UNIVERSIDAD DE LA RIOJA

TRABAJO FIN DE ESTUDIOS

Título

Primos en progresiones aritméticas

Autor/es

ELINA MALTSEVA

Director/es

JUAN LUIS VARONA MALUMBRES

Facultad

Facultad de Ciencia y Tecnología

Titulación

Grado en Matemáticas

Departamento

MATEMÁTICAS Y COMPUTACIÓN

Curso académico

2020-21

publicaciones.unirioja.es
E-mail: publicaciones@unirioja.es

UNIVERSIDAD DE LA RIOJA

Facultad de Ciencia y Tecnología

TRABAJO FIN DE GRADO

Grado en Matemáticas

Primos en progresiones aritméticas

Realizado por:

Elina Maltseva

Tutelado por:

Juan Luis Varona Malumbres

Logroño, marzo de 2021

PRIMOS EN PROGRESIONES ARITMÉTICAS

Autora: Elina Maltseva
Tutor: Juan Luis Varona Malumbres

Grado en Matemáticas
Facultad de Ciencia y Tecnología
Universidad de La Rioja

Curso académico: 2020/2021

Resumen

En este trabajo hacemos un recorrido desde la prueba realizada por Euclides en el año 300 a.C. de la existencia de infinitos números primos hasta la conjetura de Bunyakowsky, a día de hoy sin demostrar, que establece que, bajo tres condiciones, una función entera polinomial de grado $m > 1$ genera infinitos números primos.

Comenzamos el trabajo dando unas primeras definiciones generales, que nos ayudarán a introducirnos en el tema, seguidas de una breve introducción histórica. Continuaremos con la demostración del teorema de Euclides y con ella deduciremos un principio que se puede aplicar para demostrar la infinitud de números primos de cierta forma. Pero también veremos y demostraremos los límites de este principio, el cual denominaremos demostración euclidiana y observaremos que sirve para demostrar la existencia de infinitos números primos en progresiones como $4n - 1$, pero que falla para progresiones como, por ejemplo, $5n + 2$. A lo largo del capítulo 4, nos adentraremos en los conceptos que nos servirán para comprender la demostración del teorema de Dirichlet, la cual veremos en el penúltimo capítulo de esta memoria. La prueba del teorema que presentaremos es la realizada por Harold S. Shapiro, que hace uso de un resultado dado y demostrado por Franz Mertens en el año 1874, que también probaremos en este capítulo.

Finalizaremos el trabajo dando dos generalizaciones del teorema de Dirichlet, por un lado extenderemos el concepto de número primo a los ideales primos, relacionando este concepto con el teorema de densidad de Chebotarev. Por el otro, lo generalizaremos hacia la ya mencionada conjetura de Bunyakowsky.

Palabras clave: Teorema de Dirichlet, Primo, Progresión aritmética, teorema de Euclides, Demostración euclidiana, Función aritmética, Convolución, Teorema de Mertens, Teorema de Shapiro, Caracteres de Dirichlet.

Summary

In this work, we trace from the proof made by Euclid in the year 300 B.C. of the existence of infinite prime numbers to Bunyakowsky's conjecture, still unproven today, which establishes that, under three conditions, a polynomial integer function of degree $m > 1$ generates infinite prime numbers.

We begin the work giving some first general definitions, which will help us to introduce ourselves in the subject, followed by a brief historical introduction. We will continue with the demonstration of Euclid's theorem and with it we will deduce a principle that can be applied to prime numbers in a certain way. But we will also see and demonstrate the limits of this principle, which we will call Euclidean proof and we will observe that it serves to demonstrate the existence of infinite prime numbers in progressions like $4n - 1$, but that it fails for progressions like, for example, $5n + 2$.

Throughout the chapter 4, we will already go into the concepts that will serve us to understand the proof of Dirichlet's theorem, which we will see in the penultimate chapter of this report. The proof of the theorem that we will present is the one made by Harold S. Shapiro, it makes use of a result given and demonstrated by Franz Mertens in the year 1874, that we will also proof in this chapter.

We will finish the work giving two generalizations of Dirichlet's theorem, on one hand we will extend the concept of prime number to the prime ideals, relating this concept with Chebotarev's density theorem. On the other hand, we will generalize it towards the already mentioned conjecture of Bunyakowsky.

Keywords: Dirichlet theorem, Prime Numbers, Arithmetic Progression, Euclidean Theorem, Euclidean Proof, Arithmetic Function, Convolution, Mertens Theorem, Shapiro Theorem, Dirichlet Characters.

Índice general

Capítulo 1

Introducción

La mayor parte de la información de esta memoria fue obtenida del libro *Introducción a la teoría analítica de números* de T. M. Apostol [1]. Si se quiere profundizar más en el tema de los números primos en progresiones aritméticas, en los primos o en la teoría analítica de números en general, es un libro muy interesante para hacerlo.

La idea de este trabajo es demostrar la existencia de infinitos primos en cualquier progresión aritmética, un teorema enunciado y demostrado por Lejeune Dirichlet en el año 1837, lo enunciamos a continuación.

Teorema de Dirichlet. *Si* p, q *son enteros positivos tales que* $\mathrm{mcd}(p, q) = 1$*, entonces la progresión aritmética* $p, p+q, p+2q, \dots$ *contiene infinitos primos.*

En este primer capítulo vamos a definir los conceptos de número primo y de progresión aritmética, entre otros, seguidos de una breve introducción histórica.

1.1. Primeras definiciones

Antes de comenzar con las primeras definiciones, hagamos algunas observaciones acerca de la **notación** seguida a lo largo de este trabajo. Los números naturales son los pertenecientes al conjunto $\{1, 2, 3, \dots\}$, es decir, no vamos a considerar al 0 natural. Este conjunto se representará mediante $\mathbb{N}$. En caso de que querramos incluir al 0, lo denotaremos como $\mathbb{N}_0$. El conjunto de los enteros por $\mathbb{Z}$, el de los racionales por $\mathbb{Q}$, por $\mathbb{P}$ el conjunto de los primos, por $\mathbb{R}$ el de los reales y, por último, $\mathbb{C}$ representará el conjunto de los complejos. El máximo común divisor de dos números a y b se denotará por $\mathrm{mcd}(a, b)$. Para cualquier x real, $\lfloor x \rfloor$ denotará la parte entera de x, es decir, el mayor entero menor o igual que x. $\mathrm{Re}(x)$ denotará la parte real de un número complejo x.

Estas son las notaciones generales que se van a seguir a lo largo del trabajo. En los distintos capítulos se especificarán las diferentes notaciones utilizadas. También mencionar que la mayor parte de las definiciones y demostraciones incluidas en este capítulo están sacadas del libro *Recorridos por la teoría de números* de J. L. Varona, véase [16].

Una vez aclarado esto, comenzamos con las primeras definiciones:

Definición (Divisibilidad)**.** Sea $a, b \in \mathbb{Z}$ con $a \neq 0$. Decimos que a divide á b, y escribiremos $a \mid b$, si existe otro número entero m tal que $b = ma$. Diremos también que b es un múltiplo de a, que a es un divisor de b, o que a es un factor de b. Si a no divide á b escribiremos $a \nmid b$.

La divisibilidad es un **orden parcial** en $\mathbb{N}$, se cumple:

- Reflexividad: $a \mid a$
- Antisimetría: $a \mid b$ y $b \mid a \iff a = b$
- Transitividad: $a \mid b$ y $b \mid c \implies a \mid c$

Observación. La antisimetría falla en $\mathbb{Z}$ por los signos: $a \mid -a \mid a$. Además, observemos que 1 es el único entero que divide a todos los enteros y 0 es el único entero divisible por todos los enteros no nulos.

Definición (Número primo)**.** Decimos que un número natural $p > 1$ es un número primo si sus únicos divisores naturales son el 1 y él mismo. Los números no primos se denominan números compuestos.

Por convenio, el 1 no se considera primo ni compuesto.

Definición (Máximo común divisor)**.** El máximo común divisor (de forma abreviada mcd) de dos números enteros a y b no ambos nulos se define como

$$\text{mcd}(a, b) = \text{máx}\{d \in \mathbb{Z} : d \mid a \text{ y } d \mid b\}.$$

Definición (Números coprimos)**.** Decimos que dos números $a, b \in \mathbb{Z} \setminus \{0\}$ son coprimos, o primos entre sí, si $\text{mcd}(a, b) = 1$.

Una vez dada la definición de primo, la primera palabra clave, pasemos a la segunda (o a las segundas). Definamos el concepto de progresión aritmética:

Definición (Sucesión)**.** Una sucesión de elementos de un conjunto es una aplicación con dominio $\mathbb{N}$ y codominio dicho conjunto. En particular, una sucesión de números reales es una función real con dominio $\mathbb{N}$, es decir, $s : \mathbb{N} \to \mathbb{R}$.

El valor que toma una sucesión s en cada $n \in \mathbb{N}$ se denota por s_n. Como el dominio $\mathbb{N}$ es común a todas las sucesiones, en vez de utilizar la notación $s : \mathbb{N} \to \mathbb{R}$ para una sucesión usaremos (s_n) si no da lugar a confusión. Un ejemplo de sucesiones son las sucesiones recurrentes, definidas a continuación:

Definición (Sucesión recurrente)**.** Las sucesiones recurrentes son aquellas sucesiones cuyos términos se definen en función de los anteriores (definición inductiva o recursiva).

Las **progresiones aritméticas** de primer término x y razón h son sucesiones recurrentes que pueden definirse recursivamente por

$$s_1 = p, \quad s_{n+1} = s_n + q.$$

Denotaremos $\mathbb{N}(p, q)$ a la progresión aritmética $px + q$ y $\mathbb{P}(p, q)$ a los primos en ella.

Definición (Congruencia módulo m)**.** Dados enteros a, b, m con $m \geq 1$, decimos que a es congruente con b módulo m y escribimos $a \equiv b \pmod{m}$ si m divide la diferencia $a - b$. El número m se llama módulo de la congruencia.

Teorema 1.1. $\equiv$ *es una* ***relación de equivalencia****: cumple las propiedades*

- *reflexiva:* $a \equiv a \pmod{m}$*,*
- *simétrica:* $a \equiv b \pmod{m}$ *implica* $b \equiv a \pmod{m}$ *y*
- *transitiva:* $a \equiv b \pmod{m}$ *y* $b \equiv c \pmod{m}$ *implica* $a \equiv c \pmod{m}$*.*

Definición (Clase de restos)**.** Consideremos un módulo fijo $m > 0$. Designemos por $\hat{a}$ el conjunto de todos los enteros x tales que $x \equiv a \pmod{m}$, y diremos que es la clase de restos de a módulo m.

Teorema 1.2. *La clase de* $a \pmod{m}$ *es una unidad en* $\mathbb{Z}/m\mathbb{Z}$ *si y sólo si* $\mathrm{mcd}(a, m) = 1$*. El grupo de las unidades se denota por* $\mathbb{U}_m$*.*

Comentemos algunas propiedades:

a) El número de unidades es la función phi de Euler

$$\phi(m) = \mathrm{card}(\mathbb{U}_m),$$

que es el número de a con $1 \leq a \leq m$ y $\mathrm{mcd}(a, m) = 1$.

b) p es primo si y sólo si $\phi(p) = p - 1$. $\mathbb{Z}/m\mathbb{Z}$ es un cuerpo.

c) $\phi(p^k) = p^{k-1}(p-1) = p^k(1 - p^{-1})$ para $p \in \mathbb{P}$. En general,

$$\phi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right)$$

por el teorema chino del resto.

d) $\mathbb{U}_m$ es cíclico si y sólo si $m = 2, 4, p^k, 2p^k$ con $p \in \mathbb{P}$ impar (Gauss).

1.2. Introducción histórica

Los números primos siempre han sido un tema interesante de estudio. Ya los antiguos griegos comenzaron a trabajar con ellos. Los pitagóricos (500 a.C. a 300 a.C.) sabían que los números estaban en todas partes, fueron ellos los primeros en multiplicar números y observar que ciertos de ellos no se podían dividir entre ningún otro salvo el 1 y ellos mismos: los primos. Ellos dieron el primer paso hacia el teorema más importante de la aritmética:

Teorema 1.3 (Teorema fundamental de la aritmética)**.** *Cada entero $n > 1$ se puede descomponer como un producto de factores primos de forma única (salvo permutación de los factores).*

Aproximadamente en el 300 a.C. aparecieron *Los Elementos* de Euclides, donde se recogían muchos resultados importantes sobre los números primos. En el Libro IX, Euclides demuestra que hay infinitos números primos. Esta es una de las primeras pruebas conocidas que utiliza el método de la contradicción para establecer un resultado. Euclides también da una prueba del teorema fundamental de la aritmética, que acabamos de enunciar.

Un siglo más tarde, el griego Eratóstenes ideó un algoritmo para calcular números primos denominado la **criba de Eratóstenes**. Es un algoritmo que permite hallar todos los números primos menores que un número natural dado n. Se forma una tabla con todos los números naturales comprendidos entre 2 y n y se van tachando los números que no son primos.

Los próximos desarrollos importantes fueron hechos por Fermat a comienzos del siglo XVII, que demostró que todo número de la forma $4n+1$ puede ser escrito de forma única como suma de dos cuadrados. Ideó un nuevo método para factorizar números grandes que demostró factorizando el número $2027651281 = 44021 \times 46061$. Demostró lo que ha llegado a conocerse como el pequeño teorema de Fermat, que establece que, si p es primo, entonces para cualquier entero a tenemos $a^p \equiv a \pmod{p}$.

Fermat mantuvo correspondencia con otros matemáticos de su época y, en particular, con el monje Marin Mersenne. En una de sus cartas a Mersenne, conjeturó que los números $2^n + 1$ son siempre primos si n es potencia de 2. Esto, Fermat lo había verificado para $n = 1, 2, 4, 8$ y 16 y sabía que si n no era potencia de 2, no se cumplía. Los números de esta forma pasaron a llamarse los números de Fermat y no fue hasta 100 años más tarde que Euler demostró que en el siguiente caso obtenemos $2^{32} + 1 = 4294967297$, que es divisible por 641 y por lo tanto, no es primo.

Por otro lado, los números de la forma $2^n - 1$ también han llamado la atención ya es es fácil demostrar que si n no es primo los números con esa forma deben ser compuestos. A menudo se los conoce como números de Mersenne.

El trabajo de Euler tuvo un gran impacto en la teoría de números en general y en los primos en particular. Amplió el pequeño teorema de Fermat, introdujo la función ϕ de Euler y, como se mencionó anteriormente, factorizó en quinto número de Fermat.

Euler no sólo probó que la serie armónica $\sum 1/n$ es divergente, sino también que la serie de los inversos de los números primos lo es. Como consecuencia inmediata, obtenemos otra demostración del teorema de Euclides.

Esto ocurrió en el año 1737, otros 100 años más tarde, Dirichlet se basó en el trabajo de Euler para demostrar que en cualquier progresión aritmética tal que el primer término es coprimo con la razón, existen infinitos primos. Se puede decir que la teoría analítica de números nació aquí.

A lo largo de la memoria, vamos a seguir un poco el camino de la historia: comenzaremos con la demostración de Euclides y nos daremos cuenta de que el esquema que sigue a lo largo de su demostración lo podemos aplicar para demostrar la existencia de infinitos números primos en distintas progresiones aritméticas. La pregunta que nos surgirá es si podemos aplicar ese tipo de demostración, a la cual llamaremos demostración euclidiana, para cualquier tipo de progresión aritmética. Es decir, si podemos demostrar el teorema de Dirichlet mediante una demostración euclidiana. La contestaremos al final del capítulo 2. Veremos la demostración de Euler del teorema de Euclides y de ahí sacaremos las ideas de usó Dirichlet para probar su teorema y lo probaremos.

Capítulo 2

Teorema de Euclides

"Reductio ad absurdum, que tanto le gustaba a Euclides, es una de las mejores armas de un matemático."

— G.H. Hardy

El objetivo de este capítulo es demostrar la existencia de infinitos números primos, teorema enunciado y demostrado por Euclides en el año 300 a.C. Poco se conoce de la vida de Euclides, pese a ser el matemático más famoso de la Antigüedad. Se cree que se educó en Atenas, lo que explicaría su buen conocimiento de la geometría elaborada en la escuela de Platón. Enseñó en Alejandría, donde abrió una escuela que acabaría siendo la más importante del mundo helénico. Euclides fue autor de diversos tratados, pero su nombre se asocia principalmente a uno de ellos, *Los Elementos*. Nos centraremos en los que nos interesan a nosotros, los libros del séptimo al décimo, que tratan distintas cuestiones numéricas entre las cuales se encuentran las principales propiedades de la teoría de números: divisibilidad, números primos, entre otros. La demostración de la que hablaremos en este capítulo se encuentra en su noveno libro [3]. Procedamos a verla enunciando antes algunas proposiciones y teoremas:

2.1. Demostración de Euclides

Proposición 2.1 (Principio de buena ordenación de los números naturales)**.** $(\mathbb{N}_0, \leq)$ *es un conjunto bien ordenado (es decir, cualquier subconjunto de* $\mathbb{N}_0$ *no vacío tiene mínimo).*

Al contrario que los naturales, los enteros ya no son un conjunto bien ordenado (por ejemplo, el conjunto de enteros negativos no tiene mínimo), pero ocurre algo muy parecido: cualquier subconjunto no vacío de $\mathbb{Z}$ acotado inferiormente tiene mínimo (y, multiplicando por -1, si es acotado superior-

mente, tiene máximo). A esta última propiedad le vamos a dar el nombre de **axioma de buen orden en** $\mathbb{Z}$, el cual enunciamos a continuación:

Proposición 2.2 (Axioma del buen orden en $\mathbb{Z}$)**.** *Cualquier subconjunto no vacío de* $\mathbb{Z}$ *acotado inferiormente tiene mínimo.*

Teorema 2.3. *Cada entero mayor que* 1 *tiene un divisor primo.*

Demostración. Vamos a realizar la demostración por reducción al absurdo. Para ello, supongamos que no es cierto. Sea n el menor entero mayor que 1 que no tiene ningún divisor primo (tal n debe existir por la proposición 2.2). Como $n \mid n$ y n no tiene divisores primos, n no puede ser primo. Por tanto n podrá escribirse como $n = ab$ con $1 < a < n$ y $1 < b < n$. Como $a < n$ y n es el menor entero mayor que 1 sin divisores primos, a deberá tener un divisor primo p. Pero como $p \mid a$ y $a \mid n$ tenemos que $p \mid n$, y eso contradice que n no tenía divisores primos. □

Con esto, ya podemos proceder a dar la demostración de Euclides:

Demostración. La realizamos también por reducción al absurdo. Supongamos que sólo existe una cantidad finita de números primos, a los que denominaremos $S = \{p_1, p_2, \ldots, p_n\}$. Sea $N = p_1 p_2 \cdots p_n + 1$. El número N es entero y mayor que 1, además es distinto de cualquier p_i con $i = 1, \ldots, n$ luego N no pertenece a S, lo que quiere decir que N no es primo. Por el teorema 2.3 podemos afirmar que N tiene un divisor primo, al que denominaremos p. Pero p es distinto de cualquiera de los p_i con $i = 1, \ldots, n$ (ya que si $p_i \mid N$ entonces $N - p_1 p_2 \cdots p_n = 1$, lo que implica que $p_i \mid 1$, y eso es falso pues ningún número, salvo él mismo, divide al 1). Hemos llegado a la contradicción que buscábamos ya que hemos encontrado un número primo p que no pertenece a S. □

Usando la misma idea para la demostración tenemos varias alternativas, presentamos dos de ellas:

- **Reformulación de Kummer**: Demostración publicada por Enrst Kummer en uno de sus artículos en el año 1878. Podemos encontrarla en [7]. Supongamos que existe una cantidad finita de números primos distintos y ordenados de forma creciente $p_1 < p_2 < p_3 < \cdots < p_n$, con $n > 1$. Sea $N = p_1 \cdot p_2 \cdots p_n > 2$. Sea $N - 1 \in \mathbb{Z}$. Por el teorema 2.3, $N - 1$ tiene un divisor primo, p_i que también es divisor de N. Por lo que p_i divide a su resta $N - (N - 1) = 1$. Luego $p_i = 1$, lo cual es un absurdo.

- **Demostración de Stieltjes**: Thomas Stieltjes trabajó en numerosos campos de las matemáticas. Realizó una demostración del teorema de

Euclides en el año 1890. Podemos encontrar la siguiente demostración en [15]. Supongamos que existe un número finito de números primos $p_1, p_2, \ldots, p_n$. Sea $N = p_1 \cdot p_2 \cdots p_n$ y sean m y n dos enteros tal que $N = m \cdot n$, con m, r positivos mayores que 1 y primos entre sí. Se tiene que todo número primo p_i divide, o bien a m, o bien a r, pero no a ambos. Por lo que $m + r$ no puede tener ningún divisor primo de nuestra lista inicial y, por el teorema 2.3, $m+r$ tendrá un factor primo p en caso de no ser primo (en caso de ser primo, $p = m + r$). Llegamos a una contradicción.

2.2. Demostración euclidiana

Se puede usar el mismo mecanismo de demostración para ver que existen infinitos primos de una cierta forma. Por ejemplo, nos sirve para ver que existen infinitos primos de la forma $4k - 1$ (lo que equivale a decir que existen infinitos números primos congruentes con -1 módulo 4, que es lo mismo que decir que existen infinitos primos congruentes con 3 módulo 4). Veamos la demostración de esto.

Teorema 2.4. *Existen infinitos primos de la forma* $4k - 1$.

Demostración. Dada una lista finita $S = p_1, \ldots, p_n$ de tales primos, consideremos el polinomio

$$f(x) = 4x - 1 \quad \text{y sea} \quad N = f(p_1, \ldots, p_n) = 4(p_1, \ldots, p_n) - 1.$$

Vemos que $N > 1$ y que, por el teorema 2.3, tiene algún factor primo. Llamemos a ese factor primo p. Tenemos que:

- N no puede ser primo, ya que tiene la forma $4k - 1$ y es mayor que todos los primos de esa forma.
- Además, como $N \neq 1$ (mód 4), no todos los factores primos de N pueden ser congruentes con 1 (mód 4), ya que el producto de dos números de la forma $4k + 1$ es de la misma forma.

Concluimos que N tiene un divisor primo $p \in \mathbb{P}(3, 4)$, pero p no está en nuestra lista S y, por lo tanto, hay infinitos primos en $\mathbb{P}(3, 4)$. □

Existe una prueba similar para probar que existen infinitos números primos de la forma $4x + 1$:

Teorema 2.5. *Existen infinitos primos de la forma* $4k + 1$.

Antes de ver la demostración de este teorema, veamos la siguiente definición:

Definición (Residuo cuadrático)**.** Se denomina residuo cuadrático módulo m a cualquier entero no nulo r coprimo con m para el que tenga solución la congruencia

$$x^2 \equiv r \pmod{m}.$$

Procedemos a la demostración del teorema:

Demostración. Dada una lista finita $S = p_1 \ldots, p_n$ de tales primos, consideremos el polinomio $f(x) = 4x^2 + 1$. Y sea

$$N = f(p_1, \ldots, p_n) = 4(p_1, \ldots, p_n)^2 + 1.$$

Este número tiene que tener un divisor primo, por el teorema 2.3, llamémosle q. Por lo tanto -1 es un residuo cuadrático módulo q. Con lo que tenemos $q \equiv 1 \pmod{4}$. Luego o bien N es primo congruente con 1 (mód 4) o bien es divisible por un primo $q \equiv 1 \pmod{4}$ que no pertenece a la lista S. Lo que nos da una infinitud de primos siempre y cuando encontremos uno. Como $5 \equiv 1 \pmod{4}$ hemos acabado. □

Llamemos a este tipo de prueba demostración euclidiana, ya que los pasos a seguir son similares a la demostración seguida por Euclides para demostrar la existencia de infinitos números primos. Vamos a intentar dar una definición más rigurosa de este concepto:

En una progresión aritmética, $\mathbb{N}(p, q)$, si $\text{mcd}(p, q) > 1$ todos los números de la progresión son compuestos (salvo, quizás, el primero). Luego una primera condición necesaria para que existan infinitos primos en dicha progresión es que $\text{mcd}(p, q) = 1$. Una vez establecido esto, seguimos observando las demostraciones realizadas para probar el teorema 2.4 y el teorema 2.5.

Nos percatamos de que ambas pruebas contienen un polinomio con coeficientes enteros cuyos valores en $\mathbb{Z}$ son divisibles por primos en la progresión requerida. En el caso de la primera demostración, el polinomio era $4x - 1$, llamémosle a partir de ahora $f(x)$, en el cual todos los valores son sólo divisibles por primos congruentes con 1 (mód 4), mientras que en la segunda era $4x^2 + 1$, llamémosle $g(x)$, y esta vez, todos los valores sólo divisibles por primos congruentes con 3 (mód 4).

En cualquier caso, existe un polinomio en $\mathbb{Z}[x]$ tal que en el conjunto de divisores primos de los valores del polinomio en argumentos enteros hay infinitos primos en la progresión aritmética deseada. En consecuencia, diremos que un primo p es un divisor primo del polinomio si $f \in \mathbb{Z}[x]$ si p divide a $f(n)$ para algún n entero. Así, el primer requisito para obtener una demostración euclidiana para la progresión aritmética $\mathbb{N}(l, k)$ es la existencia de un polinomio con infinitos divisores primos congruentes con l (mód k).

Puede no parecer claro que un polinomio tenga infinitos divisores primos. Esto, fue demostrado por Schur en el año 1912. Encontramos dicha demostración en [14] y a continuación:

Teorema 2.6 (Schur)**.** *Si $f \in \mathbb{Z}[x]$ no es constante, entonces f tiene infinitos divisores primos.*

Demostración. Si $f(0) = 0$ tenemos que $p \mid f(0)$ para todo p, f y se demuestra trivialmente que tiene infinitos divisores primos. Supongamos por lo tanto que $f(0) = a \neq 0$. Ahora, $f(x) = \pm 1$ solo tiene soluciones finitas, por lo que f tiene que tener al menos un divisor primo. Supongamos que f tiene un número de divisores primos finito $p_1, p_2, \ldots, p_k$ y llamemos $Q = p_1 p_2 \cdots p_k$ a su producto. Entonces $f(Qax) = ag(x)$ para algún polinomio $g \in \mathbb{Z}[x]$ de la forma $1 + a_1 x + a_2 x^2 + \ldots$ con $Q \mid a_i$ para cada i. Siguiendo el mismo razonamiento que con f, vemos que g tiene también al menos un divisor primo, al que llamaremos p. Como p divide a g, también divide a f, pero p no divide a Q (ya que en caso de que lo hiciera, p dividiría a 1). Concluimos con una contradicción obtenida al suponer que f tiene un número finito de divisores primos. □

De aquí en adelante, $P(f)$ denotará el conjunto de los divisores primos de f. La siguiente restricción impuesta a nuestro polinomio euclidiano surge de un teorema de Nagell. Vamos a ver una prueba directa mediante la teoría de grupos. Una prueba más larga, pero más elemental, fue dada por Nagell y la podemos encontrar en [11].

Teorema 2.7 (Nagell)**.** *Si $f, g \in \mathbb{Z}[x]$ son polinomios no constantes, entonces $P(f) \cap P(g)$ es infinita.*

Demostración. Supongamos que α es una raíz de f y β es una raíz de g. Por el teorema de Dedekind (podemos encontrarlo enunciado y demostrado en [4]), excepto por un número finito de excepciones, p es un divisor primo de f cuando p tiene un factor ideal de primer grado en el cuerpo $\mathbb{Q}(\alpha)$. Lo mismo ocurre con g. Consideremos el cuerpo $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$ para algún θ en O_K, el anillo de enteros en K. Si h es el polinomio mínimo de θ, el teorema 2.6 nos asegura que existen infinitos números primos que tienen un factor ideal de primer grado en $\mathbb{Q}(\alpha, \beta)$, y por lo tanto en $\mathbb{Q}(\alpha)$ y en $\mathbb{Q}(\beta)$. Por lo que, salvo para un número finito de excepciones, estos primos están en $P(f)$ y en $P(g)$. □

Se deduce del teorema de Nagell que cualquier polinomio tiene infinitos divisores primos congruentes con 1 (mód k) para cualquier número entero k. Esto obliga a nuestro polinomio euclidiano a tener tales divisores primos.

Así, la definición más razonable de una demostración euclidiana para la progresión aritmética $\mathbb{N}(l, k)$ es la existencia de un polinomio $f \in \mathbb{Z}[x]$ tal que todos los divisores primos de f (aparte de los finitos) son o bien congruentes con 1 (mód k) o con l (mód k). También podemos suponer que este polinomio es irreducible.

Definición (Demostración euclidiana)**.** Se llama demostración euclidiana a una demostración de infinitud para $\mathbb{P}(a, m)$ que procede de la siguiente manera:

- Se da una lista finita $S \subseteq \mathbb{P}(a, m)$ y $x = \prod_{p \in S} p$.
- Se construye un entero N que es un polinomio en x.
- Se tiene que cumplir que $N > 1$ y $\text{mcd}(N, x) = 1$.
- N debe tener al menos un divisor primo $p \in \mathbb{P}(a, m)$.

La pregunta que nos surge ahora es ¿hasta qué punto se puede generalizar esta antigua prueba? En 1837, Dirichlet demostró que para cualquier l y k coprimos hay infinitos p tales que $p \equiv l \pmod{k}$. Pero su enfoque fue por medio de L-funciones y análisis. Lo que nosotros nos preguntamos es hasta dónde se puede llevar la prueba de Euclides para obtener el teorema de Dirichlet. Ya hemos visto que para ciertas progresiones aritméticas existe una demostración euclidiana (para $\mathbb{N}(1, 4)$, para $\mathbb{N}(3, 4)$). Del mismo modo se pueden dar una demostración euclidiana para probar que existen infinitos primos en la progresión $\mathbb{N}(1, k)$ para cualquier número entero k (se realiza utilizando propiedades del polinomio ciclotómico). La demostración para las progresiones $\mathbb{N}(3, 4)$ y $\mathbb{N}(5, 6)$ las podemos encontrar [6] dadas por G. H. Hardy y E. M. Wright. Para caracterizar las progresiones aritméticas para las que existe tal prueba, Murty demostró en [9]:

Teorema 2.8 (Murty)**.** *Existe una demostración euclidiana de infinitud de* $\mathbb{P}(a, m)$ *sólo si* $a^2 \in \mathbb{N}(1, m)$.

Duda resuelta, es imposible demostrar el teorema de Dirichlet para ciertas progresiones aritméticas por el método de Euclides, porque incluso para ejemplos de apariencia simple como $5x + 2$ no se puede encontrar un polinomio adecuado.

Capítulo 3

Las ideas de Euler

"Lo primero que haría si volviese a la vida dentro de quinientos años sería averiguar si alguien había resuelto la Hipótesis de Riemann"

— D. Hilbert

La mayor parte de la información recogida en este capítulo ha sido obtenida de las diapositivas de L. Navas sobre la infinitud de primos en progresiones aritméticas. Podemos verle hablando de la infinitud de los primos en una conferencia del ciclo *Más Temáticas* de la Universidad de Salamanca. Podemos encontrarla en YouTube, el enlace lo vemos en [12].

Leonhard Euler (Basilea, 1707 - San Petersburgo, 1783) fue un matemático suizo que trabajó prácticamente en todos los ámbitos de las matemáticas: geometría, cálculo, trigonometría, álgebra, teoría de números, además de física continua, teoría lunar, entre otras.

En un artículo de 1737 titulado *Variae observationes circa series infinitas* Euler (que encontramos en [8]) demostró que la divergencia de la serie armónica implica la existencia de infinitos números primos. Para demostrarlo, introducimos los siguientes conceptos:

Definición (Singularidad)**.** Se dice que una función f tiene una singularidad en a si no es holomorfa en ese punto y en todo entorno de a existen puntos donde la función es holomorfa.

Definición (Singularidad aislada)**.** Un punto $a \in \mathbb{C}$ se dice que es una singularidad aislada si la función compleja f no es holomorfa en a y existe un $R > 0$ tal que f es holomorfa en $\{z \in \mathbb{C};\, 0 < |z - a| < R\}$.

El conjunto $B_R(a) = \{z \in \mathbb{C};\, 0 < |z-a| < R\}$ se denomina disco abierto, bola abierta o entorno de centro a y radio R. Usualmente se utiliza el nombre de singularidad para denominar a las singularidades aisladas.

Sea $a \in \mathbb{C}$ es una singularidad aislada de f. Se dice que:

a) es una **singularidad evitable** si $\lim_{z\to a} f(z) \in \mathbb{C}$;

b) es un polo si $\lim_{z\to a} f(z) = \infty$;

c) es una **singularidad esencial** si no es una singularidad evitable ni un polo.

Definición (Función meromorfa)**.** Se dice que una función es meromorfa en un abierto Ω de $\mathbb{C}$ si f es holomorfa en Ω excepto en un conjunto aislado de singularidades, en cada una de las cuales f tiene un polo o una singularidad aislada evitable.

Definición (Cero)**.** Un cero en una función holomorfa f es un número complejo a que cumple la condición $f(a) = 0$.

Definición (Función zeta de Riemann)**.** La función zeta de Riemann está definida por

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad \text{con } \operatorname{Re}(s) > 1.$$

La función zeta de Riemann se prolonga analíticamente a una función meromorfa con un polo simple en $s = 1$ y ceros triviales en los enteros pares negativos. Además, satisface la ecuación funcional

$$\zeta(s) = 2(2\pi)^{s-1}\Gamma(1-s)\sin\Big(\frac{\pi s}{2}\Big)\zeta(1-s), \tag{3.1}$$

donde

$$\Gamma(s) = \int_0^{\infty} x^{s-1}e^{-x}\,ds. \tag{3.2}$$

Esta simetría posiblemente llevó a la hipótesis de Riemann que dice lo siguiente: la parte real de todos los ceros no triviales de la función zeta de Riemann es $1/2$. ¿Pero qué son los ceros no triviales? Si en la ecuación (3.1) sustituimos s por un número par negativo, el seno se anula y con él, la función zeta de Riemann. A esto se les llaman ceros triviales. Es cierto que si sustituimos s por un número par positivo, el seno también se anula, pero lo que ocurre en este caso es lo siguiente: la función Gamma (3.2) es positiva si le aplicamos un número positivo, pero su extensión analítica aplicada a un número negativo, tiene un polo que anula ese efecto del seno. Por lo que la función en los pares positivos no es cero.

Todos los demás ceros de la función zeta son complejos cuya parte real está entre 0 y 1. Podemos encontrar el teorema que afirma y demuestra esta afirmación en el teorema 13.11, del capítulo 13 del libro de Apostol [1].

A esa franja se le conoce como franja crítica y en medio de esa región está la línea crítica, que es la línea de los números complejos cuya parte real

es $1/2$. La hipótesis de Riemann afirma que todos los ceros no triviales están ahí.

Esta hipótesis fue uno de los 23 problemas de la lista de Hilbert y es uno de los famosos problemas del milenio. A día de hoy está sin resolver pero se sabe que:

- En 1915 Hardy probó que hay una infinidad de ceros situados en la recta crítica.
- Un par de años más tarde, en el 1921 Hardy y Littlewood [5] demostraron que el número de ceros que hay en el segmento rectilíneo que une $1/2$ con $1/2 + (iT)$ es por lo menos AT para una cierta constante positiva A, si T es suficientemente grande.
- En el año 1942 Selberg lo perfeccionó probando que el número es por lo menos $AT \log T$ para un cierto $A > 0$.
- En 1974 Levinson probó que esa fracción es por lo menos $7/10$. Es decir, que la constante del teorema de Selberg satisface $A \geq 7/(20\pi)$.
- Al final de la Segunda Guerra Mundial, Turing comenzó a trabajar con Max Newman en el recién construido Laboratorio de Cálculo de la Royal Society. Construyeron una máquina calculadora programable para cálculos diversos. Con esta máquina Turing comprobó en 1950 que los 1104 primeros ceros no triviales de la función zeta estaban situados sobre la recta $x = 1/2$.
- En 2004 Gourdon anunció la comprobación numérica de que los primeros 10^{13} ceros no triviales de la función zeta están situados sobre la recta crítica. En 2005 se desarrolló el proyecto ZetaGrid de computación distribuida capaz de verificar 10^9 ceros por día. Tampoco consiguió el contraejemplo de un zero de la función zeta no situado en la recta crítica.

Riemann calculó 3 ceros no triviales, hoy en día se conocen billones. Aun así, a día de hoy, nadie ha conseguido probar la hipótesis ni encontrar ningún contraejemplo.

Veamos ahora la fórmula del producto para la función zeta.

Teorema 3.1. *Para* $\mathrm{Re}(s) > 1$ *se tiene*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1}. \tag{3.3}$$

Observación. Antes de continuar, una pequeña aclaración: de aquí en adelante reservaremos la letra p para referirnos a un número primo.

Demostración. Cada factor se desarrolla en serie geométrica:

$$\left(1-\frac{1}{p^s}\right)^{-1} = 1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\cdots+\frac{1}{p^{ms}}+\cdots.$$

Al distribuir, la factorización única implica que

$$P(x) = \prod_{p\le x}\left(1-\frac{1}{p^s}\right)^{-1} = \sum_{n\in\mathbb{N}_x}\frac{1}{n^s}$$

donde $\mathbb{N}_x$ son los $n\in\mathbb{N}$ con sólo factores primos $p\le x$. Como $\mathbb{N}_x$ crece a $\mathbb{N}$ cuando $x\to\infty$ se demuestra el teorema. □

Veamos algunas observaciones acerca de la fórmula del producto para la función zeta. Para empezar, la fórmula implica que $\zeta(s)$ no tiene ceros en $\mathrm{Re}(s)>1$ (es un producto infinito convergente de factores no nulos). Además, muestra que la distribución de los ceros de $\zeta(s)$ condiciona la de los primos. Por otro lado, que la prolongación de $\zeta(s)$ no tenga ceros con $\mathrm{Re}(s)=1$ equivale (no trivialmente) al teorema del Número Primo:

$$\pi(x) := \{\mathrm{card}\, p\in\mathbb{P} : p\le x\} \sim \frac{x}{\log x} \qquad (x\to\infty).$$

Si supiéramos que no hay ceros con $\mathrm{Re}(s)>1-\epsilon$, donde $0<\epsilon<\frac{1}{2}$, tendríamos cotas más precisas para $\pi(x)$. A día de hoy, esto no ha sido demostrado para ningún ϵ.

Introducimos un teorema que equivale a decir que $\zeta(s)$ tiene un polo en $s=1$.

Teorema 3.2. *La serie de los recíprocos de los primos es divergente, es decir,*

$$\sum_{p\in\mathbb{P}}\frac{1}{p}=\infty.$$

En particular, hay infinitos primos (si sólo hubiera un número finito de sumandos, la suma sería finita y racional).

Demostración. Probaremos

$$\lim_{s\to1^+} P(s)=\infty, \quad \text{donde} \quad P(s)=\sum_{p\in\mathbb{P}}\frac{1}{p^s}.$$

Demostrando esto, probaremos también el teorema, ya que

$$P(s)=\sum_{p\in\mathbb{P}}\frac{1}{p^s}\le\sum_{p\in\mathbb{P}}\frac{1}{p} \quad (s>1).$$

Comparando con la serie armónica vemos que

$$\zeta(1^+) = \lim_{s\to 1^+} \zeta(s) = \infty$$

pues $\zeta(s)$ decrece en $(1,\infty)$ y, para todo $s > 1$ y $x > 0$,

$$\zeta(s) \geq \sum_{n\leq x} \frac{1}{n^s} \xrightarrow{s\to 1} \zeta(1^+) \geq \sum_{n\leq x} \frac{1}{n} \xrightarrow{x\to\infty} \zeta(1^+) \geq \sum_{n=1}^{\infty} \frac{1}{n} = \infty.$$

Aplicando logaritmos en (3.3) tenemos

$$\log \zeta(s) = -\sum_p \log\left(1 - \frac{1}{p^s}\right) \quad (s > 1).$$

La aproximación $-\log(1-x) = x + \mathcal{O}(x^2)$ implica que

$$\log \zeta(s) = \sum_p \frac{1}{p^s} = \mathcal{O}(1) = P(s) + \mathcal{O}(1) \quad (s \to 1^+).$$

Si tendemos $s \to 1^+$, queda

$$\lim_{s\to 1^+} P(s) = \infty,$$

con lo que se prueba el teorema. □

Esta es la demostración de Euler del teorema de Euclides. En el siguiente apartado vamos a ver cómo Dirichlet se inspiró en sus ideas para demostrar su teorema.

3.1. Las ideas de Dirichlet

Peter Gustav Lejeune Dirichlet, nacido el 13 de febrero de 1805 en Düren, Imperio francés (ahora Alemania) y fallecido el 5 de mayo de 1859 en Gotinga, Hannover, fue un matemático alemán que hizo valiosas contribuciones a la teoría de números, el análisis y la mecánica. Enseñó en las universidades de Breslau y Berlín, y en 1855 sucedió a Carl Friedrich Gauss en la Universidad de Gotinga como profesor. Una vez presentado Dirichlet, presentemos sus ideas:

Sea $m \geq 2$ fijo y $\mathbb{P}(a,m)$ el conjunto de primos $p \equiv a \pmod m$. Inspirado por Euler, Dirichlet considera la función

$$P_a(s) = \sum_{p\in\mathbb{P}(a,m)} \frac{1}{p^s} \quad (\mathrm{Re}(s) > 1).$$

Si conseguimos demostrar que

$$\lim_{s\to 1^+} P_a(s) = \infty,$$

como corolario habremos demostrado que hay infinitos primos de la forma $p \equiv a \pmod{m}$, ya que

$$\infty = \lim_{s\to 1^+} \sum_{p\in\mathbb{P}(a,m)} \frac{1}{p^s} \leq \sum_{p\in\mathbb{P}(a,m)} \frac{1}{p}.$$

Lo que vamos a realizar, por lo tanto, es estudiar las propiedades analíticas de la función $P_a(s)$.

Al igual que Euler, buscamos una fórmula del producto. Pero no es tan sencillo relacionar

$$\sum_{n\in\mathbb{N}(a,m)} \frac{1}{n^s} \quad \text{con} \quad \prod_{p\in\mathbb{P}(a,m)} \left(1-\frac{1}{p^s}\right)^{-1}$$

ya que, en general, $x, y \equiv a \pmod{m}$ no implica que $xy \equiv a \pmod{m}$. Lo que quiere decir que la función delta o característica de $\mathbb{N}(a,m)$ con m fijo

$$1_a(n) = \begin{cases} 1, & \text{si } n \equiv a \pmod{m}, \\ 0, & \text{en otro caso,} \end{cases}$$

en general no es multiplicativa: $1_a(xy) \neq 1_a(x)\,1_a(y)$.

Aun así, tenemos

$$\sum_{n\in\mathbb{N}(a,m)} \frac{1}{n^s} = \sum_{n=1}^{\infty} \frac{1_a(n)}{n^s}, \qquad \sum_{p\in\mathbb{P}(a,m)} \frac{1}{p^s} = \sum_{p\in\mathbb{P}} \frac{1_a(p)}{p^s}.$$

En el siguiente capítulo veremos el resto de los conceptos que nos ayudarán a entender la demostración del teorema de Dirichlet, introduciendo conceptos como L-funciones de Dirichlet, caracteres de Dirichlet, entre otros.

Capítulo 4

El método de Dirichlet

El enfoque revolucionario de Dirichlet con respecto a la demostración dada por Euler es marcar, por así decirlo, los números primos de una determinada progresión aritmética para luego aislarlos de la suma mencionada y demostrar su divergencia. Para llevar a cabo esta selección, Dirichlet utilizó los llamados caracteres, que veremos con más detalle al final de este capítulo. Comenzamos definiendo algunos conceptos iniciales:

Definición (Función aritmética)**.** Una función $f : \mathbb{N} \to M$, con $M \subseteq \mathbb{C}$ se denomina función aritmética.

Veamos tres ejemplos importantes, comenzando por la función de Möbius. El matemático alemán August F. Möbius la introdujo en el año 1832.

Definición (Función de Möbius)**.** La función de Möbius μ se define como

- Si $n = 1$, $\mu(1) = 1$.
- Si $n > 1$, lo descomponemos en factores primos $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, todos ellos distintos entre sí. En caso de que $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 1$, $\mu(n) = (-1)^k$. En caso contrario, $\mu(n) = 0$.

Observación. $\mu(n) = 0$ si, y sólo si, n admite un divisor cuadrado > 1.

Vemos que la función de Möbius satisface la siguiente propiedad:

Teorema 4.1. *Si $n \geq 1$ tenemos*

$$\sum_{d|n} \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1, & si\ n = 1, \\ 0, & si\ n > 1. \end{cases} \tag{4.1}$$

Demostración. Para $n = 1$ la fórmula es cierta. Probemos para $n > 1$ escribiendo $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. En $\sum_{d|n} \mu(d)$ los términos no nulos vienen de $d = 1$

y de los divisores de n que son productos de primos distintos. Entonces,

$$\sum_{d|n}\mu(d) = \mu(1) + \cdots + \mu(p_k) + \mu(p_1p_2) + \cdots + \mu(p_{k-1}p_k) + \cdots + \mu(p_1p_2\cdots p_k)$$
$$= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k = (1-1)^k = 0. \qquad \square$$

Presentamos otra función aritmética importante: la función de von Mangoldt, propuesta por Hans von Mangoldt en 1894.

Definición (Función de von Mangoldt)**.** La función de von Mangoldt $\Lambda(n)$ se define para cada entero $n \geq 1$ como

$$\Lambda(n) = \begin{cases} \log p, & \text{si } n = p^m \text{ para un cierto primo } p \text{ y un cierto } m \geq 1, \\ 0, & \text{en otro caso.} \end{cases}$$

Esta función satisface lo siguiente:

Teorema 4.2. *Si $n \geq 1$ tenemos*

$$\log n = \sum_{d|n}\Lambda(d). \tag{4.2}$$

Demostración. La fórmula es cierta para $n = 1$. Probémosla para $n > 1$ escribiendo

$$n = \sum_{k=1}^{r} p_k^{\alpha_k}.$$

Tomamos logaritmos y obtenemos

$$\log n = \sum_{k=1}^{r} \alpha^k \log p_k.$$

Consideramos $\sum_{d|n}\Lambda(d)$. Los únicos términos no nulos de la suma provienen de los divisores d de la forma p_k^m para $m = 1, 2, \ldots, \alpha_k$ y $k = 1, 2, \ldots, r$. Por lo que nos queda

$$\sum_{d|n}\Lambda(d) = \sum_{k=1}^{r}\sum_{m=1}^{\alpha_k}\Lambda(p_k^m) = \sum_{k=1}^{r}\sum_{m=1}^{\alpha_k}\log p_k = \sum_{k=1}^{r}\alpha_k \log p_k = \log n. \qquad \square$$

Terminamos con otra función aritmética interesante, conocida como indicatriz de Euler y presentada por el mismo alrededor del año 1760.

Definición (Indicatriz de Euler)**.** La función indicatriz de Euler $\phi(n)$ es el número de enteros positivos menores que n que son primos con n, es decir,

$$\phi(n) = \text{card}\{m \leq n : \text{mcd}(m,n) = 1\} = \sum_{\substack{m \leq n \\ \text{mcd}(m,n)=1}} 1.$$

Definamos la función $\pi(n)$ que cuenta el número de primos menores o iguales a n, esto es,

$$\pi(n) = \text{card}\{p \leq n : p \text{ primo}\} = \sum_{p \leq n} 1.$$

4.1. Convolución de Dirichlet

El conjunto de funciones aritméticas forma un anillo conmutativo, el anillo de Dirichlet, bajo la adición componente a componente (la suma habitual de funciones) y la convolución de Dirichlet que definimos a continuación:

Definición (Producto de Dirichlet)**.** Si f y g son dos funciones aritméticas definimos su producto de Dirichlet (o convolución de Dirichlet) como la función aritmética h definida por

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

Observación. Escribiremos $f * g$ en vez de h y $(f * g)(n)$ en vez de $h(n)$. El símbolo N se utilizará para la función aritmética tal que $N(n) = N$ para todo n.

La multiplicación de Dirichlet es asociativa, distributiva respecto a la suma y conmutativa. Además, hay una única función aritmética, I, definida por

Definición (Identidad del producto de Dirichlet)**.** Se denomina identidad del producto de Dirichlet a la función aritmética

$$I(n) = \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{si } n \geq 2, \end{cases}$$

que satisface $f * I = I * f = f$ para toda f función aritmética.

Además se cumple:

Teorema 4.3. *Si f es una función aritmética con $f(1) \neq 0$, entonces existe una única función aritmética f^{-1} tal que*

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

que denominamos ***inversa de Dirichlet*** *de f.*

Teorema 4.4 (Fórmula de inversión de Möbius)**.** *Dadas f y g dos funciones aritméticas, se cumple*

$$f(n) = \sum_{d|n} g(d) \quad \textit{si y sólo si} \quad g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right).$$

Demostración. La primera ecuación establece que $f = g * u$. Multiplicando por μ tenemos $f * \mu = (g * u) * \mu = g * (u * \mu) = g * I = g$. Que es la segunda ecuación. Recíprocamente, la multiplicación de $f * \mu = g$ por u nos da la primera ecuación. □

Usaremos la fórmula que acabamos de definir para demostrar la siguiente propiedad de la función de von Mangoldt:

Teorema 4.5. *Si $n \geq 1$ tenemos*

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

Demostración. Invertimos la igualdad obtenida en el teorema 4.2 mediante la fórmula de inversión de Möbius con lo que podemos escribir:

$$\begin{aligned}\Lambda(n) = \sum_{d|n} \mu(n) \log \frac{n}{d} = \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d = \\ = I(n) \log n - \sum_{d|n} \mu(d) \log d.\end{aligned}$$

Como $I(n) \log n = 0$ para todo n, queda probado el teorema. □

Una vez vistas las funciones aritméticas, veamos las funciones multiplicativas:

Definición (Función multiplicativa)**.** Una función multiplicativa es una función aritmética no nula tal que

$$f(mn) = f(m)f(n) \qquad \text{si } \operatorname{mcd}(m, n) = 1.$$

Una función f es **completamente multiplicativa** si

$$f(mn) = f(m)f(n) \qquad \text{para todo } m, n \in \mathbb{Z}.$$

Teorema 4.6 (Fórmula del producto para funciones completamente multiplicativas)**.** *Para $f : \mathbb{N} \to \mathbb{C}$ completamente multiplicativa, se cumple*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p \in \mathbb{P}} \Big(1 - \frac{f(p)}{p^s}\Big)^{-1}$$

si la serie es absolutamente convergente. Para funciones multiplicativas, tenemos la siguiente igualdad:

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p \in \mathbb{P}} \sum_{k=0}^{\infty} \frac{f(p^k)}{p^{ks}} = \prod_{p \in \mathbb{P}} \Big(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \cdots\Big).$$

Relacionemos las funciones multiplicativas con el anteriormente visto producto de Dirichlet por medio del siguiente teorema:

Teorema 4.7. *Si f y g son funciones multiplicativas, también lo es su producto de Dirichlet $f * g$.*

Observación. La función μ es multiplicativa, pero no completamente multiplicativa. Por el contrario, Λ no es multiplicativa.

Demostración. Para probar que μ no es completamente multiplicativa basta encontrar m, n enteros tal que $\mu(mn) \neq \mu(m)\mu(n)$. Tomemos por ejemplo $\mu(9) = \mu(3 \cdot 3) = 0 \neq 1 = \mu(3)\mu(3)$. Para probar que es multiplicativa, tomemos dos descomposiciones en factores primos $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ y $n = q_1^{\beta_l} \cdots q_l^{\beta_l}$, tenemos que $\text{mcd}(m, n) = 1$ si y sólo si $p_j \neq q_i$ para todo i, j. Analizamos ahora la definición de la función de Möbius, diferenciando nueve casos (los obtenemos al combinar los tres posibles valores de m con los tres posibles valores de n). Los casos en los que o m o n valen 1 o su descomposición en factores primos no es simple, son triviales, para todos ellos se tiene que $\mu(mn) = \mu(m)\mu(n)$. Luego comprobemos el caso restante, el caso en el que tanto m como n se descomponen en factores primos simples, es decir, $m, n > 1$ con $m = p_1 \cdots p_k$ y $n = q_1 \cdots q_l$ y $p_j \neq q_i$ para todo i, j. Tenemos por lo tanto $\mu(mn) = (-1)^{k+l} = \mu(m)\mu(n)$. Con lo que queda demostrado.

Veamos ahora que la función de von Mangoldt no es multiplicativa. Es fácil encontrar contraejemplos, pongamos por caso $\Lambda(2) = \log 2$ y $\Lambda(3) = \log 3$. Tenemos que $\Lambda(2 \cdot 3) = \Lambda(6) = 0 \neq \Lambda(2)\Lambda(3)$. □

Designemos con F una función con valores reales o complejos definida en el eje real positivo $(0, \infty)$ de forma que $F(x) = 0$ para $0 < x < 1$. Sea α una función aritmética y

$$G(x) = \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right).$$

La función G se anula también para $0 < x < 1$. Escribiremos $\alpha \circ F$ en vez de G. Tenemos por lo tanto

$$(\alpha \circ F)(x) = \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right).$$

Si $F(x) = 0$ para todo x no entero, la restricción de F a los enteros es una función aritmética y tenemos que

$$(\alpha \circ F)(m) = (\alpha * F)(m)$$

para todo entero $m \geq 1$. Por lo que la operación $\circ$ se puede considerar una **generalización de la convolución de Dirichlet** $*$. La operación $\circ$ en general no es ni conmutativa, ni asociativa.

Teorema 4.8 (Propiedad asociativa que relaciona $\circ$ y $*$)**.** *Para todo par de funciones aritméticas α y β tenemos*

$$\alpha \circ (\beta \circ F) = (\alpha * \beta) \circ F. \tag{4.3}$$

Demostración. Para $x > 0$ tenemos

$$\begin{aligned}(\alpha \circ (\beta \circ F))(x) &= \sum_{n \le x} \alpha(n) \sum_{m \le x/n} \beta(m) F\left(\frac{x}{mn}\right) = \sum_{mn \le x} \alpha(n)\beta(m) F\left(\frac{x}{mn}\right) \\ &= \sum_{k \le x} \left(\sum_{n \mid k} \alpha(n) \beta\left(\frac{k}{n}\right) \right) F\left(\frac{x}{k}\right) = \sum_{k \le x} (\alpha * \beta)(k) F\left(\frac{x}{k}\right) \\ &= ((\alpha * \beta) \circ F)(x). \end{aligned}$$

□

También observamos que el elemento neutro respecto a $*$ es también un elemento neutro de izquierda respecto a $\circ$ ya que

$$(I \circ f)(x) = \sum_{n \le x} \left\lfloor \frac{1}{n} \right\rfloor f\left(\frac{x}{n}\right) = f(x).$$

Con este teorema podemos demostrar el siguiente:

Teorema 4.9 (Fórmula de inversión generalizada)**.** *Si α tiene inversa de Dirichlet α^{-1} entonces*

$$G(x) = \sum_{n \le x} \alpha(n) \left(\frac{x}{n}\right) \quad \textit{si y sólo si} \quad F(x) = \sum_{n \le x} \alpha^{-1}(n) G\left(\frac{x}{n}\right).$$

Demostración. Si $G = \alpha \circ F$, entonces

$$\alpha^{-1} \circ G = \alpha^{-1} \circ (\alpha \circ F). \tag{4.4}$$

Y aplicando el teorema 4.8 tenemos que

$$(4.4) = (\alpha^{-1} * \alpha) \circ F = I \circ F = F.$$

Análogamente, si $F = \alpha^{-1} \circ G$ tenemos

$$\alpha \circ F = \alpha \circ (\alpha^{-1} \circ G) = (\alpha * \alpha^{-1}) \circ G = G.$$

□

Presentamos ahora un caso particular de este teorema, donde la inversa de Dirichlet de α es $\alpha^{-1}(n) = \mu(n)\alpha(n)$.

Teorema 4.10 (Fórmula de inversión de Möbius generalizada)**.** *Si α es completamente multiplicativa,*

$$\sum_{n \le x} \alpha(n) F\left(\frac{x}{n}\right) \quad \textit{si y sólo si} \quad F(x) = \sum_{n \le x} \mu(n)\alpha(n) G\left(\frac{x}{n}\right). \tag{4.5}$$

A lo largo de esta sección hemos visto las funciones aritméticas, el producto de Dirichlet de las mismas, las funciones multiplicativas,... Pero lo que nos interesa es conocer el comportamiento de estas funciones cuando n tiende a infinito. Pero a veces esto es difícil, por lo que para facilitarnos el trabajo, elegimos trabajar con su media aritmética (de aquí en adelante, eso haremos). Comenzamos definiendo este concepto:

Definición (Media aritmética)**.** Sea f una función aritmética. Definimos su media aritmética como

$$\bar{f}(n) = \frac{1}{n}\sum_{k=1}^{n} f(k).$$

E introducimos los siguientes términos:

Definición (o pequeña de Landau)**.** Sean $f : [a, \infty) \to \mathbb{R}$ y $g : [a, \infty) \to \mathbb{R}^+$. Escribiremos

$$f(x) = o(g(x))$$

cuando $x \to \infty$ si $\lim_{x\to\infty} f(x)/g(x) = 0$.

Definición (O grande de Landau)**.** Sean $f, g : [a, \infty) \to \mathbb{R}$. Escribiremos

$$f(x) = O(g(x))$$

cuando $x \to \infty$ si existen $M > 0$ y $b \geq a$ tales que $|f(x)| \leq Mg(x)$ para todo $x \geq b$.

A partir de ahora usaremos $\mathcal{O}$ para denotar la O grande de Landau. La siguiente fórmula nos otorga una expresión precisa del error cometido al aproximar los valores asintóticos de una suma parcial por una integral.

Teorema 4.11 (Fórmula de sumación de Euler)**.** *Sea f cuya derivada f' es continua en el intervalo $[y, x]$ con $0 < y < x$. Tenemos que*

$$\begin{aligned}\sum_{y<n\leq x} f(n) = \int_y^x f(t)\,dt + \int_y^x (t - \lfloor t\rfloor)f'(t)\,dt \\ + f(x)(\lfloor x\rfloor - x) - f(y)(\lfloor y\rfloor - y).\end{aligned} \tag{4.6}$$

Demostración. Sea $m = \lfloor y\rfloor, k = \lfloor x\rfloor$. Para enteros n y $n-1$ de $\lfloor y, x\rfloor$ tenemos

$$\begin{aligned}\int_{n-1}^{n} \lfloor t\rfloor f'(t)\,dt = \int_{n-1}^{n} (n-1)f'(t)\,dt &= (n-1)(f(n) - f(n-1)) \\ &= (n-1)f(n) - (n-1)f(n-1) \\ &= nf(n) - (n-1)f(n-1) - f(n).\end{aligned}$$

Si ahora sumamos desde $n = m + 1$ hasta $n = k$ obtenemos

$$\begin{aligned}\int_m^k \lfloor t \rfloor f'(t)\, dt &= \sum_{n=m+1}^{k} nf(n) - (n-1)f(n-1) - \sum_{y<n\leq x} f(n) \\ &= kf(k) - mf(m) - \sum_{y<n\leq x} f(n),\end{aligned}$$

con lo que tenemos

$$\begin{aligned}\sum_{y<n\leq x} f(n) &= -\int_m^k \lfloor t \rfloor f'(t)\, dt + kf(k) - mf(m) \\ &= -\int_y^x \lfloor t \rfloor f'(t)\, dt + kf(x) - mf(y).\end{aligned}$$

Por otro lado, si integramos por partes obtenemos que

$$\int_y^x f(t)\, dt = xf(x) - yf(y) - \int_y^x tf'(t)\, dt.$$

Sumando las dos últimas igualdades obtenidas, probamos el teorema. □

Veamos algunas fórmulas asintóticas que son consecuencias fáciles de la fórmula de sumación de Euler.

Teorema 4.12. *Si $x \geq 1$ podemos escribir:*

a) $\displaystyle\sum_{n\leq x} \frac{1}{n} = \log x + C + \mathcal{O}\left(\frac{1}{x}\right).$

b) $\displaystyle\sum_{n\leq x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} - \zeta(s) + \mathcal{O}(x^{-s})$ *si* $s > 0$ *y* $s \neq 1$.

En el apartado a) la constante de Euler definida por la ecuación

$$C = \lim_{n\to\infty} \Big(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n\Big).$$

En el apartado b), $\zeta(s)$ es la función zeta de Riemann que podemos definir por

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

en caso de que $s > 1$ y por la ecuación

$$\zeta(s) = \lim_{x\to\infty} \Big(\sum_{n\leq x} \frac{1}{n^s} - \frac{x^{1-s}}{1-s} \Big)$$

si $0 < s < 1$.

4.2. Sumas parciales de un producto de Dirichlet

En este apartado veremos una fórmula general que relaciona las sumas parciales de dos funciones aritméticas arbitrarias con su producto de Dirichlet. Veremos también algunas identidades elementales que involucran a la función de Möbius y la indicatriz de Euler. Comenzamos viendo el siguiente teorema:

Teorema 4.13. *Sea* $h = f * g$ *y*

$$H(x) = \sum_{n \leq x} h(n), \quad F(x) = \sum_{n \leq x} f(n) \quad y \quad G(x) = \sum_{n \leq x} g(n).$$

Entonces tenemos

$$H(x) = \sum_{n \leq x} f(n) G\left(\frac{x}{n}\right) = \sum_{n \leq x} g(n) F\left(\frac{x}{n}\right). \tag{4.7}$$

Demostración. Sea

$$U(x) = \begin{cases} 0, & \text{si } 0 < x < 1, \\ 1, & \text{si } x \geq 1. \end{cases}$$

Se cumple que $F = f \circ U$, $G = g \circ U$ y

$$\begin{aligned} f \circ G &= f \circ (g \circ U) = (f * g) \circ U = H, \\ g \circ F &= g \circ (f \circ U) = (g * f) \circ U = H. \end{aligned}$$ □

Si $g(n) = 1$ para todo n tenemos que $G(x) = \lfloor x \rfloor$. Sustituyendo en (4.7) obtenemos el siguiente resultado:

Teorema 4.14. *Sea* $F(x) = \sum_{n \leq x} f(n)$ *tenemos*

$$\sum_{n \leq x} \sum_{d \mid n} f(d) = \sum_{n \leq x} f(n) \left\lfloor \frac{x}{n} \right\rfloor = \sum_{n \leq x} F\left(\frac{x}{n}\right). \tag{4.8}$$

Ahora, si en el teorema 4.14 hacemos $f(n) = \mu(n)$ obtenemos el teorema que enunciamos y demostramos a continuación:

Teorema 4.15. *Para* $x \geq 1$,

$$\sum_{n \leq x} \mu(n) \left\lfloor \frac{x}{n} \right\rfloor = 1. \tag{4.9}$$

Demostración. Utilizando el teorema 4.1 tenemos

$$\sum_{n \leq x} \mu(n) \left\lfloor \frac{x}{n} \right\rfloor = \sum_{n \leq x} \sum_{d \mid n} \mu(d) = \sum_{n \leq x} \left\lfloor \frac{1}{n} \right\rfloor = 1.$$ □

Por otro lado, si en el teorema 4.14 hacemos $f(n) = \Lambda(n)$ obtenemos la siguiente identidad:

Teorema 4.16. *Para $x \geq 1$ tenemos*

$$\sum_{n\leq x} \Lambda(n)\left\lfloor \frac{x}{n}\right\rfloor = \log(\lfloor x\rfloor !) \tag{4.10}$$

Demostración. Utilizando los teoremas 4.14 y 4.2 tenemos

$$\sum_{n\leq x} \Lambda(n)\left\lfloor \frac{x}{n}\right\rfloor = \sum_{n\leq x}\sum_{d|n} \Lambda(d) = \sum_{n\leq x} \log n = \log(\lfloor x\rfloor !) \qquad \square$$

Una vez vistas las identidades fundamentales de las que hablábamos en la introducción de esta sección, pasamos a usar la fórmula de sumación de Euler para determinar una fórmula asintótica para $\log(\lfloor x\rfloor !)$:

Teorema 4.17. *Si $x \geq 2$ tenemos*

$$\log\lfloor x\rfloor ! = x\log x - x + \mathcal{O}(\log x) \tag{4.11}$$

y con ello

$$\sum_{n\leq x} \Lambda(n)\left\lfloor \frac{x}{n}\right\rfloor = x\log x - x + \mathcal{O}(\log x). \tag{4.12}$$

Demostración. Haciendo $f(t) = \log t$ en la fórmula de sumación de Euler (4.6) tenemos

$$\begin{aligned}\sum_{n\leq x} \log n &= \int_1^x \log t\, dt + \int_1^x \frac{t - \lfloor t\rfloor}{t}\, dt - (x - \lfloor x\rfloor)\log x \\ &= x\log x - x + 1 + \int_1^x \frac{t-\lfloor t\rfloor}{t}\, dt + \mathcal{O}(\log x).\end{aligned}$$

Y como

$$\int_1^x \frac{t-\lfloor t\rfloor}{t}\, dt = O\left(\int_1^x \frac{1}{t}\, dt\right) = \mathcal{O}(\log x).$$

Con lo que queda probado (4.11). Al probarlo y con (4.10) queda demostrado (4.12). $\square$

Teorema 4.18. *Para $x \geq 2$ tenemos*

$$\sum_{p\leq x} \left\lfloor \frac{x}{p}\right\rfloor \log p = x\log x + \mathcal{O}(x). \tag{4.13}$$

Donde la suma se halla extendida a todos los primos $\leq x$.

Demostración. Puesto que $\Lambda(n) = 0$ excepto si n es una potencia de primo, tenemos que

$$\sum_{n\leq x}\Big\lfloor\frac{x}{n}\Big\rfloor\Lambda(n) = \sum_{\substack{p^m\leq x\\ p}}\sum_{m=1}^{\infty}\Big\lfloor\frac{x}{p^m}\Big\rfloor\Lambda(p^m).$$

Pero como $p^m \leq x$ implica que $p \leq x$ y $\lfloor x/p^m\rfloor = 0$, si $p < x$ podemos escribir

$$\sum_{\substack{p^m\leq x\\ p}}\sum_{m=1}^{\infty}\left\lfloor\frac{x}{p^m}\right\rfloor\Lambda(p^m) = \sum_{p\leq x}\sum_{m=1}^{\infty}\left\lfloor\frac{x}{p^m}\right\rfloor\log p = \sum_{p\leq x}\left\lfloor\frac{x}{p}\right\rfloor\log p + \sum_{p\leq x}\sum_{m=2}^{\infty}\left\lfloor\frac{x}{p^m}\right\rfloor\log p.$$

Centrémonos en la última suma. Tenemos

$$\begin{aligned}\sum_{p\leq x}\log p\sum_{m=2}^{\infty}\left\lfloor\frac{x}{p^m}\right\rfloor &\leq \sum_{p\leq x}\log p\sum_{m=2}^{\infty}\frac{x}{p^m} = x\sum_{p\leq x}\log p\sum_{m=2}^{\infty}\left(\frac{1}{p}\right)^m\\ &= x\sum_{p\leq x}(\log p)\frac{1}{p^2}\frac{1}{1-\frac{1}{p}} = x\sum_{p\leq x}\frac{\log p}{p(p-1)}\\ &\leq x\sum_{n=2}\frac{\log n}{n(n-1)} = \mathcal{O}(x),\end{aligned}$$

por lo que ese último término es $\mathcal{O}(x)$, con lo que obtenemos

$$\sum_{n\leq x}\Big\lfloor\frac{x}{n}\Big\rfloor\Lambda(n) = \sum_{p\leq x}\left\lfloor\frac{x}{p}\right\rfloor\log p + \mathcal{O}(x),$$

que junto con (4.12) demuestra el teorema. □

Comenzamos este apartado con el teorema 4.13 donde tomábamos

$$H(x) = \sum_{n\leq x}(f*g)(n), \quad F(x) = \sum_{n\leq x}f(n) \quad y \quad G(x) = \sum_{n\leq x}g(n),$$

con lo que obtenemos

$$H(x) = \sum_{n\leq x}\sum_{d|n}f(d)g\Big(\frac{n}{d}\Big) = \sum_{\substack{q,d\\ qd\leq x}}f(d)g(q).$$

Teorema 4.19. *Sean a y b dos númros reales positivos de forma que $ab = x$. Bajo estas condiciones,*

$$\sum_{\substack{q,d\\ qd\leq x}}f(d)g(q) = \sum_{n\leq a}f(n)G\Big(\frac{x}{n}\Big) + \sum_{n\leq b}g(n)F\Big(\frac{x}{n}\Big) - F(a)G(b).$$

Aunque la demostración de este teorema no es muy complicada, no se incluye en esta memoria por no alargarla más. La podemos encontrar en [1].

4.3. Teorema tauberiano de Shapiro

Como ya sabemos, las convergencias fuertes siempre implican convergencias más débiles. Por ejemplo, el teorema de Abel establece que si una serie $\sum_{n=0}^{\infty} a_n x^n$ converge para $x \in (-1,1)$ y $\sum_{n=0}^{\infty} a_n$ converge, entonces

$$\lim_{x\to 1^-} a_n x^n = \sum_{n=0}^{\infty} a_n.$$

En 1897 A. Tauber probó que si la serie

$$f(x) = \sum_{n=0}^{\infty} a_n x^n$$

converge en el intervalo $(-1,1)$, $f(x) \to A$ cuando $x \to 1^-$, y los coeficientes de la serie cumplen $a_n = o(1/n)$, entonces $\sum_{n=0}^{\infty} a_n$ converge a A. En este caso, una convergencia débil implica una convergencia fuerte (con ayuda de hipótesis adicionales). Estos tipos de teoremas se conocen como teoremas tauberianos. Nosotros veremos el teorema tauberiano de Shapiro, demostrado por el mismo en el año 1950.

Teorema 4.20. *Sea $\{a(n)\}$ una sucesión no negativa tal que*

$$\sum_{n\le x} a(n)\left\lfloor \frac{x}{n}\right\rfloor = x\log x + \mathcal{O}(x) \tag{4.14}$$

para $x \ge 1$. Se cumplen las siguientes afirmaciones:

a) Para $x \ge 1$ tenemos

$$\sum_{n\le x} \frac{a(n)}{n} = \log x + \mathcal{O}(1).$$

b) Existe una constante $B > 0$ tal que

$$\sum_{n\le x} a(n) \le Bx \qquad \text{para todo } x \ge 1.$$

Demostración. Comencemos probando el apartado b). Sean

$$S(x) = \sum_{n\le x} a(n), \qquad T(n) = \sum_{n\le x} a(n)\left\lfloor \frac{x}{n}\right\rfloor.$$

Si tomamos

$$S(x) - S\left(\frac{x}{2}\right) \le T(x) - 2T\left(\frac{x}{2}\right), \tag{4.15}$$

podemos escribir

$$T(x) - 2T\left(\frac{x}{2}\right) = \sum_{n\le x}\left\lfloor\frac{x}{n}\right\rfloor a(n) - 2\sum_{n\le x/2}\left\lfloor\frac{x}{2n}\right\rfloor$$
$$= \sum_{n\le x/2}\left(\left\lfloor\frac{x}{n}\right\rfloor - 2\left\lfloor\frac{x}{2n}\right\rfloor\right)a(n) + \sum_{x/2<n\le x}\left\lfloor\frac{x}{n}\right\rfloor a(n).$$

Como $\lfloor 2y\rfloor - \lfloor 2\rfloor y$ es 0 o 1, tenemos

$$T(x) - 2T\left(\frac{x}{2}\right) \ge \sum_{x/2<n\le x}\left\lfloor\frac{x}{n}\right\rfloor a(n) = \sum_{x/2<n\le x} a(n) = S(x) - S\left(\frac{x}{2}\right).$$

De esta forma queda demostrada la desigualdad (4.15). Ahora, como (4.14) implica

$$T(x) - 2T\left(\frac{x}{2}\right) = x\log x + \mathcal{O}(x) - 2\left(\frac{x}{2}\log\frac{x}{2} + \mathcal{O}(x)\right) = \mathcal{O}(x),$$

la ecuación (4.15) implica $S(x) - S(x/2) = \mathcal{O}(x)$. Por lo que existe una constante $K > 0$ de forma que

$$S(x) - S\left(\frac{x}{2}\right) \le Kx \quad \text{para todo} \quad x \ge 1.$$

Si sustituimos sucesivamente x por $x/2, x/4, x/8, \ldots$ obtenemos

$$S\left(\frac{x}{2}\right) - S\left(\frac{x}{4}\right) \le K\,\frac{x}{2},$$
$$S\left(\frac{x}{4}\right) - S\left(\frac{x}{8}\right) \le K\,\frac{x}{4}, \ldots$$

Observamos que $S(x/2^n) = 0$ cuando $2^n \ge x$. Si sumamos las desigualdades tenemos

$$S(x) \le Kx\left(1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots\right) = 2Kx.$$

Tomando $B = 2K$, demostramos b). Una vez probado, procedemos a demostrar a). Recordemos que

$$T(x) = \sum_{n\le x} a(n)\left\lfloor\frac{x}{n}\right\rfloor.$$

Si tomamos $\left\lfloor\frac{x}{n}\right\rfloor = \frac{x}{n} + \mathcal{O}(1)$ obtenemos

$$T(x) = \sum_{n\le x} a(n)\left\lfloor\frac{x}{n}\right\rfloor = \sum_{n\le x} a(n)\Big(\frac{x}{n} + \mathcal{O}(1)\Big) = x\sum_{n\le x}\frac{a(n)}{n} + \mathcal{O}\Big(\sum_{n\le x} a(n)\Big).$$

Ahora, aplicando el apartado b) tenemos

$$T(x) = x\sum_{n\le x}\frac{a(n)}{n} + \mathcal{O}(x).$$

Dividimos entre x, de forma que

$$\sum_{n\leq x}\frac{a(n)}{n}=\frac{1}{x}T(x)+\mathcal{O}(1)=\log x+\mathcal{O}(1),$$

con lo que queda probado el apartado a). □

Observación. Aparte de los apartados a) y b), también se cumple que existe una constante $C>0$ y un $x_0>0$ tal que

$$\sum_{n\leq x}a(n)\geq Cx \qquad \text{para todo } x\geq x_0.$$

Reescribimos la ecuación (4.13), hallada en la sección anterior, de la siguiente manera:

$$\sum_{n\leq x}\Lambda_1(n)\left\lfloor\frac{x}{n}\right\rfloor=x\log x+\mathcal{O}(x),$$

donde

$$\Lambda_1=\begin{cases}\log p, & \text{si } n \text{ es primo,}\\ 0, & \text{si no.}\end{cases}$$

Como $\Lambda_1(n)\geq 0$, aplicando el primer apartado del teorema de Shapiro obtenemos el siguiente teorema:

Teorema 4.21 (Primer teorema de Mertens)**.** *Para $x\geq 1$ tenemos*

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

Recordaremos este resultado más tarde. Presentemos ahora los caracteres de Dirichlet, introduciendo antes un pequeño resumen sobre teoría de grupos.

4.4. Caracteres de Dirichet

Comenzamos definiendo los conceptos que vamos a utilizar:

Definición (Grupo)**.** Un grupo G es un conjunto no vacío provisto de una operación binaria (usualmente llamada multiplicación)

$$\begin{aligned}G\times G&\to G\\ (x,y)&\mapsto xy,\end{aligned}$$

que satisface las siguientes propiedades, denominadas axiomática de grupo: es asociativa (es decir, $(xy)z=x(yz)$), existe un elemento neutro (comúnmente denotado por e que cumple $ex=x=xe$ para todo $x\in G$) y para cada elemento $x\in G$, existe un elemento, denotado por x^{-1} y llamado inverso de x, tal que $xx^{-1}=x^{-1}x=e$.

Si la multiplicación es conmutativa ($xy = yx$ para todo $x, y \in G$), el grupo se dice conmutativo o abeliano.

Definición (Subgrupo)**.** Sea G un grupo y H un subconjunto no vacío H de grupo G. Decimos que H es un subgrupo de G si para todo $x, y \in H$, xy y x^{-1} viven en H.

Definición (Grupo finito)**.** Un grupo G es finito si G es un conjunto finito. El número de elementos de G se denomina orden de G y se designa por $|G|$.

Una vez vistas, pasamos a ver los caracteres de grupos abelianos finitos.

Definición (Carácter)**.** Sea G un grupo. Una función f con valores complejos definida en G se denomina carácter f en G si f no es idénticamente nula y si f tiene la propiedad multiplicativa

$$f(ab) = f(a)f(b)$$

para todo $a,\ b$ de G.

Los caracteres poseen una serie de propiedades que se nombran a continuación. Las demostraciones de las mismas se pueden encontrar en [1].

Sea f un carácter de un grupo finito G de orden n y con elemento identidad e. Como $f(e) = 1$ y dado que el orden de un elemento divide al orden del grupo, para todo a perteneciente a G tenemos que $(f(a))^n = f(a^n) = f(e) = 1$ lo que implica que $|f(a)| = 1$.

Cada grupo G admite un carácter por lo menos, que es la función idénticamente igual a 1 en G. A este carácter se le suele llamar **carácter principal**.

Teorema 4.22. *Si G es un grupo abeliano y tiene orden n, entonces hay exactamente n caracteres diferentes en G.*

Sea G es un grupo abeliano finito de orden n. Designemos al carácter principal por f_1 y a los no principales (al resto) por $f_2, f_3, \ldots, f_n$. Los caracteres no principales cumplen que $f(a) \neq 1$ para algún $a \in G$.

El conjunto de caracteres de G forma un grupo multiplicativo G con la operación

$$(f_i)(f_j)(a) = f_i(a)f_j(a)$$

para cada a de G. Llamemos a ese grupo $\widehat{G}$. El elemento neutro de este grupo es el llamado carácter principal, f_1. El inverso de f_i es $1/f_i$.

Hemos visto que, para cualquier carácter $a \in G$, se cumple $|f(a)| = 1$, así que $(f(a))^{-1}$ es el complejo conjugado $\overline{f(a)}$. Por lo tanto la función $\bar{f}$ definida por $\bar{f}(a) = \overline{f(a)}$ es también un carácter de G. Por lo que, para cada a de G, se tiene

$$\bar{f}(a) = \frac{1}{f(a)} = f(a^{-1}).$$

Además, la función $\bar{f}$ también es un carácter de G.

Una propiedad importante de los caracteres es la ortogonalidad. En particular, esto juega un papel importante para los caracteres de Dirichlet y será el punto de partida para la prueba de la infinidad de números primos en las progresiones aritméticas.

Sea G un grupo abeliano finito de orden n, de elementos $a_1, a_2, \ldots, a_n$, y sean $f_1, f_2, \ldots, f_n$ los caracteres de G con f_1 el carácter principal. Llamemos $A = A(G)$ a la matriz $n \times n$ cuyo elemento a_{ij} de la i-ésima fila j-ésima columna es

$$a_{ij} = f_i(a_j).$$

Una vez definida la notación que vamos a seguir, presentemos los teoremas.

Teorema 4.23. *La suma de los elementos de la i-ésima fila de A viene dada por*

$$\sum_{r=1}^{n} f_i(a_r) = \begin{cases} n, & \text{si } i = 1, \\ 0, & \text{en otro caso.} \end{cases}$$

Demostración. Sea $S = \sum_{r=1}^{n} f_i(a_r)$. Si $i = 1$, todos los términos de la suma son 1 (f_1 es el carácter principal) y por lo tanto $S = n$. En caso de que $i \neq 1$, existe un elemento b de G tal que $f_i(b) \neq 1$. Tenemos

$$S = \sum_{r=1}^{n} f_i(ba_r) = f_i(b) \sum_{r=1}^{n} f_i(a_r) = f_i(b)S,$$

por lo que $S(1 - f_i(b)) = 0$. Y como $f_i(b) \neq 1$, obtenemos que $S = 0$. □

Con este teorema hemos determinado la suma de los elementos de cada fila de A.

Teorema 4.24. *Sea A^* la matriz conjugada traspuesta de la matriz A. Tenemos*

$$AA^* = nI,$$

donde I es la matriz identidad $n \times n$. Luego $n^{-1}A^*$ es la inversa de A.

Demostración. Sea $B = AA^*$. El elemento b_{ij} de B viene dado por

$$b_{ij} = \sum_{r=1}^{n} f_i(a_r)\bar{f}_j(a_r) = \sum_{r=1}^{n} (f_i\bar{f}_j)(a_r) = \sum_{r=1}^{n} f_k(a_r),$$

donde $f_k = f_i\bar{f}_j = f_i/f_j$. Tenemos que $f_i/f_j = 1$ si, y sólo si, $i = j$. Por el teorema 4.23 podemos escribir

$$b_{ij} = \begin{cases} n, & \text{si } a_i = a_j, \\ 0, & \text{en otro caso.} \end{cases}$$

Lo que equivale a decir que $B = nI$. □

Hemos demostrado que A tiene inversa. Utilizaremos el hecho de que una matriz conmuta con su inversa para obtener el siguiente resultado:

Teorema 4.25 (Relaciones de ortogonalidad para caracteres)**.** *Utilizando el hecho de que una matriz conmuta con su inversa, obtenemos*

$$\sum_{r=1}^{n} \bar{f}_r(a_i) f_r(a_j) = \begin{cases} n, & si \quad a_i = a_j, \\ 0, & si\ no. \end{cases}$$

Demostración. Como ya hemos mencionado, una matriz conmuta con su inversa, por lo tanto la relación $AA^* = nI$ implica $A^*A = nI$. El elemento de la i-ésima fila y la j-ésima columna de A^*A es la sumatorio de la izquierda de la igualdad anterior. □

Una vez vistos los caracteres de grupos abelianos finitos y su relación de ortogonalidad, ya podemos presentar los caracteres de Dirichlet. A partir de ahora, G es el grupo de las clases reducidas de restos módulo k, con k un entero positivo fijo. Un sistema residual reducido módulo k es un conjunto de $\phi(k)$ enteros $\{a_1, a_2, \ldots, a_{\phi(k)}\}$ incongruentes módulo k, cada uno de ellos primo con k. Para cada entero a la clase de restos correspondientes $\hat{a}$ es

$$\hat{a} = \{x \in \mathbb{Z} : x \equiv a \ (\text{mód } k)\}.$$

La multiplicación de las clases de restos se define por la relación

$$\hat{a}\hat{b} = \widehat{ab}.$$

Definición (Carácter de Dirichlet)**.** Sea G el grupo de clases reducidas de restos módulo k. En correspondencia con cada carácter f de G definimos una función aritmética $\chi = \chi_f$ de la siguiente manera:

$$\chi(n) = f(\hat{n}) \quad \text{si } \operatorname{mcd}(n,k) = 1,$$
$$\chi(n) = 0 \quad \text{si } \operatorname{mcd}(n,k) > 1.$$

A la función χ se le llama carácter de Dirichlet módulo k. El carácter principal χ_1 es el que verifica

$$\chi_1(n) = \begin{cases} 1, & \text{si } \operatorname{mcd}(n,k) = 1, \\ 0, & \text{si } \operatorname{mcd}(n,k) > 1. \end{cases}$$

A continuación vemos algunas de sus propiedades.

Teorema 4.26. *Existen $\phi(k)$ caracteres módulo k, cada uno de los cuales es completamente multiplicativo y periódico de período k. Recíprocamente, si χ es completamente multiplicativo y periódico de período k y si $\chi(n) = 0$ para $\operatorname{mcd}(n,k) > 1$, entonces χ es uno de los caracteres de Dirichlet módulo k.*

Demostración. Que cada carácter sea completamente multiplicativo y periódico de período k quiere decir que se verifica

$$\chi(mn) = \chi(m)\chi(n) \text{ para todo } m, n \in \mathbb{Z} \tag{4.16}$$

y que

$$\chi(n+k) = \chi(n) \text{ para todo } n \text{ entero.} \tag{4.17}$$

Procedemos a demostrarlo. Sabemos que existen $\phi(k)$ caracteres f para el grupo G de las clases reducidas de restos módulo k, por lo que existen $\phi(k)$ caracteres χ_f módulo k. El carácter f es completamente multiplicativo cuando m y n son primos con k. Si uno de ellos, m o n, no es primo con k, tampoco lo es mn, luego los dos miembros de (4.16) son cero. Esto implica la propiedad multiplicativa (4.16) de χ_f. Como $a \equiv b \pmod{k}$ implica que $\text{mcd}(a,k) = \text{mcd}(b,k)$ y $\chi_f(n) = f(\hat{n})$, la periodicidad queda probada.

Ahora probaremos el recíproco. Observamos que la función f definida en el grupo G por la ecuación $f(\hat{n}) = \chi(n)$ en caso de que $\text{mcd}(n,k) = 1$, es un carácter de G. Por lo tanto χ es un carácter de Dirichlet módulo k. □

Teorema 4.27. *Sean $\chi_1, \chi_2, \ldots, \chi_{\phi(k)}$ los $\phi(k)$ caracteres de Dirichlet módulo k y sean m y n dos enteros de forma que* $\text{mcd}(m,n) = 1$. *Tenemos:*

$$\sum_{r=1}^{\phi(k)} \chi_r(m)\bar{\chi_r}(n) = \begin{cases} \phi(k), & \text{si } m \equiv n \pmod{k}, \\ 0, & \text{si no.} \end{cases}$$

Demostración. Si $\text{mcd}(m,k) = 1$, tomando $a_i = \hat{n}$ y $a_j = \hat{m}$ en el teorema 4.25 (en las relaciones de ortogonalidad para caracteres), se cumple que $a_i = a_j$ si y sólo si $m \equiv n \pmod{k}$. Si $\text{mcd}(m,k) > 1$, cada término del sumatorio se anula y $m \not\equiv n \pmod{k}$. □

Ciertas sumas contienen caracteres de Dirichlet, algunas de ellas las presentamos a continuación. Las usaremos en la demostración del teorema de Dirichlet, en el capítulo 5.

Antes de verlas, enunciamos dos resultados, muy conocidos, que nos servirán para la demostración de los teoremas relacionados con las sumas que vamos a ver. Ninguno de los dos se prueba, para ver la demostración, se puede consultar [1].

Teorema 4.28 (Identidad de Abel)**.** *Para toda función aritmética $a(n)$, sea*

$$A(x) = \sum_{n \le x} a(n),$$

donde $A(x) = 0$ si $x < 1$. Si f posee derivada continua en el intervalo $[y,x]$ con $0 < y < x$, entonces

$$\sum_{y < n \le x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)\,dt.$$

Teorema 4.29 (Criterio de convergencia de Cauchy)**.** *Una sucesión de números reales es convergente si y sólo si es una sucesión de Cauchy. Es decir, el conjunto de los números reales es un espacio métrico completo.*

Teorema 4.30. *Sea χ un carácter no principal módulo k, y sea f una función no negativa que, para todo $x \geq x_0$, admite derivada continua no negativa $f'(x)$. En estas circunstancias, si $y \geq x \geq x_0$ entonces*

$$\sum_{x<n\leq y} \chi(n)f(n) = \mathcal{O}(f(x)). \tag{4.18}$$

Si además $f(x) \to 0$ cuando $x \to \infty$, entonces

$$\sum_{n\leq x} \chi(n)f(n) = \sum_{n=1}^{\infty} \chi(n)f(n) + \mathcal{O}(f(x)). \tag{4.19}$$

Demostración. Sea

$$A(x) = \sum_{n\leq x} \chi(n).$$

Como χ no es principal tenemos que

$$A(k) = \sum_{n=1}^{k} \chi(n) = 0. \tag{4.20}$$

Por la periodicidad obtenemos que $A(nk) = 0$ para $n > 1$ entero, luego $|A(x)| = \mathcal{O}(1)$ para todo x. Utilizamos la identidad de Abel que acabamos de ver para expresar la suma de (4.18) en forma de integral, con lo que tenemos

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

Con esto hemos demostrado (4.18). Probemos ahora (4.19). Por hipótesis tenemos que $f(x) \to 0$ cuando $x \to \infty$; entonces la igualdad (4.18) prueba que la serie

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

converge por del criterio de convergencia de Cauchy. Por lo que, para probar (4.19) observamos que

$$\sum_{n=1}^{\infty} \chi(n)f(n) = \sum_{n\leq x} \chi(n)f(n) + \lim_{y\to\infty} \sum_{x<n\leq y} \chi(n)f(n).$$

Aplicando (4.18) tenemos que

$$\lim_{y\to\infty} \sum_{x<n\leq y} \chi(n)f(n) = \mathcal{O}(f(x)).$$

Con lo que terminamos la demostración. □

Si, en el teorema que acabamos de probar, tomamos $f(x)$ primero como $1/x$, después como $(\log x)/x$ y por último como $1\sqrt{x}$ para $x \geq 1$, obtenemos las tres igualdades siguientes:

Teorema 4.31. *Si χ es un carácter no principal módulo k y $x \leq 1$ tenemos:*

$$\sum_{n\leq x} \frac{\chi(n)}{n} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} + \mathcal{O}\left(\frac{1}{x}\right), \tag{4.21}$$

$$\sum_{n\leq x} \frac{\chi(n)\log n}{n} = \sum_{n=1}^{\infty} \frac{\chi(n)\log n}{n} + \mathcal{O}\left(\frac{\log x}{x}\right), \tag{4.22}$$

$$\sum_{n\leq x} \frac{\chi(n)}{\sqrt{n}} = \sum_{n=1}^{\infty} \frac{\chi(n)}{\sqrt{n}} + \mathcal{O}\left(\frac{1}{\sqrt{x}}\right). \tag{4.23}$$

Usaremos ahora $L(1,\chi)$ para denotar la serie de (4.21)

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

Para la demostración del teorema de Dirichlet necesitamos probar que $L(1,\chi) \neq 0$. Procedemos a hacerlo con ayuda de los siguientes teoremas.

Teorema 4.32. *Sea χ un carácter real módulo k y sea*

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

Entonces $A(n) \geq 0$ para todo n, y $A(n) \geq 1$ si n es un cuadrado.

Demostración. Si tomamos $n = p^a$, con p primo podemos escribir

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

Como χ es real, los únicos valores posibles para $\chi(p)$ son 0, 1 y -1. Si $\chi(p) = 0$, entonces $A(p^a) = 1$. Si $\chi(p) = 1$, entonces $A(p^a) = a + 1$. Si $\chi(p) = -1$, entonces

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

En cualquiera de los tres casos, si a es par entonces $A(p^a) \geq 1$. Descomponemos n en factores primos distintos $n = p_1^{a_1} \cdots p_r^{a_r}$. Como A es multiplicativa, podemos escribir $A(n) = A(p_1^{a_1}) \cdots A(p_r^{a_r})$. Como cada $p_i^{a_i} \geq 0$, tenemos que $A(n) \geq 0$. Hemos demostrado así la primera parte del teorema. Ahora, si n es un cuadrado, entonces cada exponente a_i es par, luego cada factor $A(p_i^{a_i}) \geq 1$. Con lo que tenemos $A(n) \geq 1$. □

Teorema 4.33. *Para todo carácter no principal real χ módulo k, sea*

$$A(n) = \sum_{d|n} \chi(d) \quad y \quad B(x) = \sum_{n \leq x} \frac{A(n)}{\sqrt{n}}.$$

Entonces tenemos:

a) $B(x) \to \infty$ cuando $x \to \infty$.

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

Por lo tanto, $L(1,\chi) \neq 0$.

Demostración. En el teorema 4.32 hemos probado que en caso de que n sea un cuadrado, $A(n) \geq 1$, por lo tanto podemos escribir

$$B(x) \geq \sum_{\substack{n \leq x \\ n = m^2}} \frac{1}{\sqrt{n}} = \sum_{m \leq \sqrt{x}} \frac{1}{m}.$$

Como la serie armónica $\sum \frac{1}{m}$ diverge, $\sum_{m \leq \sqrt{x}} \frac{1}{m}$ tiende a ∞ cuando $x \to \infty$.

Con esto hemos probado la parte a) del teorema. Para probar la segunda parte escribimos

$$B(x) = \sum_{n \leq x} \frac{1}{\sqrt{n}} \sum_{d|n} \chi(d) = \sum_{\substack{q,d \\ qd \leq x}} \frac{\chi(d)}{\sqrt{qd}}.$$

Recordamos la identidad obtenida en el teorema 4.19:

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

donde $ab = x$,

$$F(x) = \sum_{n \leq x} f(n) \quad \text{y} \quad G(x) = \sum_{n \leq x} g(n).$$

Tomamos $a = b = \sqrt{x}$ y hacemos $f(n) = \chi(n)/\sqrt{n}$, $g(n) = 1/\sqrt{n}$ para obtener

$$B(x) = \sum_{n\leq\sqrt{x}} \frac{\chi(n)}{\sqrt{n}} G\Big(\frac{x}{n}\Big) + \sum_{n\leq\sqrt{x}} \frac{1}{\sqrt{n}} F\Big(\frac{x}{n}\Big) - F(\sqrt{x})G(\sqrt{x}). \tag{4.24}$$

Como $1/2 > 0$, por el apartado b) del teorema 4.12 podemos escribir

$$G(x) = \sum_{n\leq x} \frac{1}{\sqrt{n}} = 2\sqrt{x} + A + \mathcal{O}\left(\frac{1}{\sqrt{x}}\right), \tag{4.25}$$

donde A es una constante. Por otro lado, por la tercera igualdad del teorema 4.31,

$$F(x) = \sum_{n\leq x} \frac{\chi(n)}{\sqrt{n}} = B + \mathcal{O}\left(\frac{1}{\sqrt{x}}\right),$$

donde $B = \sum_{n=1}^{\infty} \chi(n)/\sqrt{n}$. Como $F(\sqrt{x})G(\sqrt{x}) = 2Bx^{1/4} + \mathcal{O}(1)$, podemos escribir la ecuación (4.24) de la siguiente forma:

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

Con esto, demostramos b). □

Una vez presentados los caracteres de Dirichlet, procedemos a la demostración de su teorema.

Capítulo 5

Demostración del teorema de Dirichlet

En este capítulo presentamos una lista de lemas con sus respectivas demostraciones que nos ayudarán a demostrar el teorema de Dirichlet. A lo largo del capítulo usaremos la siguiente notación: el entero positivo k representa un módulo fijo y el entero fijo h un número de forma que $\text{mcd}(h,k)=1$. Los $\phi(k)$ caracteres de Dirichlet módulo k se representarán por

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

donde χ_1 designará el carácter principal. Para $\chi \neq \chi_1$ escribiremos $L(1,\chi)$ y $L'(1,\chi)$ para representar las siguientes sumas de series:

$$L(1,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n},$$
$$L'(1,\chi) = -\sum_{n=1}^{\infty} \frac{\chi(n)\log n}{n}.$$

La convergencia de cada una de estas series se estableció en el teorema 4.31. Además, en el teorema 4.33 se vio que si el carácter χ es una función real, entonces $L(1,\chi) \neq 0$. El símbolo p designará un primo y $\sum_{p\leq x}$ la suma extendida a todos los primos $p \leq x$. Con esto aclarado, vamos a ver y demostrar los siguientes lemas, que nos ayudarán a mostrar fácilmente el teorema de Dirichlet.

Lema 5.1. *Para $x > 1$ tenemos*

$$\sum_{\substack{p\leq x \\ p\equiv h \pmod{k}}} \frac{\log p}{p} = \frac{1}{\phi(k)}\log x + \frac{1}{\phi(k)}\sum_{r=2}^{\phi(k)} \phi_r(h) \sum_{p\leq x} \frac{\chi_r \log p}{p} + \mathcal{O}(1). \quad (5.1)$$

Demostración. En el teorema 4.21 obtuvimos la fórmula asintótica

$$\sum_{p\leq x}\frac{\log p}{p}=\log x+\mathcal{O}(1). \tag{5.2}$$

Ahora nos quedamos con aquellos términos que sean congruentes con h módulo k. Lo realizamos con ayuda del teorema 4.27. Si $\mathrm{mcd}(n,k)=1$ tenemos

$$\sum_{r=1}^{\phi(k)}\chi_r(m)\bar{\chi_r}(n)=\begin{cases}\phi(k), & \text{si } m\equiv n \text{ (mód } k),\\ 0, & \text{si no.}\end{cases}$$

Tomamos $m=p$ y $n=h$ tal que $\mathrm{mcd}(h,k)=1$. Multiplicamos la ecuación anterior a ambos lados por $\log p/p$ y lo sumamos para todo $p\leq x$. Obtenemos la siguiente igualdad:

$$\sum_{p\leq x}\sum_{r=1}^{\phi(k)}\chi_r(p)\bar{\chi_r}(h)\frac{\log p}{p}=\phi(k)\sum_{\substack{p\leq x\\ p\equiv h \text{ (mód } k)}}\frac{\log p}{p}.$$

En el término izquierdo de la igualdad anterior aislamos aquellos sumandos que contienen únicamente el carácter principal χ_1, obteniendo

$$\bar{\chi_1}(h)\sum_{p\leq x}\frac{\chi_1\log p}{p}+\sum_{r=2}^{\phi(k)}\bar{\chi_r}(h)\sum_{p\leq x}\frac{\chi_r\log p}{p}=\phi(k)\sum_{\substack{p\leq x\\ p\equiv h \text{ (mód } k)}}\frac{\log p}{p}. \tag{5.3}$$

Tenemos que $\bar{\chi_1}(h)=1$. Por otro lado, en caso de que $\mathrm{mcd}(p,k)=1$, $\chi_1(p)=1$. Por lo tanto, el primer término de la igualdad anterior nos queda

$$\bar{\chi_1}(h)\sum_{p\leq x}\frac{\chi_1(p)\log p}{p}=\sum_{\substack{p\leq x\\ \mathrm{mcd}(p,k)=1}}\frac{\log p}{p}=\sum_{p\leq x}\frac{\log p}{p}-\sum_{\substack{p\leq x\\ p|k}}\frac{\log p}{p}.$$

Y como el número de primos que divide a k es finito, tenemos que

$$\sum_{\substack{p\leq x\\ p|k}}\frac{\log p}{p}=\mathcal{O}(1).$$

Nos queda

$$\bar{\chi_1}(h)\sum_{p\leq x}\frac{\chi_1\log p}{p}=\sum_{p\leq x}\frac{\log p}{p}+\mathcal{O}(1). \tag{5.4}$$

Sustituimos (5.4) en (5.3) y reordenamos:

$$\phi(k)\sum_{\substack{p\leq x\\ p\equiv h \text{ (mód } k)}}\frac{\log p}{p}=\sum_{p\leq x}\frac{\log p}{p}+\sum_{r=2}^{\phi(k)}\bar{\chi_r}(h)\sum_{p\leq x}\frac{\chi_r\log p}{p}+\mathcal{O}(1).$$

Usamos la formula asintótica que rescatábamos del teorema 4.21 en (5.2), con lo cual

$$\phi(k) \sum_{\substack{p\leq x \\ p\equiv h \pmod k}} \frac{\log p}{p} = \log x + \sum_{r=2}^{\phi(k)} \overline{\chi}_r(h) \sum_{p\leq x} \frac{\chi_r \log p}{p} + \mathcal{O}(1).$$

Y dividiendo por $\phi(k)$ demostramos el lema. □

Lema 5.2. *Para $x > 1$ y $\chi \neq \chi_1$ tenemos*

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

Demostración. Tomemos la suma

$$\sum_{n\leq x} \frac{\chi(n)\Lambda(n)}{n}$$

donde $\Lambda(n)$ es la función de von Mangoldt. Recordamos su definición:

$$\Lambda(n) = \begin{cases} \log p, & \text{si } n = p^m \text{ para un cierto primo } p \text{ y un cierto } m \geq 1, \\ 0, & \text{en otro caso.} \end{cases}$$

Sustituyendo, obtenemos

$$\sum_{n\leq x} \frac{\chi(n)\Lambda(n)}{n} = \sum_{p\leq x} \sum_{\substack{a=1 \\ p^a\leq x}}^{\infty} \frac{\chi(p^a)\log p}{p^a}.$$

Separamos $a = 1$ del resto de términos, lo que nos da

$$\sum_{n\leq x} \frac{\chi(n)\Lambda(n)}{n} = \sum_{p\leq x} \frac{\chi(p)\Lambda(p)}{p} + \sum_{p\leq x} \sum_{\substack{a=2 \\ p^a\leq x}}^{\infty} \frac{\chi(p^a)\log p}{p^a}. \tag{5.5}$$

Por otro lado, $\displaystyle\sum_{p\leq x} \sum_{\substack{a=2 \\ p^a\leq x}}^{\infty} \frac{\chi(p^a)\log p}{p^a}$ está acotada superiormente por

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

Por lo que (5.5) nos queda

$$\sum_{p\leq x} \frac{\chi(p)\log p}{p} = \sum_{n\leq x} \frac{\chi(n)\Lambda(n)}{n} + \mathcal{O}(1). \tag{5.6}$$

En el teorema 4.5 vimos que $\Lambda(n) = \sum_{d|n} \mu(n)\log(n/d)$, por lo que podemos reescribir

$$\sum_{n\leq x} \frac{\chi(n)\Lambda(n)}{n} = \sum_{n\leq x} \frac{\chi(n)}{n} \sum_{d|n} \mu(d)\log\frac{n}{d}.$$

Si en la parte derecha de la igualdad tomamos $n = cd$ y usamos la propiedad multiplicativa de χ tenemos que

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

Como $x/d \geq 1$ podemos utilizar la segunda fórmula del teorema 4.31 en la suma respecto de c, con lo que obtenemos la siguiente igualdad:

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

Con esto, podemos escribir

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

Centrémonos ahora en el $\mathcal{O}$-término, concretamente en su suma:

$$\sum_{d\leq x} \frac{\log x/d}{x} = \frac{1}{x}\sum_{d\leq x}(\log x - \log d) = \frac{1}{x}\Big(\lfloor x\rfloor \log x - \sum_{d\leq x} \log d\Big). \tag{5.7}$$

Por el teorema 4.17, se cumple

$$\sum_{d\leq x} \log d = \log(\lfloor x\rfloor !) = x\log x + \mathcal{O}(x),$$

y sustituyendo en (5.7) obtenemos que

$$\sum_{n\leq x} \frac{\chi(n)\Lambda(n)}{n} = -L'(1,\chi)\sum_{d\leq x} \frac{\mu(d)\chi(d)}{d} + \mathcal{O}(1). \tag{5.8}$$

En (5.6) vimos que

$$\sum_{p\leq x} \frac{\chi(p)\log p}{p} = \sum_{n\leq x} \frac{\chi(n)\Lambda(n)}{n} + \mathcal{O}(1),$$

que junto a (5.8), finaliza la prueba del lema. □

Lema 5.3. *Para $x > 1$ y $\chi \neq \chi_1$ tenemos*

$$L(1,\chi)\sum_{n\leq x}\frac{\mu(n)\chi(n)}{n} = \mathcal{O}(1). \tag{5.9}$$

Demostración. Si en la fórmula de inversión de Möbius generalizada (4.5) usamos $\alpha(n) = \chi(n)$ y $F(x) = x$, obtenemos

$$x = \sum_{n\leq x}\mu(n)\chi(n)G\left(\frac{x}{n}\right) \quad \text{donde} \quad G(x) = \sum_{n\leq x}\chi(n)\frac{x}{n} = x\sum_{n\leq x}\frac{\chi(n)}{n}. \tag{5.10}$$

Por la primera ecuación del teorema 4.31 tenemos $G(x) = xL(1,\chi) + \mathcal{O}(1)$. Sustituimos en (5.10) y obtenemos

$$\begin{aligned} x &= \sum_{n\leq x}\mu(n)\chi(n)\left\{\frac{x}{n}L(1,\chi) + \mathcal{O}(1)\right\} \\ &= xL(1,\chi)\sum_{n\leq x}\frac{\mu(n)\chi(n)}{n} + \mathcal{O}(x). \end{aligned} \tag{5.11}$$

De nuevo, dividimos por x y demostramos el lema. □

Lema 5.4. *Si $\chi \neq \chi_1$ y $L(1,\chi) = 0$ tenemos*

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

Demostración. Tomamos $F(x) = x\log x$ en la fórmula de inversión de Möbius generalizada (4.5), obteniendo

$$x\log x = \sum_{n\leq x}\mu(n)\chi(n)G\left(\frac{x}{n}\right) \tag{5.12}$$

donde

$$G(x) = \sum_{n\leq x}\chi(n)\frac{x}{n}\log\frac{x}{n} = x\log x\sum_{n\leq x}\frac{\chi(n)}{n} - x\sum_{n\leq x}\frac{\chi(n)\log n}{n}.$$

Ahora utilizamos la primera y la segunda fórmula del teorema 4.31 y obtenemos

$$\begin{aligned} G(x) &= x\log x\left\{L(1,\chi) + O\left(\frac{1}{x}\right)\right\} + x\left\{L'(1,\chi) + \mathcal{O}\left(\frac{\log x}{x}\right)\right\} \\ &= xL'(1,\chi) + \mathcal{O}(\log x), \end{aligned}$$

ya que $L(1,\chi)=0$. Luego

$$(5.12) = \sum_{n\le x}\mu(n)\chi(n)\left\{\frac{x}{n}L'(1,\chi)+O\left(\frac{\log x}{x}\right)\right\}$$
$$= xL'(1,\chi)\sum_{n\le x}\frac{\mu(n)\chi(n)}{n}+\mathcal{O}\left(\sum_{n\le x}(\log x-\log n)\right).$$

Veamos que el $\mathcal{O}$-término de la derecha es $\mathcal{O}(1)$:

$$\sum_{n\le x}(\log x-\log n)=\lfloor x\rfloor\log x-\sum_{n\le x}\log n=\mathcal{O}(x),$$

ya que, por (4.11),

$$\sum_{n\le x}\log n=\log\lfloor x\rfloor=x\log x+\mathcal{O}(x).$$

Y dividiendo por x, el lema queda probado. □

Sea $N(k)$ el número de caracteres no principales χ (mód k) que cumplen $L(1,\chi)=0$. Como los caracteres siempre aparecen en pares conjugados, $N(k)$ es par. Nuestro propósito es demostrar que $N(k)=0$, y esto se deduce del siguiente lema.

Lema 5.5. *Para $x>1$ tenemos*

$$\sum_{\substack{p\le x\\ p\equiv h(k)}}\frac{\log p}{p}=\frac{1-N(k)}{\phi(k)}\log x+\mathcal{O}(1). \tag{5.13}$$

Antes de dar la demostración, observemos que si $N(k)\neq 0$, entonces $N(k)\ge 2$ ya que $N(k)$ es par, luego

$$\frac{1-N(k)}{\phi(k)}\log x$$

es negativo, por lo que el término de la derecha de (5.13) tiende a $-\infty$ cuando $x\to\infty$. Es absurdo, ya que todos los sumandos de la izquierda son positivos. Por lo que si probamos el lema, demostraremos que $N(k)=0$.

Demostración. Tomamos $h=1$ en el lema 5.1, obteniendo

$$\sum_{\substack{p\le x\\ p\equiv 1 \text{ (mód } k)}}\frac{\log p}{p}=\frac{1}{\phi(k)}\log x+\frac{1}{\phi(k)}\sum_{r=2}^{\phi(k)}\sum_{p\le x}\frac{\chi_r(p)\log p}{p}+\mathcal{O}(1). \tag{5.14}$$

En $\sum_{p\leq x} p^{-1}\chi_r(p)\log p$ hacemos uso del lema 5.2 obteniendo:

$$\sum_{p\leq x} p^{-1}\chi_r(p)\log p = -L'(1,\chi_r)\sum_{n\leq x}\frac{\mu(n)\chi_r(n)}{n} + \mathcal{O}(1).$$

En caso de que $L(1,\chi_r)\neq 0$, el lema 5.3 demuestra que

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

Si sustituimos esto en la ecuación (5.14) nos queda que

$$\sum_{\substack{p\leq x\\ p\equiv 1 \pmod k}} \frac{\log p}{p} = \frac{1}{\phi(k)}\log x + \mathcal{O}(1).$$

Por el contrario, si $L(1,\chi_r)\neq 0$ el lema 5.4 demuestra que

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

Si sustituimos esta expresión en la ecuación (5.14) obtenemos

$$\begin{aligned}\sum_{\substack{p\leq x\\ p\equiv 1 \pmod k}} \frac{\log p}{p} &= \frac{1}{\phi(k)}\log x - \frac{1}{\phi(k)}\sum_{r=2}^{\phi(k)}\log x + \mathcal{O}(1)\\ &= \frac{1}{\phi(k)}\log x - \frac{1}{\phi(k)}N(k)\log x + \mathcal{O}(1)\\ &= \frac{1-N(k)}{\phi(k)}\log x + \mathcal{O}(1).\end{aligned}$$

Con lo que queda probado el lema 5.5. □

Como consecuencia de todo lo anterior, tenemos el siguiente resultado:

Teorema 5.6. *Si $k>0$ y $\mathrm{mcd}(h,k)=1$, tenemos, para $x>1$,*

$$\sum_{\substack{p\leq x\\ p\equiv h \pmod k}} \frac{\log p}{p} = \frac{1}{\phi(k)}\log x + \mathcal{O}(1). \tag{5.15}$$

Demostración. Es claro que el lema 5.1 implica el teorema 5.6 si probamos que

$$\sum_{p\leq x}\frac{\chi(p)\log p}{p} = \mathcal{O}(1) \tag{5.16}$$

para cada carácter de Dirichlet no principal. En el lema 5.2 probamos que

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

Por ello, si demostramos que

$$\sum_{n\leq x}\frac{\mu(n)\chi(n)}{n}=\mathcal{O}(1), \tag{5.17}$$

entonces probaríamos el lema 5.2 y, con él, el teorema.

En el lema 5.3 vimos lo siguiente: para $x>1$ y $\chi\neq\chi_1$

$$L(1,\chi)\sum_{n\leq x}\frac{\mu(n)\chi(n)}{n}=\mathcal{O}(1). \tag{5.18}$$

Además, en el capítulo anterior demostramos, como consecuencia del teorema 4.33, que $L(1,\chi)\neq 0$ para los caracteres no principales que toman valores reales; y el lema 5.3 prueba que también es cierto para caracteres que toman valores complejos. En consecuencia, (5.18) se reduce a(5.17) y hemos demostrado el teorema. □

A menudo, al teorema anterior se le denomina con el nombre de "versión de Shapiro del teorema de Dirichlet". Y la razón de este nombre es sencilla, ya que, si en (5.15) hacemos $x\to\infty$, lo que tenemos es

$$\sum_{p\equiv h\ (\text{mód }k)}\frac{\log p}{p}=\infty,$$

ya que $\log x\to\infty$ cuando $x\to\infty$. Por supuesto, esto implica que existen infinitos primos $p\equiv h$ (mód k) pues, de lo contrario, la serie tendría un número finito de sumandos y no podría diverger.

Así pues, hemos probado el teorema con el que comenzamos este trabajo, el teorema de Dirichlet.

Teorema de Dirichlet. *Si p y q son dos enteros con $q>0$ y $\operatorname{mcd}(p,q)=1$. Entonces, en la progresión aritmética $nq+p$, con $n\in\mathbb{N}$, existen infinitos primos.*

Capítulo 6

Generalizaciones

Una progresión aritmética es un caso particular de una función polinómica de grado uno,

$$f(x) = px + q.$$

Sabemos que tiene infinitos primos si $\mathrm{mcd}(p, q) = 1$. ¿Pero qué pasa con polinomios de mayor grado? ¿Tienen infinitos primos?

En el año 1772, Euler se dio cuenta de que

$$f(x) = x^2 + x + 41$$

es primo para los 40 números consecutivos $x = 0, 1, \ldots, 39$. Pero si tomamos $x = 40$, $f(40) = 1681 = 41 \times 41$ ya no es primo.

No se sabe si existe algún polinomio de segundo grado

$$f(x) = ax^2 + bx + c \quad (a, b, c \in \mathbb{N}, a \neq 0)$$

que tome infinitos valores primos. Euler se interesó por x^2+1. El avance más reciente es de Iwaniec que en el año 1978 demostró que $x^2 + 1 = P_2$ para infinitos x.

Observación. Aquí y en lo que sigue, P_k representa un producto de a lo sumo k primos. Lo que queríamos decir con P_2 es que $x^2 + 1$ es igual al producto de a lo sumo 2 primos.

Si tomamos $f(x) = x^2 + x + 2 = x(x + 1) + 2$ para valores enteros de x los valores de la función son siempre pares y por lo tanto 2 es el único primo en esta progresión.

En 1857, Viktor Bunyakovsky proporcionó un criterio posible pero aún no probado para que un polinomio $f(x)$ con coeficientes enteros dé infinitos valores primos en la sucesión $f(1), f(2), f(3), \ldots$.

Conjetura de Bunyakovsky. *Sea* $f(x) \in \mathbb{Z}[x]$ *con* $\mathrm{gr}(f) \geq 1$ *un polinomio irreducible, esto es,* $f(x) \neq a(x)b(x)$ *con* $\mathrm{gr}(a), \mathrm{gr}(b) < \mathrm{gr}(f)$*. Y supongamos que además los valores* $\{f(n) : n \in \mathbb{N}\}$ *no tienen factor común (en particular, los coeficientes de* $f(x)$ *deben ser coprimos). Entonces* $f(n)$ *es primo para infinitos* $n \in \mathbb{N}$*.*

Parece lejos de demostrarse, pero hay resultados del tipo

$$f(n) = P_k \quad \text{para infinitos } n.$$

Otra forma de generalizar el teorema de Dirichlet es estudiar los primos no como un subconjunto de los números naturales, sino analizar el comportamiento de los ideales primos en los cuerpos numéricos. De este modo, se puede generalizar el concepto de prueba euclidiana que vimos en el segundo apartado del capítulo 2 de la siguiente manera:

Sea K/k una extensión abeliana de Galois cuyo grupo de Galois lo denominamos mediante $G = \mathrm{Gal}(K/k)$, donde K es un cuerpo y k un cuerpo algebraico de números con $k \subset K$. Un **ideal** $P \subset k$ se llama divisor primo de un polinomio $f \in \mathrm{O}_k[x]$ si $P \mid f(a)$ para cierto a en el anillo de enteros O_k.

La existencia de una **prueba euclidiana** para un $\sigma \in G$ implica la existencia de un polinomio f tal que, con un número finito de excepciones, todos los divisores primos de f tienen el elemento de Frobenius igual a 1 o a σ. (No detallaremos aquí qué se denomina elemento de Frobenius; se puede encontrar más información al respecto en [13]).

Así mismo, merece la pena destacar que Murty y Thain en [10] muestran la existencia una demostración euclidiana si el orden de σ es igual a 2. La prueba se hace de manera muy similar a la realizada por Murty en [9] para mostrar que existe una demostración euclidiana para una progresión l (mód k) si, y sólo si, $l^2 \equiv 1$ (mód k), pero debido a su extensión no la discutiremos aquí. K. Conrad probó la implicación contraria, que no existe demostración euclídea en caso de que el orden de σ no sea 2. Tampoco vamos a contarla aquí, pero podemos encontrarla en [2].

Conclusiones

El objetivo de esta memoria era demostrar la existencia de infinitos números primos en cualquier progresión aritmética y lo hemos hecho poco a poco. Comenzamos con una pequeña introducción, en la que vimos unas primeras definiciones así como una introducción histórica acerca de los primos.

Continuamos con un nuevo capítulo, en el que vimos la demostración del teorema de Euclides, el cual afirma que existen infinitos números primos. Vimos que el procedimiento seguido a lo largo de la demostración se puede usar para demostrar la existencia de infinitos primos en progresiones aritméticas de cierta forma. A esa demostración le dimos el nombre de demostración euclidiana. Nos preguntamos si ese tipo de demostración probaría el teorema que a nosotros nos interesa, el teorema de Dirichlet. Automáticamente nos dimos cuenta de que no (en realidad el que se dio cuenta fue Murty en el año 1973, que sólo podemos probar la infinitud de primos en una progresión aritmética $\mathbb{N}(p, q)$ mediante una demostración euclidiana si p^2 pertenece a $\mathbb{N}(1, q)$.

Por lo que seguimos viendo otras alternativas para poder demostrar el teorema. Dirichlet se basó en las ideas que usó Euler para demostrar el teorema de Euclides. Esas ideas las vimos reflejadas en el capítulo 3. La demostración del teorema, que por fin realizamos en el capítulo 5, fue una versión más moderna dada por Shapiro.

Terminamos la memoria viendo cómo se podía generalizar el teorema de Dirichlet, dejando las conjeturas abiertas por si alguien las quiere demostrar.

Bibliografía

[1] Apostol, T. M., *Introducción a la teoría analítica de números*, Editorial Reverté, 1980.

[2] Conrad, K., *Eucliden proofs of Dirichlet's theorem.* Online a través de `https://kconrad.math.uconn.edu/blurbs/gradnumthy/dirichleteuclid.pdf`.

[3] Euclides, *Los Elementos*, Libros V–IX, traducción y notas de M. L. Puertas Castaños, revisada por P. Ortiz García, Editorial Gredos, Madrid, 1994.

[4] Dedekind, R., *Ueber den Zusammenhang zwischen der Theorie der ideale und der Theorie der höheren Congruenzen*, Göttinger Abhandlungen, (1878), 15–16.

[5] Hardy G. H. & J. E. Littlewood, J. E., *The zeros of Riemann's zeta-function on the critical line*, Math. Z. **10** (1921), 283–317.

[6] Hardy, G. H. & Wright, E. M., *An introduction to the theory of numbers*, Oxford University Press, 1960.

[7] Kummer, E. E., *Neuer elementarer Beweis des Satzes, dass die Anzahl aller Primzahlen eine unendliche ist*, Preubische Akademie der Wissenschaften, Berlin (1878/79), 777–778.

[8] Euler, L., *Variae observations circa series infinitas*, Commentarii academiae scintarum Petropolitanae, **9** (1744), 160–188.

[9] Murty M. R., *Primes in certain arithmetic progressions*, J. Madras Univ., Section B, **51** (1988), 161–169.

[10] Murty M. R. & Thain N., *Primes in certain arithmetic progressions*, Funct. Approx. Comment. Math. **35** (2006), 249–259. Online a través de `https://projecteuclid.org/euclid.facm/1229442627`

[11] Nagell, T., *Sur les diviseurs premiers des polynômes*, Acta Arith. **15** (1968/69), 235–244.

[12] Navas, L., *La infinitud de los primos*, Universidad de Salamanca, 2019, www.youtube.com/watch?v=7WyK0X4mLDY.

[13] Park, S. W., *Existence of the Frobenius element and its applications*, University of Chicago, https://math.uchicago.edu/~may/REU2015/REUPapers/Park.pdf.

[14] Schur, I., *Gesammelte Abhandlungen* [Collected Works], Springer Verlag, Berlin, 1973.

[15] Stieltjes, T. J., *Étude bibliographique. Sur la théorie des nombres*, Annales de la Faculté des sciences de Toulouse: Mathématiques, **4** (1890), 1–103.

[16] Varona, J. L., *Recorridos por la teoría de números*, segunda edición, Ediciones Electolibris y Real Sociedad Matemática Española, Murcia, 2019.