4} = \tfrac{m^2}{2},$$

y como $a^2+b^2 = mk$, entonces $mk \leqslant \frac{m^2}{2} < m^2$, por lo tanto $k < m$. pero recuerde que m es el mínimo entero positivo tal que mp es suma de dos cuadrados. Así que basta demostrar que $k > 0$ para terminar la contradicción.

Ahora, si $k = 0$, entonces $a^2 + b^2 = mk = 0$, y se tendría que $a = b = 0$, y por (2.1) $x \equiv y \equiv 0 \ (mod\ m)$; de esta forma x, y sería divisibles por m y así $m^2 \mid x^2$ y $m^2 \mid y^2$, por lo tanto $m^2 \mid x^2 + y^2 = mp$, lo cual implica $m \mid p$, pero teníamos por el lema anterior que $m < p$, entonces $m = 1$, y esto contradice nuestra hipótesis ($m > 1$). Por lo tanto $k > 0$ y cumple con que $1 \leqslant k \leqslant m$, y a la vez kp es suma de dos cuadrados, lo cual no puede suceder por la minimalidad de m y mp. En conclusión, el entero k no puede existir y m tiene que ser 1, es decir

$$mp = (1)p = p = x^2 + y^2.$$

□

Con los resultados anteriores ya podemos establecer las condiciones necesarias y suficientes para que un primo positivo impar pueda expresarse como suma de dos cuadrados.

Teorema 2.3. *Sea p un primo impar tal que $p = x^2 + y^2$, entonces p es un entero en la progresión $\{4k+1\}$.*

Demostración. Sea p un primo impar, tal que $p = x^2 + y^2$, para algunos $x, y \in \mathbb{Z}^+$, entonces x y y deben ser de distinta paridad, pues si son de la misma paridad entonces p sería par, lo cual contradice la hipótesis. De esta forma, podemos considerar $x = 2a$ y $y = 2b + 1$, por lo tanto

$$p = (2a)^2 + (2b+1)^2 = 4a^2 + 4b^2 + 4b + 1 = 4(a^2 + b^2 + b) + 1,$$

es decir, $p = 4k + 1$ donde $k = a^2 + b^2 + b \in \mathbb{Z}$, por lo tanto p es un primo en la progresión $\{4k+1\}$. □

Terminamos esta sección señalando que la cantidad de representaciones como suma de dos cuadrados de los primos en la progresión aritmética de Dirichlet $\{4k+1\}$ es única.

Teorema 2.4. *Todo primo en la progresión aritmética de Dirichlet $\{4k+1\}$ puede ser representado de manera única como suma de dos cuadrados salvo el orden y signos.*

Demostración. La demostración se puede ver en [Tattersall 2005]. □

2.1.2. Progresiones como suma de tres cuadrados

De manera natural ahora podríamos preguntarnos qué clase de progresiones se pueden representar como suma de tres cuadrados. Sabemos que no todos los enteros son suma de tres cuadrados. En esta sección trabajaremos con $\mathbb{Z}_8$ y veremos que siete de las ocho progresiones sí se pueden escribir como suma de tres cuadrados. Para demostrar esto requerimos de varios teoremas y no todos serán demostrados en la tesis.

Las progresiones en $\mathbb{Z}_8$ son: $\{8k+0\}$, $\{8k+1\}$, $\{8k+2\}$, $\{8k+3\}$, $\{8k+4\}$, $\{8k+5\}$, $\{8k+6\}$, $\{8k+7\}$. El teorema que enunciamos a continuación nos indica que la clase $\{8k+6\}$[5] se puede escribir como suma de tres cuadrados.

[5]Si $n = 8k+6 = 8k+4+2 = 4(2k+1)+2 = 4s+2$, es decir $\{8k+6\} \subset \{4s+2\}$.

Aquí no se presenta la demostración, pero se puede consultar en la obra de Nathanson [1996]

Teorema 2.5. *Si n es un entero positivo y $n \equiv 2 \ (mod\ 4)$, entonces n puede ser representado como suma de tres cuadrados.*

Para las clases $\{8k+1\}, \{8k+3\}$ *y* $\{8k+5\}$, contamos con un teorema que afirma que las tres se pueden escribir como suma de tres cuadrados. Es interesante notar que todas son progresiones aritméticas de Dirichlet.

Teorema 2.6. *Los elementos de las progresiones aritméticas de Dirichlet* $\{8k+1\}, \{8k+3\}$ *y* $\{8k+5\}$, *pueden ser representados como suma de tres cuadrados*

Demostración. Claramente, 1 es suma de tres cuadrados no negativos, así podemos considerar $n \geqslant 2$. Sea

$$c = \begin{cases} 3 & \text{si } n \equiv 1 \ (mod\ 8) \\ 1 & \text{si } n \equiv 3 \ (mod\ 8) \\ 5 & \text{si } n \equiv 5 \ (mod\ 8) \end{cases}$$

partamos del caso $n \equiv 1 \ (mod\ 8)$, entonces $cn \equiv c + 8 \ (mod\ 8)$, es decir $cn - 1 \equiv c + 7 \ (mod\ 8)$, ahora como $c = 3$, se tiene que $c + 7 \equiv 2 \ (mod\ 8)$; de esta forma

$$\frac{cn-1}{2} \equiv 1 \ (mod\ 4).$$

De manera análoga para $n \equiv 3 \ (mod\ 8)$, así si $n \equiv 1 \ o \ 3 \ (mod\ 8)$ se tiene que

$$\frac{cn-1}{2} \equiv 1 \ (mod\ 4).$$

Por otro lado si $n \equiv 5 \ (mod\ 8)$, entonces $cn \equiv 5c \ (mod\ 8)$, recordemos que en este caso $c = 3$, así $cn \equiv 15 \equiv 7 \ (mod\ 8)$. Luego $cn - 1 \equiv 6 \ (mod\ 8)$, y así

$$\frac{cn-1}{2} \equiv 3 \ (mod\ 4),$$

como $\dfrac{cn-1}{2} \equiv 1 \ (mod\ 4)$ y $\dfrac{cn-1}{2} \equiv 3 \ (mod\ 4)$, podemos reescribir los máximos comunes divisores de la siguiente manera:

$$\left(\tfrac{cn-1}{2}, 4\right) = (1, 4) = 1$$

y

$$\left(\tfrac{cn-1}{2}, 4\right) = (3, 4) = 1$$

de esta manera se tiene que en ambos casos

$$\left(\tfrac{cn-1}{2}, 4\right) = 1 \tag{2.5}$$

por otro lado supongamos que $\left(\tfrac{cn-1}{2}, n\right) = d$, luego $d \mid \tfrac{cn-1}{2}$, es decir $2d \mid cn-1$, pero $d \mid 2d$, así por transitividad se tiene que $d \mid cn-1$, por otro lado como $d \mid n$ divide a cualquier múltiplo de n, en particular $d \mid cn$, entonces $d \mid 1$ y en consecuencia

$$\left(\tfrac{cn-1}{2}, n\right) = 1 \tag{2.6}$$

luego de (2.5) *y* (2.6) se tiene que

$$\left(\tfrac{cn-1}{2}, 4n\right) = 1.$$

Así, por el teorema de Dirichlet podemos asegurar que existe un número primo p de la forma

$$p = 4nj + \frac{cn-1}{2}$$

para algún entero positivo j. Sea $d' = 8j + c$, entonces

$$\begin{aligned} 2p &= 8nj + cn - 1 \\ &= (8j + c)n - 1 \\ &= d'n - 1 \end{aligned} \tag{2.7}$$

de estas últimas dos igualdades se tiene que

$$d' = 8j + c,$$

luego por (2.7) para ver que n puede ser representado como suma de tres cuadrados basta probar que $-d'$ es un residuo cuadrático módulo $2p$.[6]

[6] Aquí usamos el siguiente resultado: para $n \geqslant 2$ si existe $d' \in \mathbb{Z}^+$ tal que $-d'$ es residuo cuadrático módulo $d'n-1$, entonces n puede ser representado como suma de dos cuadrados.

Veamos ahora que el hecho de que $-d'$ sea un residuo cuadrático módulo p implica que $-d'$ es un residuo cuadrático módulo $2p$, y así basta con probar que $-d'$ es un residuo cuadrático módulo p para demostrar que n puede ser representado como suma de tres cuadrados.

Para esto supongamos que $-d'$ es un residuo cuadrático módulo p, entonces existe un entero x_0 tal que

$$x_0^2 \equiv -d' \ (mod\ p).$$

Por otro lado $2px_0 + p^2 \equiv 0 \ (mod\ p)$ entonces $x_0^2 + 2px_0 + p^2 \equiv -d' \ (mod\ p)$, así se tiene que

$$(x_0 + p)^2 + d' \equiv 0 \ (mod\ p).$$

Sea $x = x_0$, con x_0 impar, y sea $x = x_0 + p$ si x_0 es par, en ambos casos x es impar y $x^2 + d'$ es par. Como $x^2 + d' \equiv 0 \ (mod\ 2)$ y $x^2 + d' \equiv 0 \ (mod\ p)$ y dado que $(2, p) = 1$, se sigue que

$$x^2 + d' \equiv 0 \ (mod\ 2p).$$

Veamos entonces que $-d'$ es residuo cuadrático módulo p, por el teorema fundamental de la aritmética tenemos que

$$d' = \prod_{q_i | d'} q_i^{k_i}. \tag{2.8}$$

Por otro lado de (2.7) se tiene que $2p = d'n - 1$, por lo que $2p \equiv -1 \ (mod\ d')$ y de (2.8) tenemos que

$$2p \equiv -1 \ (mod \prod_{q_i | d'} q_i^{k_i}).$$

Así $2p \equiv -1 \ (mod\ q_i)$ y $(p, q_i) = 1$ para todo primo q_i que divide a d'. Retomando los casos con los que iniciamos la demostración, si $n \equiv 1\ o\ 3 \ (mod\ 8)$, entonces $p \equiv 1 \ (mod\ 4)$, así tenemos que el símbolo de Legendre $\left(\dfrac{-1}{p}\right) = 1$, entonces

$$\left(\frac{-d'}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d'}{p}\right) = \left(\frac{d'}{p}\right) = \left(\frac{\prod_{q_i | d'} q_i^{k_i}}{p}\right) = \prod_{q_i | d'} \left(\frac{q_i}{p}\right)^{k_i} = \prod_{q_i | d'} \left(\frac{p}{q_i}\right)^{k_i}.$$

Por otro lado si $n \equiv 5 \ (mod\ 8)$, se tiene que $p \equiv 3 \ (mod\ 4)$ y $d' \equiv 3 \ (mod\ 8)$ pues en este caso $c = 3$ y $d' = 8j + c = 8j + 3$, así tenemos que

$$\begin{aligned} d' &= \prod_{\substack{q_i | d' \\ q_i \equiv 1 \ (mod\ 4)}} q_i^{k_i} \cdot \prod_{\substack{q_i | d' \\ q_i \equiv 3 \ (mod\ 4)}} q_i^{k_i} \\ &\equiv \prod_{\substack{q_i | d' \\ q_i \equiv 1 \ (mod\ 4)}} (1)^{k_i} \cdot \prod_{\substack{q_i | d' \\ q_i \equiv 3 \ (mod\ 4)}} (-1)^{k_i} \\ &\equiv \prod_{\substack{q_i | d' \\ q_i \equiv 3 \ (mod\ 4)}} (-1)^{k_i} \\ &\equiv 3 \ (mod\ 4) \equiv -1 \ (mod\ 4). \end{aligned}$$

Así

$$\prod_{\substack{q_i | d' \\ q_i \equiv 3 \ (mod\ 4)}} (-1)^{k_i} = -1 \tag{2.9}$$

dado que $p \equiv 3 \ (mod\ 4)$ se tiene que el símbolo de Legendre $\left(\frac{-1}{p}\right) = -1$, después, por la ley de reciprocidad cuadrática se tiene que

$$\left(\frac{-d'}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d'}{p}\right) = \left(\frac{d'}{p}\right)$$

así

$$\begin{aligned} -\left(\frac{d'}{p}\right) &= - \prod_{\substack{q_i | d' \\ q_i \equiv 1 \ (mod\ 4)}} \left(\frac{q_i}{p}\right)^{k_i} \cdot \prod_{\substack{q_i | d' \\ q_i \equiv 3 \ (mod\ 4)}} \left(\frac{q_i}{p}\right)^{k_i} \\ &= \prod_{\substack{q_i | d' \\ q_i \equiv 3 \ (mod\ 4)}} \left(\frac{p}{q_i}\right)^{k_i} \cdot \prod_{\substack{q_i | d' \\ q_i \equiv 1 \ (mod\ 3)}} \left(\frac{p}{q_i}\right)^{k_i} \cdot \prod_{\substack{q_i | d' \\ q_i \equiv 3 \ (mod\ 4)}} (-1)^{k_i} \end{aligned}$$

la ultima igualdad se da pues si p, q son primos impares distintos tales que $p \equiv q \equiv 3 \ (mod\ 4)$ entonces $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, recordemos además que por (2.9)

se tiene que

$$\prod_{\substack{q_i|d' \\ q_i\equiv 3 \pmod 4}} (-1)^{k_i} = -1$$

por lo tanto

$$\begin{aligned} -\left(\frac{d'}{p}\right) &= \prod_{\substack{q_i|d' \\ q_i\equiv 1 \pmod 4}} \left(\frac{p}{q_i}\right)^{k_i} \cdot \prod_{\substack{q_i|d' \\ q_i\equiv 3 \pmod 3}} \left(\frac{p}{q_i}\right)^{k_i} \cdot \prod_{\substack{q_i|d' \\ q_i\equiv 3 \pmod 4}} (-1)^{k_i} \\ &= \prod_{\substack{q_i|d' \\ q_i\equiv 3 \pmod 4}} \left(\frac{p}{q_i}\right)^{k_i} \cdot \prod_{\substack{q_i|d' \\ q_i\equiv 1 \pmod 3}} \left(\frac{p}{q_i}\right)^{k_i} \\ &= \prod_{q_i|d'} \left(\frac{p}{q_i}\right)^{k_i}. \end{aligned}$$

Se tiene que $(q_i, p) = 1$ para todos los primos q_i tales que $q_i \mid d'$, entonces $(q_i, 4p) = 1$ y $\left(\dfrac{2^2}{q_i}\right) = 1$, así $\left(\dfrac{p}{q_i}\right)\left(\dfrac{2^2}{q_i}\right) = \left(\dfrac{p}{q_i}\right)$, por lo tanto

$$\left(\frac{p}{q_i}\right) = \left(\frac{p}{q_i}\right)\left(\frac{2^2}{q_i}\right) = \left(\frac{4p}{q_i}\right) = \left(\frac{2}{q_i}\right)\left(\frac{2p}{q_i}\right)$$

luego

$$\left(\frac{-d}{p}\right) = \prod_{q_i|d'} \left(\tfrac{p}{q_i}\right)^{k_i} = \prod_{q_i|d'} \left(\tfrac{2}{q_i}\right)^{k_i} \left(\tfrac{2p}{q_i}\right)^{k_i} = \prod_{q_i|d'} \left(\tfrac{2}{q_i}\right)^{k_i} \cdot \prod_{q_i|d'} \left(\tfrac{-1}{q_i}\right)^{k_i}$$

en los últimos dos productos anteriores, nos interesan los términos en los que $\left(\dfrac{2}{q_i}\right) = -1$, es decir, cuando $q_i \equiv \pm 3 \equiv 3, 5 \ (mod\ 8)$ y los $q_i's$ donde $\left(\dfrac{-1}{q_i}\right) = -1$, es decir cuando q_i es de la forma $q_i = 4k+3$, o equivalentemente $2q_i = 8k + 6$, es decir

$$2q_i \equiv 6 \ (mod\ 8),$$

luego, tenemos que las soluciones de esta congruencia están dadas por

$$q_i \equiv 3, 7 \ (mod\ 8)$$

así

$$\begin{aligned}
\prod_{q_i|d'} \left(\tfrac{2}{q_i}\right)^{k_i} \cdot \prod_{q_i|d'} \left(\tfrac{-1}{q_i}\right)^{k_i} &= \prod_{\substack{q_i|d' \\ q_i\equiv 3 \ (mod\ 8)}} (-1)^{k_i} \cdot \prod_{\substack{q_i|d' \\ q_i\equiv 5 \ (mod\ 8)}} (-1)^{k_i} \\
&\quad \prod_{\substack{q_i|d' \\ q_i\equiv 3 \ (mod\ 8)}} (-1)^{k_i} \cdot \prod_{\substack{q_i|d' \\ q_i\equiv 7 \ (mod\ 8)}} (-1)^{k_i} \\
&\equiv \prod_{\substack{q_i|d' \\ q_i\equiv 5 \ (mod\ 8)}} (-1)^{k_i} \cdot \prod_{\substack{q_i|d' \\ q_i\equiv 7 \ (mod\ 8)}} (-1)^{k_i} \\
&= \prod_{\substack{q_i|d' \\ q_i\equiv 5,7 \ (mod\ 8)}} (-1)^{k_i}
\end{aligned}$$

por lo tanto

$$\left(\frac{-d'}{p}\right) = \prod_{\substack{q_i|d' \\ q_i\equiv 5,7 \ (mod\ 8)}} (-1)^{k_i}.$$

Así para que $-d'$ sea un residuo cuadrático módulo $2p = d'n - 1$, debe cumplirse que

$$\sum_{\substack{q_i|d' \\ q_i\equiv 5,7 \ (mod\ 8)}} k_i \equiv 0 \ (mod\ 2),$$

para demostrar esto consideraremos la descomposición de d' como producto

de primos

$$\begin{aligned} d' &= \prod_{\substack{q_i|d' \\ q_i\equiv 1 \ (mod\ 8)}} q_i^{k_i} \cdot \prod_{\substack{q_i|d' \\ q_i\equiv 3 \ (mod\ 8)}} q_i^{k_i} \cdot \prod_{\substack{q_i|d' \\ q_i\equiv 5 \ (mod\ 8)}} q_i^{k_i} \cdot \prod_{\substack{q_i|d' \\ q_i\equiv 7 \ (mod\ 8)}} q_i^{k_i} \\ &\equiv \prod_{\substack{q_i|d' \\ q_i\equiv 3 \ (mod\ 8)}} 3^{k_i} \cdot \prod_{\substack{q_i|d' \\ q_i\equiv 5 \ (mod\ 8)}} (-3)^{k_i} \cdot \prod_{\substack{q_i|d' \\ q_i\equiv 7 \ (mod\ 8)}} (-1)^{k_i} \ (mod\ 8) \\ &\equiv \prod_{\substack{q_i|d' \\ q_i\equiv 3,5 \ (mod\ 8)}} 3^{k_i} \cdot \prod_{\substack{q_i|d' \\ q_i\equiv 5,7 \ (mod\ 8)}} (-1)^{k_i} \ (mod\ 8). \end{aligned}$$

si $n \equiv 1$ *o* $5\ (mod\ 8)$, entonces $c = 3$ y $d' = 8j + 3 \equiv 3\ (mod\ 8)$, de aquí se sigue que

$$\sum_{\substack{q_i|d' \\ q_i\equiv 3,5 \ (mod\ 8)}} k_i \equiv 1\ (mod\ 2) \tag{2.10}$$

y también

$$\sum_{\substack{q_i|d' \\ q_i\equiv 5,7 \ (mod\ 8)}} k_i \equiv 0\ (mod\ 2). \tag{2.11}$$

Por otro lado, si $n \equiv 3\ (mod\ 8)$, entonces $c = 1$ y $d' = 8j + 1 \equiv 1\ (mod\ 8)$, de aquí se deduce que

$$\sum_{\substack{q_i|d' \\ q_i\equiv 3,5 \ (mod\ 8)}} k_i \equiv 0\ (mod\ 2) \tag{2.12}$$

y

$$\sum_{\substack{q_i|d' \\ q_i\equiv 5,7 \ (mod\ 2)}} k_i \equiv 1\ (mod\ 2) \tag{2.13}$$

entonces, en ambos casos (las pruebas de $(2.10), (2.11), (2.12)$ y (2.13) son directas, aunque muy largas por lo que consideramos es mejor no incluirlas) tenemos que

$$\sum_{\substack{q_i|d' \\ q_i\equiv 5,7 \ (mod\ 8)}} k_i \equiv 0\ (mod\ 2).$$

lo que concluye la prueba. □

Este teorema nos pone de manifiesto que estas progresiones aritméticas de Dirichlet sí se pueden representar como suma de tres cuadrados y en consecuencia podemos adentrarnos en el análisis de los primos que se encuentran en estas progresiones. Pero aún falta analizar una, la progresión $\{8k+7\}$.

En 1798 Adrien-Marie Legendre probó que un entero positivo puede expresarse como la suma de tres cuadrados si y sólo si no es de la forma $4^k(8m+7)$. Este resultado nos permite descartar la posibilidad de que la progresión $\{8k+7\}$ se pueda escribir como suma de tres cuadrados.

En conclusión, de las cuatro progresiones aritméticas de Dirichlet sólo tres se pueden representar como suma de tres cuadrados, ya exhibimos que en el caso $\{8k+7\}$ no es posible.

2.1.3. Suma de cuatro cuadrados y la función $R_{4,2}(n)$

Sabemos que la suma de cuatro cuadrados ya tiene la certeza de que puede representar a cualquier entero positivo, por ende cualquier entero de una progresión aritmética de Dirichlet puede ser representado como suma de cuatro cuadrados. Lagrange demostró el teorema que ahora se enuncia

Teorema (Lagrange 1770)
Para cada entero no negativo n, existen enteros no negativos a, b, c, d tales que

$$n = a^2 + b^2 + c^2 + d^2.$$

La demostración se encuentra en libros de formación inicial de teoría de números, como Rosen [2000], Koshy [2007], entre otros.

De manera natural nos surge la pregunta, porqué la representación como suma de cuatro cuadrados para cada entero positivo en las clases o progresiones tendría que ser única (salvo permutaciones). La respuesta es que no

necesariamente es única, por ejemplo

$$\begin{aligned} 204 &= 5^2 + 7^2 + 7^2 + 9^2 \\ &= 3^2 + 5^2 + 7^2 + 11^2 \\ &= 2^2 + 6^2 + 8^2 + 10^2 \\ &= 1^2 + 3^2 + 5^2 + 13^2 \\ &= 1^2 + 1^2 + 9^2 + 11^2 \\ &= 0^2 + 2^2 + 10^2 + 10^2 \\ &= 0^2 + 2^2 + 2^2 + 14^2 \end{aligned}$$

Definición 2.1. *Para cada entero positivo n definimos la función $R_{4,2}(\_) : \mathbb{N} \cup \{0\} \longrightarrow \mathbb{N}$ como sigue:*

$$R_{4,2}(n) = \left|\{(x_1, x_2, x_3, x_4) \mid x_1, x_2, x_3, x_4 \in \mathbb{N} \cup \{0\} \text{ y } n = x_1^2 + x_2^2 + x_3^2 + x_4^2\}\right|,$$

donde $0 \leqslant x_1 \leqslant x_2 \leqslant x_3 \leqslant x_4$.

De esta manera tenemos que $R_{4,2}(204) = 7$. A continuación presentamos una tabla con los primeros valores de $R_{4,2}(n)$.

n	$R_{4,2}(n)$	n	$R_{4,2}(n)$	n	$R_{4,2}(n)$
0	1	11	1	22	2
1	1	12	2	23	1
2	1	13	2	24	1
3	1	14	1	25	3
4	2	15	1	26	3
5	1	16	2	27	3
6	1	17	2	28	3
7	1	18	3	29	2
8	1	19	2	30	2
9	2	20	2	31	2
10	2	21	2	32	1

Figura 2.1: Primeros valores de la función $R_{4,2}(n)$

Intuitivamente esperaríamos que el comportamiento de la función $R_{4,2}(n)$ fuera caótico, sin embargo la *Figura* 2.2 nos muestra que de hecho el comportamiento de la imagen de la función cantidad de representaciones como

suma de cuatro cuadrados de un entero positivo no resulta ser del todo caótica.

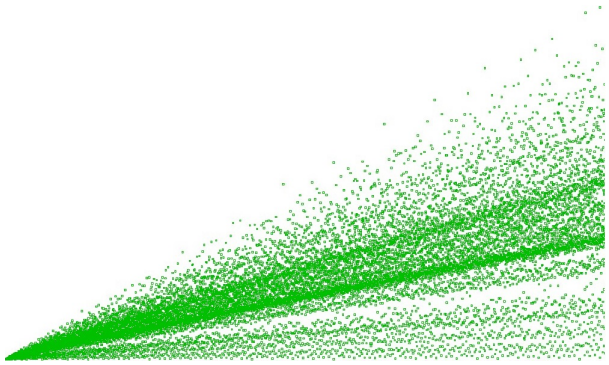

Figura 2.2: Gráfica de la función $R_{4,2}(\_)$ en el intervalo $[0, 15000]$

En el primer apéndice de esta tesis estudiaremos algunas propiedades interesantes que cumple la gráfica de la función $R_{4,2}(n)$.

2.1.4. La imagen de $\mathbb{Z}_4$ bajo la función $R_{4,2}(n)$

En esta sección nos interesa estudiar cómo se comportan las imágenes de las progresiones aritméticas de Dirichlet bajo la función cantidad de representaciones como suma de cuatro cuadrados. Después de hacer una comprobación visual nos percatamos que si adoptábamos el módulo 4 entonces las cuatro clases de equivalencia no presentaban un comportamiento tan impredecible como parecía suceder cuando se graficaba la función completa, por esta razón consideramos más conveniente trabajar con un módulo cuatro. Así, se considera que todos los enteros son de la forma $4k, 4k+1, 4k+2$ ó $4k+3$, y que además existe una infinidad de primos en las progresiones $\{4k+1\}$ y $\{4k+3\}$. Posteriormente veremos la cantidad de representaciones como suma de cuatro cuadrados de los primos contenidos en estas progresiones, es decir, veremos como se ubican dentro de la gráfica de la función $R_{4,2}(\_)$.

Cuando se marcó en la gráfica a los múltiplos de 4, es decir los elementos de la progresión $\{4k\}$, éstos aparecen en su mayoría en la parte media de la gráfica hacia abajo como se muestra a continuación en la *Figura* 2.3.

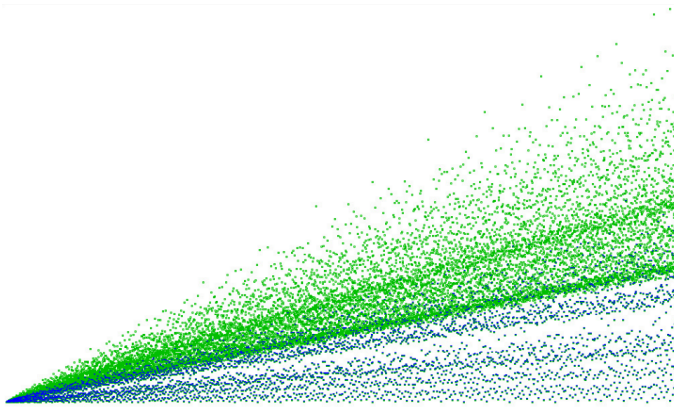

Figura 2.3: En azul la imagen de los elementos de la progresión $\{4k\}$ bajo la función $R_{4,2}(n)$ en el intervalo $[0, 15000]$

Cuando se hace con los enteros de la progresión $\{4k + 1\}$, éstos quedan ubicados principalmente por encima de la parte central de la gráfica como se muestra en la *Figura* 2.4, y es de señalar que la cota inferior se presenta con una definición interesante.

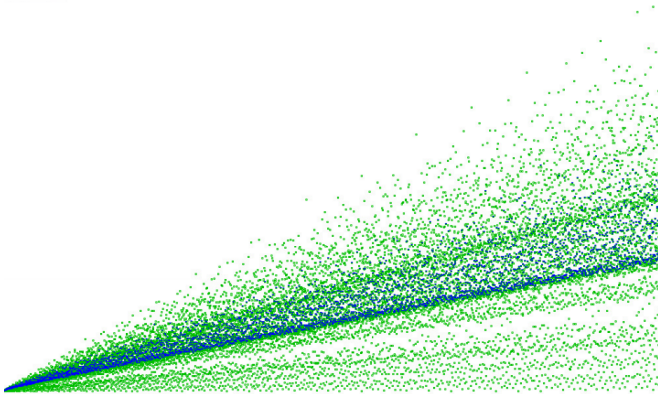

Figura 2.4: En azul la imagen de los elementos de la progresión $\{4k+1\}$ bajo la función $R_{4,2}(n)$ en el intervalo $[0, 15000]$

Los enteros de la progresión $\{4k + 2\}$ tienen sus imágenes de la función cantidad de representaciones ubicados en la parte superior de la gráfica como se muestra en la *Figura* 2.5.

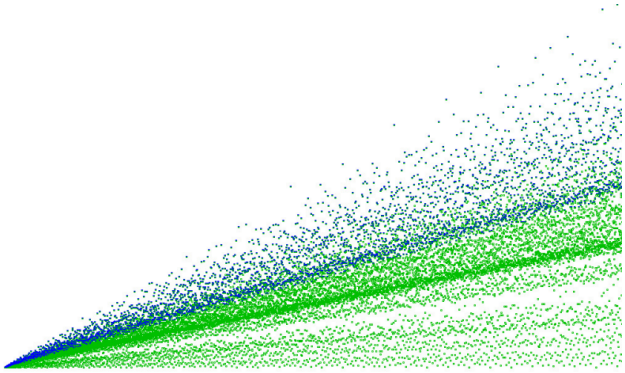

Figura 2.5: En azul la imagen de los elementos de la progresión $\{4k+2\}$ bajo la función $R_{4,2}(n)$ en el intervalo $[0, 15000]$.

Finalmente los enteros de la progresión $\{4k+3\}$ quedan representados cerca de la parte media hacia arriba como se muestra en la *Figura* 2.6, y de manera semejante a los elementos en la progresión $\{4k+1\}$ la cota inferior queda muy bien definida

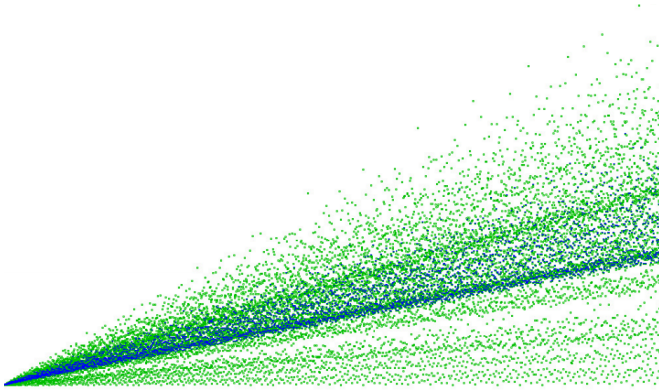

Figura 2.6: En azul la imagen de los números de la forma $4k+3$ bajo la función $R_{4,2}(n)$ en el intervalo $[0, 15000]$.

Ahora analizaremos las cuatro clases de $\mathbb{Z}_4$ y posteriormente nos centraremos sólo en las progresiones aritméticas de Dirichlet y más aún en las imágenes de los primos. Ya expusimos en las cuatro gráficas anteriores que la ubicación de los respectivos conjuntos de imágenes no corresponde a un comportamiento

impredecible, entonces daremos lugar a dar una explicación de porque las imágenes de cada una de las clases de $\mathbb{Z}_4$ están ubicadas en la posición que se nos indicó antes.

Para llevar a cabo un análisis más profundo de la ubicación de la imagen de las progresiones módulo 4, bajo la función $R_{4,2}(n)$, el procedimiento que seguiremos será el de expresar cada clase como suma de cuatro cuadrados, pero a la vez analizaremos que clases de cuadrados son los que se pueden usar en la suma. Por ejemplo veamos el caso de la clase $4k+1$ y que ésta se puede expresar como suma de cuatro cuadrados de la siguiente manera

$$\begin{aligned}
4k+1 &= (4k+1)^2+(4k)^2+(4k)^2+(4k)^2 \\
&= (4k+3)^2+(4k)^2+(4k)^2+(4k)^2 \\
&= (4k+1)^2+(4k+2)^2+(4k+2)^2+(4k+2)^2 \\
&= (4k+1)^2+(4k+2)^2+(4k)^2+(4k)^2 \\
&= (4k+1)^2+(4k+2)^2+(4k+2)^2+(4k)^2 \\
&= (4k+3)^2+(4k+2)^2+(4k+2)^2+(4k+2)^2 \\
&= (4k+3)^2+(4k+2)^2+(4k)^2+(4k)^2 \\
&= (4k+3)^2+(4k+2)^2+(4k+2)^2+(4k)^2
\end{aligned}$$

estas igualdades las podemos expresar en sus equivalencias residuales, pero sin reducirlas módulo 4. Quedan de esta forma:

$$\begin{aligned}
4k+1 &= 1+0+0+0=1 \\
&= 9+0+0+0=9 \\
&= 1+4+4+4=13 \\
&= 1+4+0+0=5 \\
&= 1+4+4+0=9 \\
&= 9+4+4+4=21 \\
&= 9+4+0+0=13 \\
&= 9+4+4+0=17
\end{aligned} \tag{2.14}$$

La sucesión de resultados es $1,5,9,13,17,21$ y son todos.

Para la clase $4k$ se tienen las sumas correspondientes que son:

$$\begin{aligned} 4k &= 0+0+0+0=0 \\ &= 4+4+4+4=16 \\ &= 4+4+0+0=8 \\ &= 4+4+4+0=12 \\ &= 4+0+0+0=4 \\ &= 1+1+1+1=4 \\ &= 9+1+1+1=12 \\ &= 9+9+1+1=20 \\ &= 4+0+0+0=4 \end{aligned} \tag{2.15}$$

Para la clase $4k+2$ es de esta manera:

$$\begin{aligned} 4k+2 &= 1+1+0+0=2 \\ &= 4+1+1+0=6 \\ &= 4+4+1+1=10 \\ &= 4+9+1+0=14 \\ &= 4+4+9+1=18 \\ &= 9+1+0+0=10 \\ &= 9+9+4+0=22 \\ &= 9+9+0+0=18 \\ &= 9+9+4+4=26 \end{aligned} \tag{2.16}$$

Para la clase $4k+3$ se tiene lo siguiente

$$\begin{aligned} 4k+3 &= 1+1+1+0=3 \\ &= 4+1+1+1=7 \\ &= 9+1+1+0=11 \\ &= 9+1+4+0=15 \\ &= 9+9+1+0=19 \\ &= 9+9+4+1=23 \\ &= 9+9+9+0=27 \end{aligned} \tag{2.17}$$

Se puede ver de las gráficas que la clase que menos representaciones tiene es la $4k$ (*Figura* 2.3). Esto se puede explicar a partir de (2.15) ya que las representaciones residuales tienen poca variedad, es decir, la representación de la forma $0+0+0+0$ sólo usa una clase de números que son los $4k$. Por otro lado los de la forma $9+9+1+1$ recurren a dos tipos de números de $\mathbb{Z}_4$, que son los $4k+3$ y $4k+1$. Esta composición lleva a que los $4k$ que tienen dos posibilidades en la representación aditiva como lo es $9+9+1+1$ tengan más representaciones como suma de cuatro cuadrados, que aquéllos que tienen una sola variante, como lo es $0+0+0+0$.

Entonces bajo este razonamiento podemos ver en (2.15) que los $4k$ pueden tener 6 representaciones con dos variantes y tres con ninguna y con este número de posibilidades se generan todas las representaciones de un $4k$ como suma de cuatro cuadrados. En la gráfica (*Figura* 2.3) vemos que los valores de los $4k$ en la función cantidad de representaciones como suma de cuatro cuadrados se encuentran en la clase media baja.

Acto seguido podemos ver que la gráfica de las representaciones de los $4k+2$ (*Figura* 2.5) se encuentran totalmente en la parte superior, pero ¿por qué pasa esto?

La explicación es que entre más variedad tengan los sumandos de cada una de las representaciones de $\mathbb{Z}_4$, entonces más representaciones como suma de cuatro cuadrados tendrán. De lo mencionado se infiere que de (2.16) se extraen cuatro formas con dos variantes, éstas son:

$$1+1+0+0$$
$$4+4+1+1$$
$$9+9+0+0$$
$$9+9+4+4$$

por otro lado se tienen cuatro de tres variantes que son:

$$4+0+1+1$$
$$4+4+9+1$$
$$9+1+0+0$$
$$9+9+4+0$$

y para terminar se tiene una de cuatro variantes que es:

$$4 + 9 + 1 + 0.$$

Esto nos muestra que la clase $4k + 2$ tiene más riqueza en la variedad de las clases que se usan para representarla como suma de cuatro cuadrados, es decir, tiene cuatro formas con dos variantes, cuatro con tres y una con cuatro; para el caso de la clase $4k$ se tienen tres con una variante y seis con dos. En conclusión, la mayor cantidad de variantes en la clase $4k+2$ respecto de la $4k$ hace que la primera tenga más posibilidades en sus representaciones como suma de cuatro cuadrados.

Con este razonamiento se puede entender la distribución de los valores de la función $R_{4,2}(n)$, ver las figuras $(Figura\ 2.3), (Figura\ 2.4), (Figura\ 2.5), (Figura\ 2.6)$.

Si se toma como base del análisis a las sumas de los residuos para extraer a los representantes de $\mathbb{Z}_4$, entonces nuestro problema se reduce a encontrar las sumas con cuatro enteros repetidos o diferentes tomados del conjunto $\{0, 1, 4, 9\}$, y que cada suma genera a las clases de $\mathbb{Z}_4$, como se puede ver en $(3.14), (3.15), (3.16)\ y\ (3.17)$.

Para el caso de la suma de cuatro cuadrados dichas sumas requieren sólo un poco de paciencia con el trabajo de las sumas modulares en $\mathbb{Z}_4$. Con esta herramienta ya podemos explorar la manera en que se distribuyen las imágenes de las progresiones aritméticas de Dirichlet $\{4k + 1\}$ y $\{4k + 3\}$ bajo la función $R_{4,2}(n)$.

Con base en lo anterior podemos proponer una conjetura que atañe a las progresiones aritméticas $\{4k + 1\}$ y $\{4k + 3\}$. Ésta se enuncia así

Conjetura 1: Si $\{p_n\}$ denota la sucesión de primos de la forma $\{4k + 1\}$ y $\{q_n\}$ denota a la sucesión de primos de la forma $\{4k+3\}$ entonces para cada n natural se tiene que $R_{4,2}(p_n) \geqslant R_{4,2}(q_n)$.

Sabemos que las clases mencionadas son las que contienen a todos los primos p impares, para estudiar el comportamiento de los primos bajo la función $R_{4,2}(n)$ necesitamos introducir una función auxiliar.

Definición 2.2. *Para cada n entero no negativo definimos la función*

$$\widehat{\Re}_{4,2}(n) = \left|\{(x_1, x_2, x_3, x_4) \mid x_1, x_2, x_3, x_4 \in \mathbb{N} \cup \{0\} \text{ y } n = x_1^2 + x_2^2 + x_3^2 + x_4^2\}\right|,$$

Notemos que la diferencia fundamental entre las funciones $R_{4,2}$ y $\widehat{\Re}_{4,2}$ consiste en que en la función $\widehat{\Re}_{4,2}$ consideramos soluciones con negativos y ademas consideramos que dada una cuarteta (a, b, c, d) tal que la suma suma de sus cuadrados sea n, entonces las cuartetas formadas por alguna permutacion de esta serán consideradas como una solución distinta de la ecuación.

A continuación se muestra la gráfica de la función $R_{4,2}(n)$ y en rojo se resalta la imagen de los primos. Aquí podemos apreciar que su comportamiento es muy estable, pues se acumulan en la parte central de la gráfica.

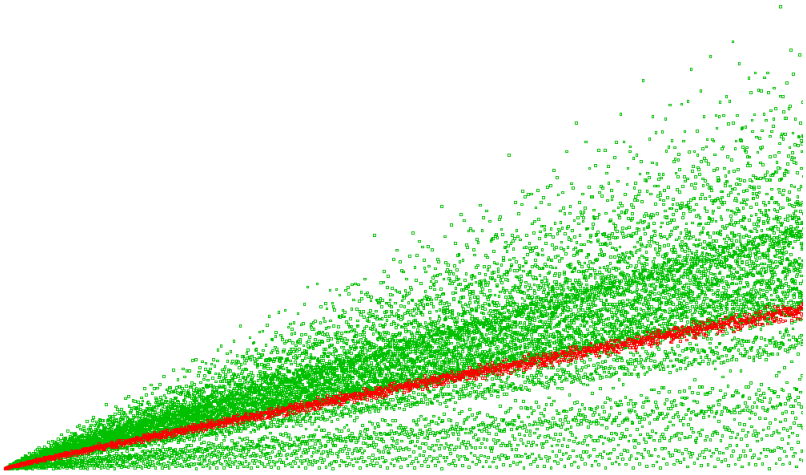

Figura 2.7: En rojo la cantidad de representaciones de los primos como suma de cuatro cuadrados en el intervalo $[0, 15000]$.

Para justificar este hecho, veamos el siguiente resultado

Teorema 2.7. *Para todo primo p se cumple que*

$$R_{4,2}(p) = 8(p+1) - \mathcal{O}(1).$$

Demostración. Para esto partiremos de la fórmula de Jacobi[7], tenemos que

[7] La prueba se puede ver en el artículo [Hirschhorn 1987].

para todo p primo.

$$\widehat{\Re}_{4,2}(p) = 8\sum_{\substack{d|n \\ 4\nmid d}} d = 8(p+1).$$

para obtener el valor de $R_{4,2}$ a partir de $\widehat{\Re}_{4,2}$ tenemos que eliminar las soluciones que están dadas tanto como por una permutacion de otra solución, así como las que tienen algún elemento negativo, las cuales son $\mathcal{O}(1)$, así tenemos el resultado deseado. □

2.2. Sumas de cubos

De manera análoga al caso de cuatro cuadrados, ahora nos planteamos la posibilidad de expresar a cualquier entero como una suma finita de cubos. Fue Waring quien conjeturó que todo entero no negativo puede ser expresado como suma de 9 cubos. En 1912 Wieferich y Kempner demostraron esto y era lógico pensar que sólo para números muy grandes ya sería necesario utilizar los nueve cubos para poder expresarlos, pero esto no resulta ser cierto. Por ejemplo, si consideramos el número 23 tenemos que 3^3 no puede ser parte de su descomposición como suma de cubos pues $3^3 > 23$, así la expresión de 23 como suma de cubos esta formada sólo por potencias de 1 y 2. La representación del número 23 es

$$23 = 2^3 + 2^3 + 1^3 + 1^3 + 1^3 + 1^3 + 1^3 + 1^3 + 1^3.$$

El número siguiente con esta propiedad es

$$239 = 5^3 + 3^3 + 3^3 + 3^3 + 2^3 + 2^3 + 2^3 + 2^3 + 1^3.$$

En [1928] y [1939] L.E. Dickson mejoró este resultado en sus artículos: *Simpler proofs of Waring's theorem on cubes with various generalizations* y *All integers except* 23 *and* 239 *are sums of eight cubes.* respectivamente.

De hecho si $1 \leqslant N \leqslant 40000$ entonces N puede ser expresado como suma de seis cubos no negativos, excepto 23 y 239 y si $N \leqslant 40000$, entonces N es representable como suma de 7 cubos no negativos, excepto

$$15, 22, 56, 114, 167, 175, 186, 212, 231, 238, 303, 364, 420, 428, 454.$$

Más aún, por los artículos de Dickson y Von Sterneck, se prueba que únicamente 121 enteros se representan como suma de 7 cubos y el mayor de ellos es 8042, de esta manera tenemos que si $N > 8042$ entonces N es la suma de 6 cubos no negativos.

El teorema que se refiere a cualquier entero como suma de cubos, es el que ya mencionamos antes que se le atribuye a Wieferich y Kempner. Este se enuncia enseguida.

Teorema (Wieferich-Kempner)
Todo entero no negativo puede ser expresado como suma de 9 cubos no negativos.

El teorema no se demostrará aquí ya que se requieren varios lemas previos además que la demostración del teorema también es extensa, y como vemos que no aportaríamos ninguna variante a la demostración original entonces consideramos que lo más apropiado es revisarla en el libro de Nathanson [1996].

Al igual que en potencias cuadráticas, dado un entero n su representación como suma de nueve cubos no es única, por ejemplo

$$\begin{aligned} 239 &= 5^3 + 3^3 + 3^3 + 3^3 + 2^3 + 2^3 + 2^3 + 2^3 + 1^3 \\ &= 4^3 + 4^3 + 3^3 + 3^3 + 3^3 + 3^3 + 1^3 + 1^3 + 1^3, \end{aligned}$$

así la siguiente definición cobra sentido.

Definición 2.3. *Definimos la función* $R_{9,3} : \mathbb{N} \cup \{0\} \longrightarrow \mathbb{N}$ *como sigue*

$$R_{9,3}(n) = \Big|\{(x_1, x_2, \ldots, x_9) \mid x_1, x_2, \ldots, x_9 \in \mathbb{N} \cup \{0\} \text{ y } n = x_1^3 + x_2^3 + \cdots + x_9^2\}\Big|,$$

donde $0 \leqslant x_1 \leqslant \cdots \leqslant x_9$.

A continuación presentamos una tabla con los primeros valores de $R_{9,3}(n)$

n	$R_{9,3}(n)$	n	$R_{9,3}(n)$	n	$R_{9,3}(n)$
0	1	8	2	16	2
1	1	9	2	17	1
2	1	10	2	18	1
3	1	11	1	19	1
4	1	12	1	20	1
5	1	13	1	21	2
6	1	14	1	22	1
7	1	15	1	23	1

Figura 2.8: Primeros valores de la función $R_{9,3}(n)$

2.2.1. La imagen de $\mathbb{Z}_6$ bajo la función $R_{9,3}(n)$

Análogamente a lo realizado en el caso cuatro cuadrados, en esta sección nos interesa estudiar cómo se comporta la imagen de una progresión aritmética de Dirichlet bajo la función cantidad de representaciones como suma de nueve cubos. Aunque en este caso adoptaremos el módulo 6. Así, se considera que todos los enteros son de la forma $6k, 6k+1, 6k+2, 6k+3, 6k+4$ ó $6k+5$, y que además existe una infinidad de primos en las progresiones $\{6k+1\}$ y $\{6k+5\}$.

La gráfica (*Figura* 2.9) que ahora presentamos nos muestran la función cantidad de representaciones como suma de nueve cubos, para cualquier entero positivo.

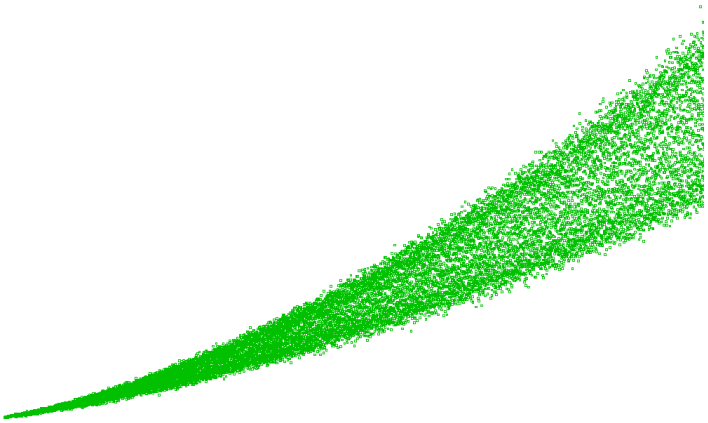

Figura 2.9: Gráfica de la función $R_{9,3}(\_)$ en el intervalo $[0, 15000]$

Acto seguido, veremos la cantidad de representaciones como suma de nueve cubos de los primos (*Figura* 2.10), es decir, veremos cómo se ubican dentro de la gráfica de la función $R_{9,3}(\_)$.

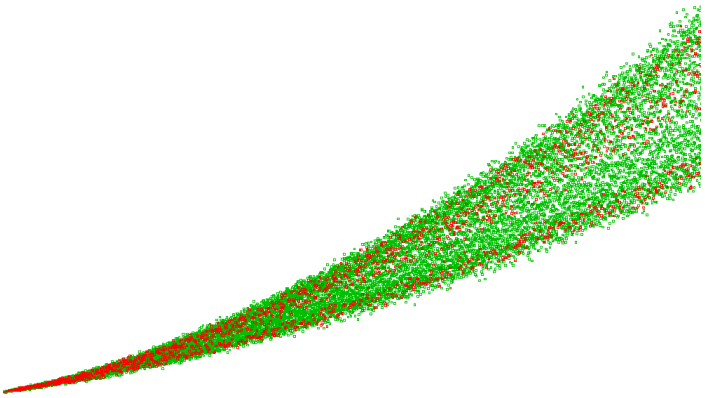

Figura 2.10: En rojo la cantidad de representaciones de los primos como suma de nueve cubos en el intervalo $[0, 15000]$

A continuación presentamos las gráficas (*Figura* 2.11 a *Figura* 2.16) donde se resalta la cantidad de representaciones para cada progresión de $\mathbb{Z}_6$. Primero, se marcó en la gráfica a los múltiplos de seis, es decir los elementos

de la progresión $\{6k\}$ éstos aparecen en su mayoría en la parte media baja y en la parte superior de la gráfica como se muestra a continuación en la *Figura* 2.11.

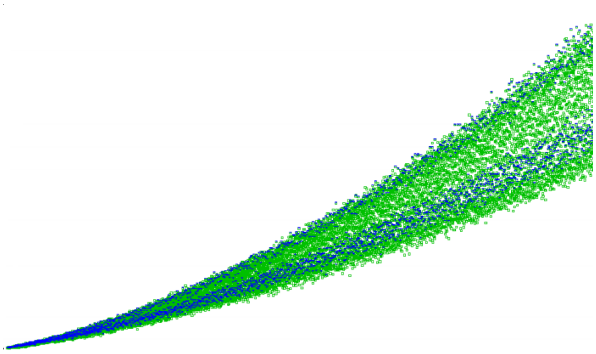

Figura 2.11: En azul la imagen de los elementos de la progresión $\{6k\}$ bajo la función $R_{9,3}(n)$ en el intervalo $[0, 15000]$

Cuando se hace con los enteros de la progresión $\{6k + 1\}$, éstos quedan ubicados en la parte inferior, superior y central de la gráfica como se muestra en la *Figura* 2.12, y es de señalar que esta progresión queda perfectamente distribuida en estas tres regiones de la gráfica.

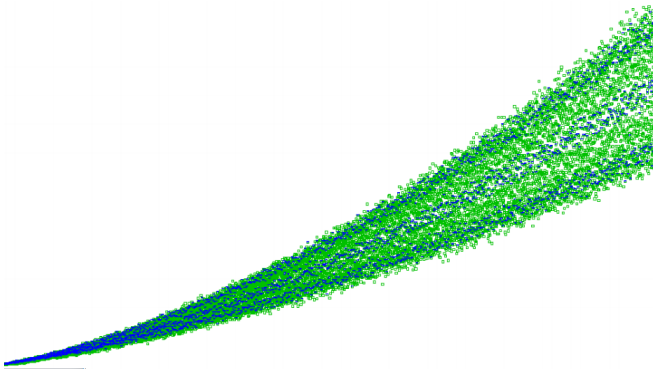

Figura 2.12: En azul la imagen de los elementos de la progresión $\{6k + 1\}$ bajo la función $R_{9,3}(n)$ en el intervalo $[0, 15000]$

Los enteros de la progresión $\{6k+2\}$ tienen sus imágenes de la función cantidad de representaciones ubicados en la parte central hacia arriba, pero sin alcanzar la parte más alta y en la parte inferior de la gráfica como se muestra en la *Figura* 2.13.

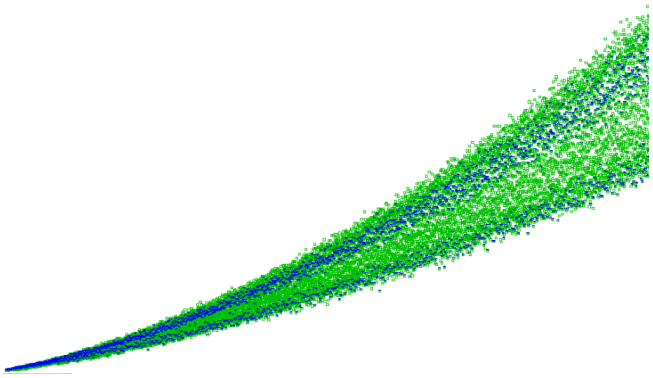

Figura 2.13: En azul la imagen de los elementos de la progresión $\{6k+2\}$ bajo la función $R_{9,3}(n)$ en el intervalo $[0, 15000]$

Los enteros de la progresión $\{6k+3\}$ tienen sus imágenes de la función cantidad de representaciones ubicados en la parte central hacia abajo, pero sin alcanzar la parte más baja y en la parte superior de la gráfica como se muestra en la *Figura* 2.14.

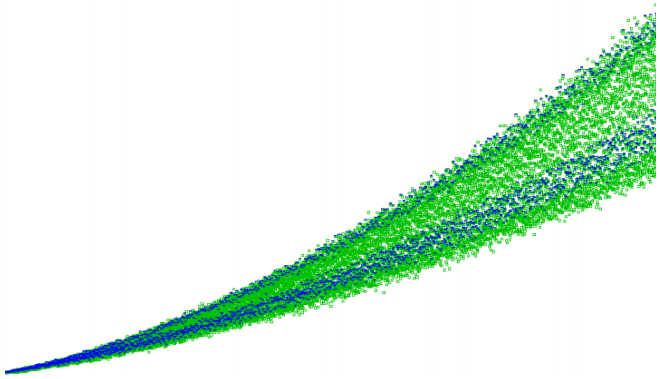

Figura 2.14: En azul la imagen de los elementos de la progresión $\{6k+3\}$ bajo la función $R_{9,3}(n)$ en el intervalo $[0, 15000]$

De manera similar a lo sucedido con los enteros de la progresión $\{6k+1\}$, los enteros de la progresión $\{6k+4\}$ tienen sus imágenes de la función cantidad de representaciones ubicados en la parte inferior, superior y central de la gráfica como se muestra en la *Figura* 2.15

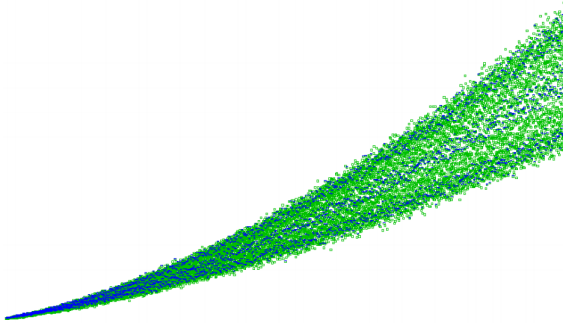

Figura 2.15: En azul la imagen de los elementos de la progresión $\{6k+4\}$ bajo la función $R_{9,3}(n)$ en el intervalo $[0, 15000]$

Finalmente, de manera similar a lo sucedido con los enteros de la progresion $\{6k+2\}$, los enteros de la progresión $\{6k+5\}$ tienen sus imágenes de la función cantidad de representaciones ubicados en la parte central hacia arriba, pero sin alcanzar la parte más alta y en la parte inferior de la gráfica como se muestra en la *Figura* 2.16.

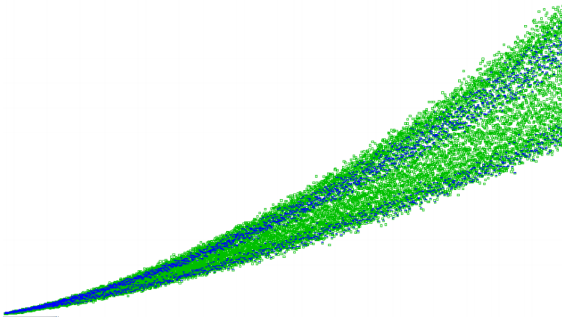

Figura 2.16: En azul la imagen de los elementos de la progresión $\{6k+5\}$ bajo la función $R_{9,3}(n)$ en el intervalo $[0, 15000]$

De manera directa podríamos pasar al estudio de la función cantidad de representaciones como suma de nueve cubos. Este análisis lo podemos hacer a partir de observar el comportamiento de las clases con base en $\mathbb{Z}_6$, pues cada clase queda representada -si se usa este módulo- con una distribución más adecuada bajo la función $R_{9,3}(n)$.

Para construir los conjuntos de representaciones aditivas con base en $\mathbb{Z}_6$ requerimos sumas de nueve cubos para cada número perteneciente a alguna clase de $\mathbb{Z}_6$. Si para el caso de la suma de cuatro cuadrados señalamos que para construir (2.14) a (2.17) se requería principalmente paciencia, ahora para el caso de suma de nueve cubos se requerirá más que eso.

Las sumas para representar a los cuatro cuadrados y nueve cubos módulo 4 y módulo 6 respectivamente se pueden plantear como un problema de particiones. Para el caso suma de cuatro cuadrados las sumas (2.14) a (2.17) son las particiones que se pueden formar con los números $\{0, 1, 4, 9\}$, cada una con cuatro sumandos que pueden ser repetidos o diferentes.

Para cuatro cuadrados ya sabemos que no es difícil encontrar estas particiones. Para el caso de la suma de nueve cubos módulo 6 ya es complicado. Este problema radica en encontrar las particiones con nueve sumandos repetidos o diferentes tomados del conjunto

$$\{0^3 = 0, 1^3 = 1, 2^3 = 8, 3^3 = 27, 4^3 = 64, 5^3 = 125\}.$$

Además, al igual que en el caso de cuatro cuadrados nos interesa saber las variantes en los sumandos, lo que hace aún más complicada la forma de encontrar dichas particiones con nueve sumandos.

Acto seguido, consideramos que lo apropiado es trabajar con una función generadora que nos pueda proporcionar las particiones y las variantes de los sumandos. Dicha función tiene que ser de la forma

$$\prod_{i=1}^{\infty} \left(\frac{1}{1 - x^i} \right)$$

para el caso cuando $i = 1$ se tiene que

$$\frac{1}{1-x} = 1 + x^1 + x^{1+1} + x^{1+1+1} + x^{1+1+1+1} + \cdots$$

cuando $i = 2$ se tiene

$$\frac{1}{1-x^2} = 1 + x^2 + x^{2+2} + x^{2+2+2} + x^{2+2+2+2} + \cdots .$$

Por lo tanto

$$\prod_{i=1}^{\infty} \left(\frac{1}{1-x^i} \right) = (1 + x^1 + x^{1+1} + \cdots)(1 + x^2 + x^{2+2} + \cdots) \cdots ,$$

y este producto infinito de polinomios nos genera las particiones de un entero que contiene tanto sumandos diferentes como repetidos. Es decir, cada término del polinomio resultante es de la forma λx^t, donde λ es la cantidad de particiones de t. Por ejemplo, el término λx^{10} nos indica que hay λ particiones del número 10, algunas de ellas son:

$$9+1, 8+2, 7+3, 1+1+8, 6+2+2, 5+1+1+1+1+1$$

y dichas particiones provienen de los exponentes generados del producto de los términos de los polinomios en

$$\prod_{i=1}^{\infty} \left(\frac{1}{1-x^i} \right).$$

Por ejemplo la partición $2+2+6$ proviene del producto $x^{2+2} \cdot x^6 = x^{2+2+6}$, y de esta manera se obtienen las particiones del número diez, que en total son λ.

Lo que nos interesa son las particiones que mostramos de (2.14) a (2.17) y sus equivalentes para sumas de 9 cubos que se construyen con base en $\mathbb{Z}_6$. Sabemos que para obtener las particiones de (2.14) a (2.17), entonces la función generadora se tiene que usar de la forma:

$$\prod_{i \in \mathcal{C}} \left(\frac{1}{1-x^i} \right)$$

con

$$\mathcal{C} = \{0^2, 1^2, 2^2, 3^2\} = \{0, 1, 4, 9\}.$$

Pero aquí tenemos un problema con el cero, y es que al ser usado como potencia genera un uno en los cálculos, por lo tanto, lo adecuado es usar las

clases residuales $4k+1, 4k+2, 4k+3, 4k+4$, para evitar dicho problema.

Así la función generadora que usaremos es:

$$\prod_{i \in \mathcal{Q}} \left(\frac{1}{1-x^i} \right)$$

con $\mathcal{Q} = \{1^2, 2^2, 3^2, 4^2\} = \{1, 4, 9, 16\}$ y como sólo queremos sumas que contengan cuatro cuadrados, entonces nos restringiremos a polinomios de esta forma

$$\begin{aligned}
&(1 + x^1 + x^{1+1} + x^{1+1+1} + x^{1+1+1+1}) \\
&(1 + x^4 + x^{4+4} + x^{4+4+4} + x^{4+4+4+4}) \\
&(1 + x^9 + x^{9+9} + x^{9+9+9} + x^{9+9+9+9}) \\
&(1 + x^{16} + x^{16+16} + x^{16+16+16} + x^{16+16+16+16}).
\end{aligned}$$

Este producto genera 625 términos, pero la mayoría de ellos nos proporciona particiones de más de cuatro sumandos, que son las que no requerimos, para extraer los términos que forman particiones en los exponentes con sólo cuatro sumandos, agregamos los contadores u, d, t, c como coeficientes en los polinomios, y se plantea ahora como sigue:

$$\begin{aligned}
&(1 + ux^1 + dx^{1+1} + tx^{1+1+1} + cx^{1+1+1+1}) \\
&(1 + ux^4 + dx^{4+4} + tx^{4+4+4} + cx^{4+4+4+4}) \\
&(1 + ux^9 + dx^{9+9} + tx^{9+9+9} + cx^{9+9+9+9}) \\
&(1 + ux^{16} + dx^{16+16} + tx^{16+16+16} + cx^{16+16+16+16}).
\end{aligned}$$

Los sumandos resultantes en este producto son de la forma

$$u^{\alpha_1} d^{\alpha_2} t^{\alpha_3} c^{\alpha_4} x^{\beta},$$

donde algún α_i o todos pueden ser cero.

Las particiones de cuatro términos -que son las que requerimos- estarán indicadas cuando la operación $u\alpha_1 + d\alpha_2 + t\alpha_3 + c\alpha_4$ sea igual a 4.[8]

[8] Como condiciones iniciales para esta operación consideramos que $u = 1, d = 2, t = 3, c = 4$.

Si esta operación es mayor que cuatro, entonces sucede que la partición tiene más de cuatro sumandos, y ya no es de las que requerimos. Además debemos considerar la condición extra que dependiendo de la progresión que deseemos estudiar, β debe ser congruente con $1, 2, 3$ o 4, según sea el caso. Y que debemos estudiar los sumandos del producto cuyo exponente sea menor o igual que 64.

Como nos interesa saber las variantes en los sumandos de la partición, entonces requerimos determinar cuales coeficientes de los señalados $u^{\alpha_1}d^{\alpha_2}t^{\alpha_3}c^{\alpha_4}$ tienen más representaciones diferentes de cero, y eso nos indicará que tienen más riqueza en las clases que los forman, como pasa con las particiones de los números $4k+2$.

De regreso a la suma de nueve cubos, recordemos que nos interesa estudiar porqué los números pertenecientes a las clases de $\mathbb{Z}_6$ tienen una cantidad de representaciones como suma de nueve cubos, como se muestra en las gráficas (*Figura* 2.11 a *Figura* 2.16). Es decir, tratamos de interpretar por qué en los primos se forman cuatro bandas; por qué la imagen bajo la función $R_{9,3}(n)$ de los números de la forma $6k+3$ se divide en dos bandas determinadas como muestra la figura (*Figura* 2.14), y de la misma manera con todas las clases en $\mathbb{Z}_6$ cuyas imágenes bajo la función $R_{9,3}(n)$ se encuentran en dos o tres bandas.

De manera similar a lo realizado en el caso de sumas de cuatro cuadrados, ahora se hace para nueve cubos, pero en $\mathbb{Z}_6$. Como ya se mencionó anteriormente, intentar calcular las particiones residuales es muy complicado, el hecho de operar con nueve cubos como sumandos complica las operaciones.

Por lo señalado ya antes, es adecuado tratar el problema directamente con la función generadora

$$\prod_{i=1}^{\infty}\left(\frac{1}{1-x^i}\right).$$

Para evitar la potencia cero usaremos las clases

$$6k+1, 6k+2, 6k+3, 6k+4, 6k+5, 6k+6,$$

y así se recurrirá al conjunto

$$K = \{1^3 = 1, 2^3 = 8, 3^3 = 27, 4^3 = 64, 5^3 = 125, 6^3 = 216\}$$

y la función generadora es

$$\prod_{i\in K}\left(\frac{1}{1-x^i}\right).$$

Como sólo nos interesan las sumas con nueve cubos entonces nuevamente restringimos los polinomios, pero ahora con diez términos. Así, el producto de polinomios que nos proporcionará las particiones es:

$(1+ux+dx^2+tx^3+cx^4+fx^5+sx^6+zx^7+ox^8+nx^9)$
$(1+ux^8+dx^{16}+tx^{24}+cx^{32}+fx^{40}+sx^{48}+zx^{56}+ox^{64}+nx^{72})$
$(1+ux^{27}+dx^{54}+tx^{81}+cx^{108}+fx^{135}+sx^{162}+zx^{189}+ox^{216}+nx^{243})$
$(1+ux^{64}+dx^{128}+tx^{192}+cx^{256}+fx^{320}+sx^{384}+zx^{448}+ox^{512}+nx^{576})$
$(1+ux^{125}+dx^{250}+tx^{375}+cx^{500}+fx^{625}+sx^{750}+zx^{875}+ox^{1000}+nx^{1125})$
$(1+ux^{216}+dx^{432}+tx^{684}+cx^{864}+fx^{1080}+sx^{1296}+zx^{1512}+ox^{1728}+nx^{1944})$

Los contadores en este caso son u,d,t,c,f,s,z,o,n y ellos nos proporcionan los datos para saber cuales son las particiones residuales que requerimos. Entonces las particiones de nueve sumandos las extraemos de los sumandos que se generan del producto anterior, cuyos sumandos resultantes son de la forma

$$u^{\omega_1}d^{\omega_2}t^{\omega_3}c^{\omega_4}f^{\omega_5}s^{\omega_6}z^{\omega_7}o^{\omega_8}n^{\omega_9}x^{\gamma}$$

y las particiones de γ que tienen nueve sumandos son las que cumplen que

$$u\omega_1+d\omega_2+t\omega_3+c\omega_4+f\omega_5+s\omega_6+z\omega_7+o\omega_8+n\omega_9=9,$$

además como en el caso cuatro cuadrados debemos considerar que dependiendo de la progresión que deseemos estudiar, γ debe ser congruente con $1,2,3,4,5$ o 6 módulo 6, según sea el caso. Y debemos estudiar los sumandos del producto cuyo exponente sea menor o igual que 1994.

Como en el caso de los cuadrados, se toman las condiciones iniciales $u=1,d=2,t=3,c=4,f=5,s=6,z=7,o=8,n=9$ para saber que clases de $\mathbb{Z}_6$ tienen más representaciones como suma de nueve cubos.

2.3. Suma de k-ésimas potencias

No hay duda que el único caso fácil en el que era posible visualizar las representaciones aditivas modulares fue la suma de cuatro cuadrados. Después mostramos que la suma de nueve cubos se complica, y en lo sucesivo será cada vez más difícil, como sería en los casos de la suma de 19 cuartas potencias; 37 quintas potencias y así hasta abordar el problema de Waring que nos plantea que *todo número se puede expresar como suma de $k-$ésimas potencias.*

Cabe notar que el razonamiento utilizado en los casos anteriores (cuatro cuadrados y nueve cubos) no depende de la potencia, es decir que de manera natural podemos extenderlo. Así por medio de las funciones generadoras se puede estudiar la cantidad de representaciones de los elementos de una progresión bajo la función $R_{g(k),k}$[9].

Dada una progresión aritmética de Dirichlet $\{a+bn\}$, para construir la función generadora que nos proporcione la información requerida debemos comenzar por considerar el conjunto

$$A = \{1^k, 2^k, \ldots, a^k\},$$

luego, de manera análoga a lo realizado anteriormente, la función generadora está dada por un producto de la forma

$$\prod_{i \in A} \left(\frac{1}{1-x^i} \right).$$

Como sólo nos interesan los términos con $g(k)$, $k-$ésimas potencias, entonces nos restringimos a los polinomios con $g(k)+1$ términos. Así, el producto de polinomios deseado es:

[9]Definimos $g(k)$ como la cantidad necesaria de sumandos para expresar a todos los enteros como suma de $k-$ésimas potencias, por ejemplo $g(2) = 4$ y $g(3) = 9$.
De manera natural se define $R_{g(k),k}(n)$ como la cantidad de representaciones (sin permutaciones) de n como suma de $k-$ésimas potencias.

$$(1 + u_1 x^{1^k} + u_2 x^{1^k+1^k} + \cdots + u_{g(k)} x^{g(k)})$$
$$(1 + u_1 x^{2^k} + u_2 x^{2^k+2^k} + \cdots + u_{g(k)} x^{g(k)2^k})$$
$$\vdots$$
$$(1 + u_1 x^{a^k} + u_2 x^{a^k+a^k} + \cdots + u_{g(k)} x^{g(k)a^k}).$$

Donde consideramos los contadores $u_1 = 1, u_2 = 2, \ldots, u_{g(k)} = g(k)$ y ellos nos proporcionan los datos para saber cuáles son las particiones residuales que requerimos. Aunque como mencionamos anteriormente los cálculos a partir de $k = 4$ se vuelven inmanejables, y por esta razón se tiene que calcular a través de medios computacionales, en nuestro caso usamos Mathematica para las sumas de cubos y cuadrados.

Existe una manera distinta de estimar la cantidad de representaciones como suma de $k-$ésimas potencias, ésta es a través de fórmulas asintóticas obtenidas mediante el uso de ingeniosas técnicas del análisis complejo. Hardy y Ramanujan desarrollaron el ahora conocido método del círculo utilizado para aproximar la cantidad de representaciones de los enteros como sumas de elementos de una base aditiva dada.[10]

Como caso particular Hardy y Littlewood utilizaron el método del círculo para estimar la cantidad de representaciones de un entero como suma de k-ésimas potencias. Más adelante Vinogradov mejoró este resultado utilizando su método de sumas trigonométricas, con una variante en la que no se consideran permutaciones y puede ser escrito de la siguiente manera[11].

[10] Sea B un subconjunto propio y no vacío de los naturales. Definimos

$$rB = \{b_1 + b_2 + \cdots + b_r \mid b_i \in B\}$$

como el conjunto formado por todos los números que pueden ser expresados como suma de r elementos de B, decimos que B es una base aditiva si existe un r tal que $rB = \mathbb{N}$.

[11] Aunque en este caso no estimamos la cantidad de representaciones como suma de $k-$ésimas potencias de los enteros clasificados de acuerdo a una clase residual.

Teorema Para todo $k \geqslant 2$ que cumple la conjetura de Euler[12], y para cada primo p el número de soluciones enteras no negativas contadas sin permutaciones de la ecuación

$$p = x_1^k + \cdots + x_{g(k)}^k$$

está dado por

$$R_{g(k),k}(p) = \wp(p)\frac{\Gamma^{g(k)}\left(1+\frac{1}{k}\right)}{\Gamma\left(\frac{g(k)}{k}\right)}p^{g(k)/k-1} + \mathcal{O}(p^{g(k)/k-1-\delta}),$$

donde $\delta = \delta(g(k),k) > 0$, $\Gamma(x) = \displaystyle\int_0^\infty e^{-x}t^{x-1}dt$ es la función Γ de Euler y $\wp(p)$ es la serie singular asociada al problema de Waring, que se define de la siguiente manera

$$\wp(p) = \sum_{q=1}^{\infty}\sum_{\substack{a=1\\(a,q)=1}}^{q}\left(\frac{S(q,a)}{q}\right)^{g(k)}e\left(\frac{-pa}{q}\right)$$

donde $S(q,a) = \displaystyle\sum_{r=1}^{q} e(ar^k/q)$ y $e(x) = e^{2\pi ix}$.

[12]Euler conjeturó que $g(k) = 2^k + [(3/2)^k] - 2$, lo cual actualmente se sabe que se cumple para una infinidad de valores.

Capítulo 3

Apéndices

Como mencionamos anteriormente consideramos que es importante estudiar algunas características de las gráficas de las funciones cantidad de representaciones como suma de cuadrados o cubos según sea el caso. En esta sección estudiaremos cuándo existen una infinidad de enteros con una única representación como suma de $k-$ésimas potencias.

Dicho de otra manera estudiaremos para qué valores de k, se cumple que $R_{g(k),k}(n) = 1$ para una infinidad de enteros n.

Cuadrados

Ya se expuso antes que dado un entero m no necesariamente su representación como suma de cuatro cuadrados es única. Entonces surge la pregunta ¿existirá una infinidad de enteros m tales que su representación como suma de cuatro cuadrados es única?

Teorema 3.1. *Si m se escribe de manera única como suma de cuatro cuadrados pares, entonces $(2^2)^k m$ se escribe de manera única como suma de cuatro cuadrados, dicho de otra manera si $m = a^2 + b^2 + c^2 + d^2$, con a, b, c, d pares y $R_{4,2}(m) = 1$, entonces $R_{4,2}((2^2)^k m) = 1$.*

Demostración. Procederemos por inducción sobre k.
Veamos que el resultado es válido para $k = 1$. Supongamos que $m = m_1^2 + m_2^2 + m_3^2 + m_4^2$ con $m_i = 2\alpha_i$ para $i = 1, 2, 3, 4$ y $R_{4,2}(m) = 1$,

luego tenemos que

$$\begin{aligned} 4m &= 2^2 m = 2^2(m_1^2 + m_2^2 + m_3^2 + m_4^2) \\ &= (2m_1)^2 + (2m_2)^2 + (2m_3)^2 + (2m_4)^2, \end{aligned}$$

es decir $4m$ se escribe como suma de cuatro cuadrados pares. Aplicando contrapuesta tenemos que si los cuadrados que aparecen en la representación como suma de cuatro cuadrados de $4m$ no son todos pares, entonces los cuadrados en la representación de m no son todos pares. Lo cual por hipótesis no puede pasar, es decir los cuadrados que aparecen en la representación de $4m$ son todos pares. Veamos que ésta es la única representación de $4m$ como suma de cuatro cuadrados. Supongamos que

$$4m = z_1^2 + z_2^2 + z_3^2 + z_4^2,$$

luego, todos los z_i *para* $i = 1, 2, 3, 4$ son pares, como $z_i = 2\vartheta_i$ *para* $i = 1, 2, 3, 4$. Entonces, tenemos que

$$\begin{aligned} &4(\vartheta_1^2 + \vartheta_2^2 + \vartheta_3^2 + \vartheta_4^2) \\ &= (2\vartheta_1)^2 + (2\vartheta_2)^2 + (2\vartheta_3)^2(2\vartheta_4)^2 \\ &= z_1^2 + z_2^2 + z_3^2 + z_4^2 \\ &= 4m \\ &= (2m_1)^2 + (2m_2)^2 + (2m_3)^2 + (2m_4)^2 \\ &= 4(m_1^2 + m_2^2 + m_3^2 + m_4^2) \end{aligned}$$

es decir, $m_i = \vartheta_i$ para $i = 1, 2, 3, 4$. Así tenemos que $z_i = 2\vartheta_i = 2m_i$ para $i = 1, 2, 3, 4$, es decir $R_{4,2}(4m) = 1$.

Supongamos que el resultado es válido para k, es decir m se representa como suma de cuatro cuadrados de manera única como sigue

$$4^k m = (2^k m_1)^2 + (2^k m_2)^2 + (2^k m_3)^2 + (2^k m_4)^2.$$

Veamos que se cumple para $k + 1$.
Tenemos que

$$\begin{aligned} 4^{k+1} m &= (2^2)^{k+1} m \\ &= (2^2)^{k+1}(m_1^2 + m_2^2 + m_3^2 + m_4^2) \\ &= (2^{k+1})^2(m_1^2 + m_2^2 + m_3^2 + m_4^2) \\ &= (2^{k+1}m_1)^2 + (2^{k+1}m_2)^2 + (2^{k+1}m_3)^2 + (2^{k+1}m_4)^2 \end{aligned}$$

veamos que ésta es la única representación como suma de cuatro cuadrados de $4^{k+1}m$, supongamos que existen z_1, z_2, z_3, z_4 tales que

$$4^{k+1}m = z_1^2 + z_2^2 + z_3^2 + z_4^2,$$

por un argumento análogo al dado en el la base de inducción, tenemos que $z_i = 2\Theta_i$ para $i = 1, 2, 3, 4$, entonces

$$\begin{aligned} 4(4^k)m = 4^{k+1}m &= z_1^2 + z_2^2 + z_3^2 + z_4^2 \\ &= (2\Theta_1)^2 + (2\Theta_2)^2 + (2\Theta_3)^2 + (2\Theta_4)^2 \\ &= 4(\Theta_1^2 + \Theta_2^2 + \Theta_3^2 + \Theta_4^2) \end{aligned}$$

luego

$$4^k m = \Theta_1^2 + \Theta_2^2 + \Theta_3^2 + \Theta_4^2$$

así, por hipótesis de inducción tenemos que $\Theta_i = 2^k m_i$ para $i = 1, 2, 3, 4$, así se tiene que

$$z_i = 2\Theta_i = 2(2^k m_i) = 2^{k+1} m_i,$$

por lo tanto esta representación es única. □

Corolario 3.2. *Existe una infinidad de enteros m, que tienen una única representación como suma de cuatro cuadrados, dicho de otra manera existen una infinidad de enteros m tales que $R_{4,2}(m) = 1$.*

Demostración. Notemos que $2^{2+1} = 8$ se escribe de manera única como suma de cuatro cuadrados pares ($8 = 2^2+2^2+0^2+0^2$), luego por el teorema anterior tenemos que $R_{4,2}(4^k 8) = 1$ para todo $k \in \mathbb{N}$. □

Cubos

Nos interesa describir el comportamiento de la gráfica de la función $R_{9,3}(n)$, para esto partiremos del siguiente resultado.

Teorema (Fermat)

Para todo $k \geqslant 1$, existen enteros N y k pares disjuntos de enteros $\{x_i, y_i\}$ tales que

$$N = x_i^3 + y_i^3.$$

La prueba se pude ver en Nathanson [1996]

Corolario 3.3. *Se cumple que*

$$\limsup_{n\to\infty} R_{9,3}(n) = \infty.$$

Demostración. Notemos que si x^3+y^3 es una representación de n como suma de dos cubos, entonces

$$n = x^3 + y^3 + 0^3 + 0^3 + 0^3 + 0^3 + 0^3 + 0^3 + 0^3$$

y así por el teorema anterior tenemos el resultado deseado. □

Esto implica que la gráfica de la función $R_{9,3}(n)$ no es acotada, mas aún, se cumple el siguiente resultado

Teorema 3.4. *No existe* $\mathcal{A} \subseteq \mathbb{N}$ *tal que* $|\mathcal{A}| = \infty$ *y* $\forall a \in \mathcal{A}$ $R_{9,3}(a) = s$, *para algún* $s \in \mathbb{N}$ *fijo.*

Demostración. Sea $s \in \mathbb{N}$ fijo y supongamos que existe $\mathcal{A}$ que cumple lo pedido. Ahora, por el teorema de Fermat, existe $m \in \mathbb{N}$ tal que $\forall n \geqslant m$ se tiene que $R_{9,3}(n) > s$, pero $|\{1, 2, \ldots, m\}| = m < \infty$ y $|\mathcal{A}| = \infty$, entonces existe $a \in \mathcal{A}$ tal que $a > m$, luego por hipótesis

$$R_{9,3}(a) = s,$$

lo cual es absurdo. □

De este modo existe $k \in \mathbb{N}$ tal que $\forall s \geqslant k$ se tiene que $R_{9,3}(s) > 1$, así a diferencia del caso cuatro cuadrados tenemos el siguiente resultado

Corolario 3.5. *Existe una cantidad finita de enteros* n, *tales que*

$$R_{9,3}(n) = 1.$$

Demostración. Inmediata por el teorema anterior □

La pregunta que resulta interesante es determinar a partir de qué punto, pasa esto. computacionalmente tenemos que en el intervalo $[0, 50000]$ el entero más grande que tiene una única representación como suma de nueve cubos es el 53, todo esto nos lleva a la siguiente conjetura

Conjetura 2: Los únicos enteros que tienen una única representación como suma de nueve cubos son

$$1 - 7, 10 - 26, 31, 38, 39, 45, 46, 47, 50, 52, 53$$

K-ésimas

Podemos ir más allá y de manera análoga a lo realizado en cuadrados preguntarnos ¿para qué valores de k existe una infinidad de enteros que se escriben de manera única como suma de $k-$ésimas potencias? Para responder este cuestionamiento partiremos del siguiente resultado.

Teorema 3.6. *Si m tiene s representaciones como suma de k-esimas potencias pares, entonces $(2^k)^n m$ tiene s representaciones como suma de k esimas potencias para todo $n \in \mathbb{N}$. Dicho de otra manera si $R_{g(k),k}(m) = s$ y todos las potencias que aparecen en la representación de m son pares, entonces $R_{g(k),k}((2^k)^n m) = s$. para todo $n \in \mathbb{N}$.*

Demostración. Es claro que si $v_1^k + v_2^k + \cdots + v_{g(k)}^k = m$ entonces

$$(2^n v_1)^k + (2^n v_2)^k + \cdots + (2^n v_{g(k)})^k = (2^k)^n m,$$

es decir si $\overline{v} = (v_1, v_2, \ldots, v_{g(k)})$ es solución de la ecuación

$$m = x_1^k + x_2^k + \cdot + x_{g(k)}^k$$

entonces $2^n \overline{v}$ es solución de la ecuación

$$(2^n)^k m = x_1^k + x_2^k + \cdot + x_{g(k)}^k$$

entonces[1]

$$2^n Sol_{g(k),k}(m) \subseteq Sol_{g(k),k}(2^n m).$$

Veamos que

$$Sol_{g(k),k}(2^n m) \subseteq 2^n Sol_{g(k),k}(m).$$

Supongamos que

$$\begin{aligned} m &= m_{1,1}^k + m_{1,2}^k + m_{1,3}^k + \cdots + m_{1,g(k)}^k \\ &= m_{2,1}^k + m_{2,2}^k + m_{2,3}^k + \cdots + m_{2,g(k)}^k \\ &\vdots \\ &= m_{s,1}^k + m_{s,2}^k + m_{s,3}^k + \cdots + m_{s,g(k)}^k \end{aligned}$$

[1] $Sol_{g(k),k}(n) = \{(v_1, \ldots, v_{g(k)}) \mid n = v_1^k + \cdots + v_{g(k)}^k \text{ y } 0 \leqslant v_1 \leqslant \ldots \leqslant v_{g(k)} \in \mathbb{N} \cup \{0\}\}$

son todas las representaciones de m como suma de k-esimas potencias, donde $m_{i,j} = 2\Theta_{i,j}$ para $1 \leqslant i \leqslant s$ y $1 \leqslant j \leqslant g(k)$, luego para $n = 1$ tenemos que si

$$2^k m = z_1^k + z_2^k + \cdots + z_{g(k)}^k$$

entonces $z_i = 2\sigma_i$ para $i = 1, 2, \ldots, g(k)$, así tenemos que

$$\begin{aligned} 2^k m &= (2\sigma_1)^k + (2\sigma_2)^k + \cdots + (2\sigma_{g(k)})^k \\ &= 2^k(\sigma_1^k + \sigma_2^k + \cdots + \sigma_{g(k)}^k), \end{aligned}$$

luego

$$m = \sigma_1^k + \sigma_2^k + \cdots + \sigma_{g(k)}^k$$

así existe $r \in \{1, 2, 3, \ldots, s\}$ tal que

$$\sigma_\alpha = m_{r,\alpha} \; para \; \alpha = 1, 2, \ldots, g(k)$$

entonces

$$2^k \sigma_\alpha = 2^k m_{r,\alpha}$$

y así

$$z_\alpha = 2^k m_{r,\alpha}$$

para alguna $r \in \{1, 2, 3 \ldots, s\}$ y para todo $\alpha \in \{1, 2, 3, \ldots, g(k)\}$.
Supongamos que el resultado es valido para n, es decir que todas las representaciones como suma de $k-$esimas potencias de $(2^k)^n m$ están dadas por

$$\begin{aligned} (2^k)^n m &= (2^n m_{1,1})^k + (2^n m_{1,2})^k + (2^n m_{1,3})^k + \cdots + (2^n m_{1,g(k)})^k \\ &= (2^n m_{2,1})^k + (2^n m_{2,2})^k + (2^n m_{2,3})^k + \cdots + (2^n m_{2,g(k)})^k \\ &\vdots \\ &= (2^n m_{s,1})^k + (2^n m_{s,2})^k + (2^n m_{s,3})^k + \cdots + (2^n m_{s,g(k)})^k. \end{aligned}$$

Supongamos además que

$$(2^k)^{n+1} = \omega_1^k + \omega_2^k + \cdots + \omega_{g(k)}^k$$

luego $\omega_i = 2\zeta_i$ para $i = 1, 2, 3, \ldots, g(k)$. Tenemos entonces que

$$\begin{aligned} 2^k (2^k)^n m &= (2^k)^{n+1} m \\ &= (2\zeta_1)^k + (2\zeta_2)^k + (2\zeta_3)^k + \cdots + (2\zeta_{g(k)})^k \\ &= 2^k(\zeta_1^k + \zeta_2^k + \zeta_3^k + \cdots + \zeta_{g(k)}^k) \end{aligned}$$

por lo tanto

$$(2^k)^n m = \zeta_1^k + \zeta_2^k + \zeta_3^k + \cdots + \zeta_{g(k)}^k$$

así por hipótesis de inducción tenemos que

$$\zeta_\alpha = 2^n m_{r,\alpha} \textit{ para algun } r \in \{1, 2, 3 \ldots, s\} \textit{ y } \alpha = 1, 2, 3, \ldots, g(k).$$

luego

$$\omega_\alpha = 2\zeta_\alpha = 2^{n+1} m_{r,\alpha} \textit{ para algun } r \in \{1, 2, 3 \ldots, s\} \textit{ y } \alpha = 1, 2, 3, \ldots, g(k).$$

□

Demostrado esto entonces bastaría con mostrar un entero m que tenga una única representación como suma $k-$ésimas potencias y a partir de él construir una infinidad.

Teorema 3.7. *Para todo $k \neq 3$ que satisfaga la conjetura de Euler, el número $n = 2^{k+1}$se escribe de manera única como suma de $k-$ésimas potencias.*

Demostración. Tenemos que

$$2^{k+1} = 2^k + 2^k + 0^k \cdots + 0^k,$$

Ahora veamos que ésta es la única representación de n como suma de $k-$ésimas potencias. Tenemos que $3^k > 2^{k+1}$, luego 3^k no puede ser parte de la descomposición de 2^{k+1} como suma de $k-$ésimas potencias, por otro lado supongamos que

$$2^{k+1} = 1_1^k + 1_2^k + \cdots + 1_{g(k)}^k = g(k),$$

así

$$2^{k+1} = g(k) = 2^k + \left[(3/2)^k\right] - 2 < 2^k + \left(3/2\right)^k$$

entonces

$$2^{k+1} - 2^k < (3/2)^k,$$

es decir

$$2^k < (3/2)^k$$

lo cual es absurdo, por lo que la descomposición como suma de $k-$ésimas potencias de 2^{k+1} no puede estar formada por únicamente potencias de uno.

Finalmente supongamos que

$$2^{k+1} = 2^k + 1_1^k + \cdots + 1_{g(k)-1}^k = 2^k + g(k) - 1$$

luego

$$g(k) = 2^k + 1$$

así

$$2^k + \left[(3/2)^k\right] - 2 = 2^k + 1$$

es decir

$$\left[(3/2)^k\right] = 3$$

lo cual es imposible por hipótesis[2]. □

Corolario 3.8. *Para todo $k \neq 3$ que satisfaga la conjetura de Euler, existen una infinidad de enteros con una única representación como suma de $k-$ésimas potencias.*

Demostración. Sea $m = 2^{k+1}$, entonces $R_{g(k),k}((2^k)^n m) = 1$ para todo n natural. □

[2]Sea $f(x) = [x]$ y $g(x) = (3/2)^x$, entonces f es no decreciente y g es creciente, así tenemos que $(f \circ g)(x)$ es una función no decreciente, por otro lado

$$\left[(3/2)^4\right] = \left[(81/16)\right] = 5 > \left[(3/2)^3\right] = 3,$$

así para todo $k \geqslant 4$ se tiene que $\left[(3/2)^k\right] \geqslant \left[(3/2)^4\right] > 3$ y también $\left[(3/2)^2\right] = 2$, así para todo $k \neq 3$ se tiene que $\left[(3/2)^k\right] \neq 3$.

Bibliografía

[1] Apostol. T. M. 2002. *Introducción a la teoría analítica de números.* España: Editorial Reverte.

[2] Dickson, L.E. 1928. *Simpler proofs of Waring's theorem on cubes with various generalizations.* Transactions of the American Mathematical Society, Vol. 30, No. 1, pp. 1-18.

[3] Dickson, L. E. 1939. *All integers except 23 and 239 are sums of eight cubes.* Transactions of the American Mathematical Society, pp. 588-591.

[4] Dirichlet, P. G. L. 1999. *Lectures on number theory.* Con un suplemento de R. Dedekind. American Mathematical Society. Serie History of Mathematics. Volumen 16.

[5] Ferraro, G. 2008. *The rise and development of the theory of series up to the early 1820s.* New York: Springer-Verlag

[6] Hirschhorn, M. D. 1987. *A simple proof of Jacobi's four-square theorem.* Proceedings of the American Mathematical Society. **101**, No. 3, pp. 436-438

[7] Koshy, Thomas, 2007. *Elementary Number Theory with Applications.* Estados Unidos de América: Academic Press, Segunda Edición.

[8] Montgomery, H. 2007. *Multiplicative number theory, I. Classical theory.* Cambridge University Press.

[9] Nathanson, M. B. 1996 *Aditive number theory the classical bases.* New York: Springer Verlag.

[10] Rosen, Kenneth H. 2010. *Elementary Number Theory and Its Application.* Ed. Pearson 6th Edition.

[11] Tattersall, J. J. 2005. *Elementary number theory in nine chapters.* New York: Cambridge University Press. Second edition.

[12] Zaldivar F. 2006. *Introducción a la teoría de grupos.* Sociedad Matemática Mexicana. Serie Aportaciones Matetemáticas. No. 32. México.

[13] Zaldivar, F. 2008. *Productos de Euler.* Sociedad Matemática Mexicana. Serie Miscelánea Matemática **46**: 49-72.