VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

Facultad de Ciencias

Grado en Matemáticas

INFINITUD DE NÚMEROS PRIMOS EN PROGRESIONES ARITMÉTICAS

Trabajo Fin de Grado

Autor: Cristian García Garcinuño

Tutor: Luis Manuel Navas Vicente

Enero 2023

VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

INFINITUD DE NÚMEROS PRIMOS EN PROGRESIONES ARITMÉTICAS

Autor: Cristian García Garcinuño

Tutor: Luis Manuel Navas Vicente

Firmado por GARCIA GARCINUÑO CRISTIAN - ***4083** el día 09/01/2023 con un certificado emitido por AC FNMT Usuarios

Firmado por NAVAS VICENTE LUIS MANUEL - ***6086** el día 09/01/2023 con un certificado emitido por AC FNMT Usuarios

Enero 2023

Certificado del/los tutor/es TFG

D./Dña. **Luis Manuel Navas Vicente,** profesor/a del Departamento de **Matemáticas** de la Universidad de Salamanca,

HACE/N CONSTAR:

Que el trabajo titulado "**Infinitud de números primos en progresiones aritméticas**", que se presenta, ha sido realizado por **Cristian García Garcinuño**, con DNI **70840830W** y constituye la memoria del trabajo realizado para la superación de la asignatura Trabajo de Fin de Grado en **Matematicas** en esta Universidad.

Salamanca, 9 de enero de 2023

Fdo.: Luis Manuel Navas Vicente

Firmado por NAVAS VICENTE LUIS MANUEL - ***6086** el día 09/01/2023 con un certificado emitido por AC FNMT Usuarios

Índice general

Capítulo 1

Introducción

Cuando hablamos de la infinitud de números primos en progresiones aritméticas, el resultado final se puede resumir en el teorema que Dirichlet demostró, el cual data de 1837 y que es conocido con el nombre del propio autor. Dicho teorema, tomando como referencia el teorema 7.9 de Apostol [2], dice:

Teorema (Teorema de Dirichlet)**.** *Dados enteros a, m con $m \geq 2$, tales que el máximo común divisor de a y m sea 1, hay infinitos números primos en la progresión aritmética $a, a+m, a+2m, \ldots,$ o sea $a+nm$ con $n = 0, 1, 2 \ldots$.*

El objetivo de este trabajo será llegar a la demostración del mismo.

Se puede ver muy fácil con un ejemplo práctico, supongamos el 4 y el 3, que serían nuestras k y h respectivamente, y por lo tanto la progresión aritmética que se forma sería: $3, 7, 11, 15, 19, 23, 27 \ldots$, donde no todos son primos, pero por ejemplo si cogemos sus 30 primeros términos tendremos como primos a 15 de ellos: 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, 107. Pues el teorema de Dirichlet nos demuestra que si cogemos toda la progresión aritmética la cantidad de primos en ella es infinita.

Aunque los números son algo que se llevan usando desde hace miles de años, no fue hasta los griegos que empezaron a estudiarse los números primos y fue Pitágoras en el 600 A.C. el cual dio las primeras clasificaciones de los números de varias maneras y entre ellas habló de los números primos, definiéndose estos como aquellos números los cuales solo son divisibles entre el 1 y el propio número, y de los números compuestos, que eran todos aquellos que no eran primos.

Y 300 años más tarde, Euclides en su obra Elementos, la cual era una colección de 13 libros, de los cuales 3 hablaban sobre teoría de números, habló sobre la infinitud de los números primos, siendo así el primero en hablar de dicho tema, y pese a ello dar una demostración que hoy día se utiliza en los colegios por su sencillez, la cual dice, basándonos en el teorema 1.7 de Apostol [2]:

Teorema 1.0.1 (Euclides)**.** *Hay infinitos números primos.*

Pero antes de ver la demostración de este teorema necesitaríamos otro teorema del propio Euclides muy trivial el cual enuncia, tomando el teorema 1.6 de Apostol [2];

Teorema 1.0.2 (Euclides)**.** *Todo número entero $n > 1$ es un número primo o es producto de números primos.*

Demostración. Demostraremos esto por inducción sobre la n. Para $n = 2$ está claro que se cumple, pues el 2 es primo. Vamos a suponerlo entonces cierto para todo entero menor que n y veamos que se cumple para n.

Para ellos supongamos que n no es primo, es decir tiene algún divisor d distinto que 1 y distinto al propio n. Entonces podemos tomar $n = c \cdot d$ donde c es distinto que n. Es obvio entonces que c y d son mayores que 1 y menores que n, y por hipótesis serán o primos o producto de primos, y por lo tanto n también lo será. □

Con esto demostramos este segundo teorema y podemos hacer la demostración del primer teorema, en el cual se usa la anterior.

Demostración del Teorema 1.0.1. Supongamos por reducción al absurdo lo contrario de lo que queremos demostrar, es decir, supongamos que el conjunto de los números primos es finito, es decir tenemos primos 2, 3, 5, ... P, con P el último primo. Y supongamos ahora N un número el cual es el resultado de multiplicar todos estos primos, es decir $N = 2 \cdot 3 \cdot 5 \cdots P$.

Tomemos ahora M otro número tal que $M = N + 1$. Y por lo tanto $M > P$.

Es evidente que como N es divisible por dos, M que es $N + 1$ no es divisible entre 2. Lo mismo pasa para el 3, como N es divisible entre 3, M no puede ser divisible entre él.

Reiterando el proceso nos damos cuenta que N es divisible por todos los primos, pero M no es divisible por ninguno, por lo tanto, M no se puede poner como producto de números primos y por el Teorema 2, esto implica que entonces M es primo.

Por lo tanto, M es un primo mayor que P que hemos supuesto que era el último primo, con lo que llegamos a una contradicción y acabamos demostrando efectivamente la infinitud de los números primos. □

Esta demostración pese a su sencillez, queda muy escasa y lejos de nuestro objetivo, aunque si que es verdad que a partir de ella podemos ver siguiendo los teoremas 7.1 y 7.2 de Apostol [2], algunos ejemplos de progresiones aritméticas en los que si se cumple.

En primer lugar, podemos observar que hay infinitos números primos de la forma $4n - 1$. Veamos una demostración de esto, la cual veremos por reducción al absurdo, suponiendo lo contrario y llegando a una contradicción.

Teorema 1.0.3. *Hay infinitos primos de la forma* $4n - 1$.

Demostración. Si en esta progresión aritmética hubiera un número finito de primos, suponiendo P el primo más grande de estos tomemos el número natural $N = 4 \cdot 3 \cdot 5 \cdot 7 \ldots \cdot P - 1$. Entonces N no podrá ser primo pues es de la forma $4 \cdot n - 1$ y mayor que P.

Evidentemente la parte del producto entre 3 y P contiene a todos los primos impares menores que P. Entonces ningún primo menor o igual a P divide a N.

No todos los factores primos que dividen a N pueden ser de la forma $4n + 1$ pues si tomamos dos de estos y los multiplicamos nos da otro número de la misma forma y por esto algún factor primo de N debe ser de la forma $4n - 1$. Este factor debe ser mayor que P. Llegamos a una contradicción pues encontramos un primo mayor que P y de la forma $4n - 1$.

Con lo que podemos concluir que el número de primos de la forma $4n - 1$ es infinito. □

El otro ejemplo dice que hay infinitos números primos de la forma $4n+1$.

Al final lo que nos dice este enunciado es que dentro de la progresión aritmética $4n+1$ la cual sería, $5, 9, 13, 17, 21\ldots$ hay infinitos números primos. Veamos una demostración de esto.

Teorema 1.0.4. *Hay infinitos primos de la forma* $4n+1$.

Demostración. Supongamos un numero entero N mayor que 1 y veamos que hay un primo P mayor que N tal que $P \equiv 1(\text{mód}4)$. Sea:

$$m = (N!)^2 + 1. \tag{1.0.1}$$

Podemos observar que m es impar, con m mayor que 1. sea además P el factor primo más pequeño de modo que ninguno de los números $2, 3, ..., N$ divide a m, y por lo tanto P es mayor que N.

También, tenemos que:

$$(N!)^2 \equiv -1(\text{mód}P) \tag{1.0.2}$$

Elevando ambos lados de la igualdad al factor $\frac{P-1}{2}$ obtenemos:

$$(N!)^{P-1} \equiv -1^{\frac{p-1}{2}}(\text{mód}P) \tag{1.0.3}$$

Ahora usaremos el teorema de Euler-Fermat, el cual enuncia que si cogemos dos números a y m cuyo máximo común divisor sea 1, es decir que sean primos entre sí, entonces:

$$a^{\phi(m)} \equiv 1 \text{ mód } m \tag{1.0.4}$$

donde el exponente es la función que suma la cantidad de números entre 1 y m, los cuales son primos con m. Por esto tenemos que la parte izquierda de la igualdad anterior es igual a $1(\text{mód}P)$, y por lo tanto tenemos,

$$(-1)^{\frac{P-1}{2}}(\text{mód}P) \equiv 1(\text{mód}P) \tag{1.0.5}$$

Entonces la diferencia de ambos lados de la igualdad puede ser, o bien 0, o bien -2, y como no puede ser -2, porque es divisible por P, debe ser 0. Entonces;

$$(-1)^{\frac{P-1}{2}} = 1 \tag{1.0.6}$$

Pero esto significa que

$$\frac{P-1}{2} \tag{1.0.7}$$

es par, y $P \equiv 1(\text{mód}4)$. En otras palabras, acabamos de demostrar que para entero N mayor que 1 hay un primo P que es mayor N tal que $P \equiv 1(\text{mód}4)$ y por lo tanto hay infinitos números primos de la forma $4n+1$. □

Argumentos muy similares de los que hemos usado para demostrar la infinidad de los números primos en estas dos progresiones aritméticas, podemos adaptarlos para otras como por ejemplo $5n-1$, $8n-1$, $8n-3$ o $8n+3$. Estos casos tienen demostraciones llamadas *euclidianas*, donde la idea principal es:

Demostraciones euclidianas. Tomamos una lista de primos, llamémosla S, contenida en el conjunto de los primos en la progresión $a + nm$, llamémosla $\mathbb{P}(a, m)$, y cogemos:

$$x = \prod_{p \in S} p \tag{1.0.8}$$

Con ello construimos un entero N mayor que 1, cuyo máximo común divisor con la x será 1 y tal que N al menos tenga un divisor primo p tal que $p \in \mathbb{P}(a, m)$.

Por ejemplo, para la progresión $4n - 1$, se construye $N = 4x - 1$, que es una expresión lineal.

Sin embargo, el N no siempre es lineal, puede ser por ejemplo cuadrático. De esta idea citamos un Teorema de Ram Murty, de 1998, que dice que con estos métodos euclidianos no se puede demostrar el caso general del Teorema de Dirichlet.

Después de Euclides, y hasta Diofanto, otro matemático griego, hubo pocos avances en relación a la teoría de números, pero los principales en torno a este tema los llevarían a cabo matemáticos de los siglos XVII y XVIII, como Fermat, reconocido como el padre de la teoría de números moderna, Euler, Lagrange, Legendre, Gauss y Dirichlet, aunque centrándonos en nuestro tema, principalmente cabe destacar a dos de ellos, en concreto a Euler y a Dirichlet.

Así cabe destacar, como ya hemos dicho, el teorema de Dirichlet, aunque fue enunciado por Legendre, nunca fue capaz de demostrarlo y fue Dirichlet el que dio la primera demostración formal de este teorema, pero no podemos centrarnos solo en ella pues a Dirichlet se le ocurrió esta demostración debido a ciertos trabajos anteriores de Euler y en concreto el punto de inicio de Dirichlet, como el mismo dijo fue una demostración de Euler sobre la existencia de infinitos números primos.

En resumen, aunque el objetivo principal del trabajo es la demostración del teorema de Dirichlet, y por lo tanto, la demostración de que hay infinitos números primos en progresiones aritméticas, no podemos llegar a ello, sin ver algo sobre la aritmética de los enteros; lo cual será lo primero que veremos, así como las ideas de Euler, no solo de la infinitud, si no sobre la función zeta y la fórmula del producto para la misma. Una vez visto esto ya podremos adentrarnos en la demostración del teorema tomando ideas de lo que son los caracteres de Dirichlet, algo de productos y series, y usando ciertos teoremas más extensos como el teorema de Landau, para al final llegar a nuestro objetivo final, la demostración de la infinitud de primos en estas progresiones aritméticas.

Para dar estructura a todo esto veremos en concreto 4 capítulos:

1. El primero que tratará sobre la aritmética de los enteros, viendo en él ciertos detalles sobre divisibilidad, números primos y multiplicidades, congruencias y el grupo de unidades, pero sin entrar en ninguno de los temas con mucho detalle.

2. El siguiente en el que veremos todas las ideas de Euler, tanto de infinitud como de la función zeta y su producto.

3. El tercero, donde encontraremos la demostración del teorema, pasando antes por definiciones, lemas y teoremas sobre la fórmula del producto, caracteres, series, el carácter principal y los no principales.

4. Y en este último, el de los apéndices donde encontraremos ciertas demostraciones a teoremas, las cuales son muy extensas y es preferible separar del cuerpo del TFG para así no desviar la atención del objetivo principal.

Capítulo 2

Aritmética de los enteros

Después de ver esta introducción sobre el tema en general, y los primeros intentos históricos de demostraciones, estaría bien ver ciertos puntos sobre aritmética de los enteros, que vamos a usar, así como la notación que utilizaremos en las demostraciones a continuación.

En resumen en este tema veremos pequeñas pinceladas sobre divisibilidad, números primos y multiplicidades, congruencias módulo m y el grupo de unidades.

2.1. Divisibilidad

En primer lugar, vamos a ver la divisibilidad, principalmente la definición, la notación que vamos a usar en dicho trabajo y algunas de sus propiedades que pueden ser útiles más adelante.

Definición 2.1.1. *Dados dos números enteros, los llamaremos a y b, con $a \neq 0$. Diremos que a divide á b si $b = ma$ con m un número entero.*

En nuestro caso la divisibilidad vamos a denotarla como:

$$a|b \tag{2.1.1}$$

En relación a las propiedades, veremos tres muy sencillas:

1. El 1 será el único entero que divide a todos los enteros.
2. El 0 es el único entero divisible por todos los enteros distintos que el propio 0.
3. La divisibilidad es un orden parcial dentro del conjunto de los enteros, es decir; verifica las propiedades reflexiva, transitiva y antisimétrica:
   - *a*) La reflexiva es obvia, pues si tomamos un número entero cualquiera distinto del 0, por ejemplo, a; tenemos que ese a se divide a si mismo.
   - *b*) Para ver la antisimétrica debemos tomar 2 números, tomaremos a y b entonces tendremos que la única manera de que a divida a b y de que b divida a a es que $a = b$
   - *c*) Por ultimo, para ver la transitividad tomaremos 3 enteros, a, b y c, y es obvio que, si b divide a c y a divide a b, como consecuencia tenemos que a divide a c.

2.2. Congruencias módulo m

Como ya vimos en la introducción el primero en dar una definición de número primo fue Pitágoras, y dicha definición puede ser utilizada a día de hoy, pues es similar.

Definición 2.2.1 (Número primo)**.** *Un número primo es todo entero, el cual, solo es divisible por el mismo y por el 1. Y a lo largo de este trabajo lo denotaremos como p. Al conjunto de todos estos números primos lo denotamos* $\mathbb{P}$*.*

Es importante saber que el 1 no es un número primo, pues todo número primo tiene dos factores, el mismo y el 1, pero el 1 tiene un único factor, que es el mismo.

También podemos dar otra definición un poco más formal, de lo que es un número primo. Un número primo es un elemento minimal respecto a dividir en el conjunto de los naturales, excluyendo el 1, es decir la descomposición de todo número compuesto, va a ser una combinación de números primos.

Y es a partir de esta definición de donde podemos tomar el teorema de factorización única en primos, el cual dice:

Teorema 2.2.2 (Teorema fundamental de la aritmética)**.** *Todo número entero mayor que 1, es el producto finito de números primos, y además la factorización es única obviando permutaciones.*

Demostración. La tomamos del Teorema 1.12 de Varona [8].

Hemos visto antes que todo número mayor que 1 es primo o producto de primos. Para ver que la factorización es única salvo permutación procedemos por inducción. Lo verificamos para $n = 2$, que es primo. Suponemos que es cierto para números menores que un n. Hay que probar que si

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

con los p_i y los q_j primos, a lo mejor repetidos, entonces $r = s$ y hay alguna permutación σ de $1, 2, \ldots, r$ tal que $p_i = q_{\sigma(j)}$.

Necesitamos recordar otro resultado de Euclides:

Lema 2.2.3 (Euclides)**.** *Si un primo divide a un producto, divide a uno de los factores.*

Entonces aplicando este lema, como p_r divide al producto $q_1 q_2 \cdots q_s$, divide a algún factor q_k. Pero como son primos tiene que ser $p_r = q_k$. Cancelando este primo de ambos lados del producto queda

$$p_1 p_2 \cdots p_{r-1} = \prod_{j \neq k}^{s-1} q_j < n$$

que es una igualdad de longitud una unidad menos. Esto suponiendo que quedan primos, pues podría ser $r = 1$ y a la izquierda tendríamos 1, pero entonces a la derecha si hubiera primos sería una contradicción porque ya sería mayor que 1. El mismo razonamiento sirve si $s = 1$. En tal caso tendríamos $r = s = 1$ y habríamos acabado.

Descartando este caso, o sea suponiendo $r, s \geq 2$, por inducción, $r-1 = s-1$, y entonces $r = s$, y los primos $p_1, \ldots, p_{r-1}$ son una permutación de los primos $\{q_1, \ldots, q_s\} \setminus \{q_k\}$. Llamemos σ a una biyección $\{1, \ldots, r-1\} \to \{1, \ldots, r\} \setminus \{k\}$ con $p_j = q_{\sigma(j)}$permutación. La extendemos por $\sigma(r) = k$ y obtenemos la permutación que queríamos para n. □

Como corolario de este teorema tenemos que las multiplicidades de cada primo en la descomposición son únicas también, es decir; dado un número compuesto, y dada su descomposición en factores primos, el número de veces que está cada divisor primo en ella es fijo.

2.3. Congruencias módulo m

En tercer lugar, una de las cosas que vamos a estar utilizando en abundancia van a ser las congruencias módulo m, las cuales veremos como en los apartados anteriores por encima, viendo la definición, algunas propiedades y la notación que vamos a utilizar en este trabajo.

Definición 2.3.1 (Congruencia)**.** *Para todo $m \geq 2$, decimos que a es equivalente a b módulo m y lo denotamos:*

$$a \equiv b \text{ mód } m \tag{2.3.1}$$

si y solo si $m|a-b$, es decir, si m divide a $a-b$.

Al igual que hicimos con el apartado de divisibilidad vamos a ver ahora una serie de propiedades sobre las congruencias:

Proposición 2.3.2. *La congruencia módulo m satisface estas propiedades:*

1. *Es una relación de equivalencia en los enteros.*
2. *Hay m clases de equivalencia distintas, llamadas clases de restos módulo m. Denotamos por $[a]$ a la clase de a* mód m.
3. *Sea $P(x)$ un polinomio con coeficientes enteros. Dados enteros a y b tenemos que $a \equiv b$* mód $m \implies P(a) \equiv P(b)$ mód m.
4. *Están bien definidas la suma y producto de clases:*

$$[a]+[b]=[a+b], \qquad [a]\cdot[b]=[a\cdot b]$$

Las clases módulo m forman un anillo conmutativo que denotamos por $\mathbb{Z}_m$ ó $\mathbb{Z}/m\mathbb{Z}$. El elemento neutro para la suma es $[0]$ y para el producto $[1]$.

Demostración.

1. Vemos las propiedades transitiva, simétrica y reflexiva.

   a) La propiedad reflexiva es trivial pues dado un número entero a, es equivalente a si mismo módulo cualquier m, pues por la definición esto significa que m divide a $a-a$ lo cual es 0 , y vimos que cualquier número distinto al 0 dividía al 0. Como $m \geq 2$ divide al 0.

   b) En segundo lugar veamos la propiedad simétrica, la cual es fácil de ver, pues tomamos a y b dos números enteros, si se verifica que $a \equiv b(\text{mód}m)$ tenemos que m divida a $a-b$, pero como trabajamos en los enteros también divide á $-(a-b)$, lo cual es igual a $b-a$ y por lo tanto $b \equiv a(\text{mód}m)$.

c) Por último, nos queda la propiedad transitiva, la cual es algo más compleja que las otras dos, pero veamos su demostración siguiendo el punto 2.1 del libro de Varona [8]. Para ello tomaremos 3 enteros, los llamaremos a, b y c, de modo que si $a \equiv b$ mód m significa que $a - b = km$ y de manera equivalente tenemos que $b \equiv c$ mód m lo que significa que $b - c = k'm$. De aquí obtenemos que si tomamos $a - c$ tenemos $a - c = (a - b) + (b - c) = km + k'm = (k + k')m$ y por lo tanto $a \equiv c(\text{mód}m)$, con lo que concluimos.

2. Hay m clases de restos módulo m, pues si tomamos cualquier número entero y lo dividimos por m, hay m restos distintos posibles, desde el 0 hasta el $m - 1$, al conjunto de números tales que al dividir entre m tienen resto r es una clase de equivalencia, también conocida como clase de resto y se denota como $[r]$.

3. Para verlo escribimos $P(x) = \sum_{k=0}^{n} c_k x^k$ con c_k enteros y $b - a = lm$. Entonces

$$P(b) - P(a) = \sum_{k=1}^{n} c_k(b^k - a^k)$$

porque se cancela el término constante c_0. Como para $k \geq 1$ tenemos la igualdad

$$b^k - a^k = (b - a)(b^{k-1} + b^{k-2}a + \cdots + ba^{k-2} + a^{k-1}) = lm \cdot N_k$$

con un entero N_k, concluimos que $P(b) - P(a)$ es múltiplo de m.

4. Por último, tenemos que las distintas clases $[a]$ forman un anillo. Primero venos que están bien definidas la suma y producto de clases de equivalencia.

   - Tomaremos dos clases de equivalencia, $[a]$ y $[b]$ y veamos en primer lugar que la suma esta bien definida, es decir, que no depende del representante escogido. Para ello, tomamos $a \equiv c$ mód m y $b \equiv d$ mód m y por tanto $a - c = km$ y $b - d = lm$ y tenemos que $(a + b) - (c + d) = (k + l)m$ por tanto $a + b \equiv c + d$ mód m, y por lo tanto esta bien definida.
   - De manera similar para el producto tenemos, que tomaremos dos clases de equivalencia, $[a]$ y $[b]$ y vamos a ver ahora que el producto esta bien definido, es decir, que no depende del representante escogido. Para ello, tomamos $a \equiv c$ mód m y $b \equiv d$ mód m con $a - c = km$ y $b - d = lm$ y tenemos que $ab - cd = (c + km)(d + lm) - cd = (cl + dk + lkm)m$ y por lo tanto tenemos que $a \cdot b \equiv c \cdot d$ mód m, y por lo tanto esta bien definido.
   - Por último, se comprueba de lo anterior que el elemento neutro para la suma es $[0]$ y el elemento neutro del producto $[1]$.
   - El resto de propiedades de anillo conmutativo se deducen a partir de las definiciones anteriores y de las propiedades correspondientes para los enteros.

□

2.4. El grupo de unidades

El último apartado que veremos en este capítulo será el grupo de unidades, el cual tiene bastante que ver con el apartado anterior.

En primer lugar, veremos una caracterización de lo que es dicho grupo.

Lema 2.4.1 (Unidades módulo m)**.** *Una clase de las anteriores, llamémosla $[a]$, es una unidad en $\mathbb{Z}_m$, si y solo si el máximo común divisor de a y m es 1, es decir; si son primos entre sí. Denotaremos al grupo de unidades de $\mathbb{Z}_m$ por $\mathbb{U}_m$.*

Demostración. Si $[a]$ es una unidad hay una clase $[b]$ con $[a] \cdot [b] = [ab] = [1]$. Entonces $ab = 1 + qm$ o sea $ab - qm = 1$. Con esto, si d es un divisor de a y de m también es divisor de 1, por tanto $d = 1$.

Si el máximo común divisor de a y m es 1, por la **identidad de Bézout** existen enteros b y q con $ab - qm = 1$, de lo cual se concluye que $[a] \cdot [b] = [1]$. □

Definición 2.4.2. *El tamaño de este grupo lo mediremos con la **función phi de Euler**, la cual denotamos como ϕ. De modo que dado un $m \geq 2$, tenemos que:*

$$\phi(m) = \#\mathbb{U}_m \tag{2.4.1}$$

Por el lema anterior, y siguiendo, la función ϕ de Euler es el número de enteros positivos menores que n los cuales son primos con n, es decir;

$$\phi(n) = \sum_{k=1}^{n}{}' 1 \tag{2.4.2}$$

donde ' indica que la suma es solo para esos k los cuales son primos respecto de n.

Ejemplo 2.4.3. *Para $n = 5$ tendríamos que el 1, el 2, el 3 y el 4 serían primos con respecto con 5 y por lo tanto $\phi(5) = 4$.*

Para $n = 6$ tendríamos que el 1 sería primo, el 2 no, porque el 2 es un divisor común de 2 y 6, el 3 tampoco pues sería divisor común del 3 y el 6, el 4 tampoco, pues tienen un divisor común que es el 2, el 5 sería primo, y el 6 no, por lo tanto solo tendríamos 2 primos el 1 y el 5 con respecto de 6, y entonces $\phi(6) = 2$. Con este ejemplo podemos darnos cuenta de que cuando decimos que k y n son primos, no nos referimos a que k no sea divisor de n si no a que no tengan ningún divisor en común, por ejemplo, en el caso anterior el 4 no divide al 6, pero tienen el 2 como divisor común.

La tabla de los primeros 10 valores de ϕ es

n	1	2	3	4	5	6	7	8	9	10
$\phi(n)$	1	1	2	2	4	2	6	4	6	4

Ahora que hemos visto la definición y algún ejemplo, veamos algunas de sus propiedades:

Proposición 2.4.4. *La función phi de Euler satisface:*

1. *Si tomamos un número primo, p; tenemos que $\phi(p) = p - 1$, es decir, que la función de Euler de un primo p es uno menos.*

2. *Si tomamos ahora un primo cualquiera p del conjunto de los primos, y tomamos $k \geq 1$ un número entero, se verifica que:*

$$\phi(p^k) = p^{k-1}(p-1) = p^k \left(1 - \frac{1}{p}\right) \tag{2.4.3}$$

3. *En tercer lugar, para cualquier m tenemos que:*

$$\phi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right) \tag{2.4.4}$$

Demostración.

1. Esto es obvio, porque si un número es primo cualquier número menor que p es primo con él, y por lo tanto hay $p-1$ números que lo cumplen.

2. Veamos una demostración de esto, basándonos en el punto 13.5 del libro de Saban Alaca y Kenneth S. William [1].

   Tomando como referencia dicho teorema, tomamos p un número primo y k un número natural, sin contar el 0 como natural.

   Es obvio que hay $p^k - 1$ números menores que p^k, de los cuales cada p términos hay un múltiplo de p, y por lo tanto hay $p^{k-1} - 1$ y el resto son coprimos con p. Por lo tanto queda:

$$\phi(p^k) = (p^k - 1) - (p^{k-1} - 1) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k \left(1 - \frac{1}{p}\right) \tag{2.4.5}$$

   con lo cual concluimos.

3. Para demostrar esto último cabe tener en cuenta que si tomamos dos números a y b, que sean coprimos entre sí, se verifica:

$$\phi(ab) = \phi(a)\phi(b) \tag{2.4.6}$$

   porque los factores de ab con a y b coprimos entre sí, son los productos de un factor de a por un factor de b y esto es de manera única. Si juntamos esto con la demostración anterior, y tomamos la descomposición en primos de un número m, tenemos:

$$\phi(m) = \phi\left({p_1}^{n_1} {p_2}^{n_2} ... {p_r}^{n_r}\right) \tag{2.4.7}$$

   Como cada una de las p_i son los primos que componen m con sus multiplicidades, por lo anterior podemos separarlo de modo que obtenemos:

$$\phi\left({p_1}^{n_1} {p_2}^{n_2} ... {p_r}^{n_r}\right) = \phi\left({p_1}^{n_1}\right) \phi\left({p_2}^{n_2}\right) ... \phi\left({p_r}^{n_r}\right) \tag{2.4.8}$$

   Y por el apartado anterior podemos extenderlo y nos quedará:

$$= {p_1}^{n_1} {p_2}^{n_2} ... p_r^{n_r} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) ... \left(1 - \frac{1}{p_r}\right) \tag{2.4.9}$$

donde la primera parte del producto es la descomposición de m y la segunda parte se puede poner como el producto de esas diferencias para todos los primos que dividen m, de modo que acabaríamos pues lo anterior es:

$$m \prod_{p|m} \left(1 - \frac{1}{p}\right) \tag{2.4.10}$$

y quedaría demostrado.

□

Capítulo 3

Las ideas de Euler

Como ya hemos dicho anteriormente la primera condición para que las progresiones aritméticas del tipo $a+mn$ tenga infinitos números primos es que a y m sean primos entre sí, es decir, que su máximo común divisor sea el 1, pues si no fuera así y el máximo común divisor fuese un entero d mayor que 1, todo término de esta progresión sería divisible entre d, y por lo tanto no sería primo.

Dirichlet fue el primero en demostrar que esta condición era suficiente para que existieran infinitos números primos en estas progresiones en el teorema que queremos demostrar.

Aunque Dirichlet baso su idea en una demostración de Euler, con la cual demostró la infinitud de los números primos demostrando que el sumatorio de $\frac{1}{p}$ donde p tomaba el valor de todos los primos diverge, es decir;

$$\sum_{p} \frac{1}{p} = \infty \tag{3.0.1}$$

Y esta idea, es la que vamos a desarrollar en este apartado.

3.1. Función zeta

En primer lugar, veamos lo que se conoce como la función zeta de Riemann, la cual denotamos como ζ.

Definición 3.1.1. *Definimos la* ***función zeta de Riemann*** *como:*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \tag{3.1.1}$$

donde s es un número complejo cuya parte real es mayor que 1.

Veamos varias cosas de dicha función pero que no demostramos al no necesitarlas aquí. Para ello vamos a guiarnos con la nota 8.9 del libro de Varona [8].

En primer lugar vamos a ver como esta zeta de Riemann prolonga a una función sobre todo el plano complejo, la cual tiene un único polo en $s = 1$, que es simple. En segundo lugar siguiendo el punto 10.7.1 de Varona [8] tenemos que realizando integrales

por caminos podemos extender la propia función $\zeta(s)$ y cumpliéndose la ecuación funcional

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s) \tag{3.1.2}$$

función la cual relaciona los valores de ζ en los puntos s y $1-s$.

Además de dicha ecuación funcional se deduce que en el semiplano $Re(s) < 0$, la zeta de Riemann se anula exclusivamente en $s = -2, -4, -6...$, los cuales vamos a llamar ceros triviales.

De igual manera Riemann define la función:

$$\xi(s) = \frac{1}{2} s(s-1)\Gamma\left(\frac{s}{2}\right) \pi^{\frac{-s}{2}} \zeta(s) \tag{3.1.3}$$

la cual es entera, es decir; holomorfa en todo el plano complejo, dado que el factor s anula el polo de $\Gamma\left(\frac{s}{2}\right)$ en 0, el factor $(s-1)$ anula el polo de $\zeta(s)$ en 1, y los ceros triviales de la zeta anulan los demas polos de $\Gamma\left(\frac{s}{2}\right)$.

Además, esta ecuación funcional cumple que:

$$\xi(s) = \xi(1-s) \tag{3.1.4}$$

Es a partir de estas idea que Riemann llegó a la conocida como Conjetura de Riemman, la cual decía que todos los ceros no triviales tienen todos parte real igual a $\frac{1}{2}$, y la cual a día de hoy sigue sin demostrar.

3.2. La fórmula del producto para la función zeta

Lo siguiente que queremos ver es que para todo s tal que su parte real sea mayor que 1, se verifica la siguiente fórmula:

Teorema 3.2.1 (La fórmula del producto)**.** *Para un número complejo de parte real mayor que* 1*,*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1} \tag{3.2.1}$$

Pero antes de poder ver la demostración de esta igualdad, veremos varias cosas.

En primer lugar veamos las definiciones de función multiplicativa y completamente multiplicativa, tomando el capitulo 2 de teoría analítica de números de Carlos Ivorra Castillo [3].

Definición 3.2.2. *Una función aritmética f es* ***multiplicativa*** *si no es identicamente nula y además $f(nm) = f(n)f(m)$ para todo n y m naturales primos entre si y verifica que $f(1) = 1$.*

Definición 3.2.3. *Una función aritmética f es* ***completamente multiplicativa*** *si no es identicamente nula y además $f(nm) = f(n)f(m)$ para todo n y m naturales cualesquiera y verifica $f(1) = 1$.*

Con estas definiciones ya podemos ver la identidad de Euler siguiendo el teorema 9.1 del Varona [8], con la cual la posterior demostración de la fórmula del producto para la función zeta se simplifica mucho.

Teorema 3.2.4. *Sea f una función multiplicativa tal que la serie $\sum_n f(n)$ es absolutamente convergente. Entonces:*

$$\sum_{n=1}^{\infty} f(n) = \prod_p (1 + f(p) + f(p^2) + ...) \tag{3.2.2}$$

Si f es completamente multiplicativa, se tiene, además;

$$\sum_{n=1}^{\infty} f(n) = \prod_p \frac{1}{1 - f(p)} \tag{3.2.3}$$

En ambos casos, a los productos se los llama ***producto de Euler*** *de la serie.*

Demostración. Tenemos que ver dos partes en la demostración, para demostrar ambas fórmulas.

Veamos en primer lugar que se verifica la primera fórmula del teorema. Para ello cogemos un numero real $x \geq 2$ y consideramos el producto finito siguiente:

$$P(x) = \prod_{p \leq x} (1 + f(p) + f(p^2) + ...) \tag{3.2.4}$$

donde cada factor del producto es una serie. Como $\sum_n f(n)$ es absolutamente convergente, en la fórmula anterior podemos multiplicar y reordenar términos, sin que cambie el valor final de P(x), y entonces podremos poner cada término como:

$$f\left(p1^{a1}\right) f\left(p2^{a2}\right) ... f\left(pn^{an}\right) = f\left(p1^{a1} p2^{a2} ... pn^{an}\right) \tag{3.2.5}$$

ya que por hipótesis f es multiplicativa.

Tomemos ahora el conjunto de todos los números naturales n tal que todos sus factores primos sean $\leq x$ y llamemos a este conjunto A_x.

Entonces podemos escribir $P(x) = \sum_{n \in A_x} f(n)$ y

$$\sum_{n=1}^{\infty} f(n) - P(x) = \sum_{n \in B_x} f(n) \tag{3.2.6}$$

donde B_x es igual al conjuntos de los naturales menos A_x que sera el conjuntos de aquellos naturales que tienen un factor primo mayor que x, y por lo tanto tenemos:

$$|\sum_{n=1}^{\infty} f(n) - P(x)| = |\sum_{n \in B_x} f(n)| \leq \sum_{n \in B_x} |f(n)| \leq \sum_{n > x} |f(n)| \tag{3.2.7}$$

Como por hipótesis, $\sum_{n=1}^{\infty} |f(n)|$ es convergente, podemos asegurar que cuando la x tienda a infinito, el ultimo sumatorio del desarrollo anterior tiende a 0, luego despejando tenemos que cuando la x tiende a infinito, $P(x)$ tiende a $\sum_{n=1}^{\infty} f(n)$ de donde sacamos la primera fórmula del enunciado.

Para ver la segunda, lo único que vamos a hacer es una deducción de ella a partir de la primera. De modo que sabiendo que f es completamente multiplicativa, entonces $f(p^k) = f(p)^k$, y por tanto para llegar a la segunda fórmula basta con sumar una serie geométrica:

$$1 + f(p) + f(p^2) + ... = 1 + f(p) + f(p)^2 + ... = \frac{1}{1 - f(p)} \tag{3.2.8}$$

Y estarían demostradas las dos fórmulas.

□

Podemos observar que si la serie es convergente debe ser $f(n) \to 0$ cuando $n \to \infty$. Para un primo p, como $p^k \to \infty$ cuando $k \to \infty$, esto implica que si f es completamente multiplicativa $f(p^k) = f(p)^k \to 0$ por tanto $|f(p)| < 1$ y la serie geométrica es convergente y está definida su suma $1/(1 - f(p))$.

Demostración del Teorema 3.2.1. Ahora ya podemos hacer una demostración de la fórmula vista al principio, para cual seguiremos el punto 9.1.1 del libro de Varona [8]:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1} \tag{3.2.9}$$

Euler lo que hizo fue aplicar las fórmulas del teorema anterior a la función $f(n) = n^{-s}$ la cual es completamente multiplicativa, así usando esta fórmula obtenemos:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{1}{p^s}} = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1} \tag{3.2.10}$$

□

Podemos observar que la fórmula del producto para la función zeta de Riemann es la expresión analítica de la factorización única en los enteros.

3.3. Infinitud de primos según Euler

Para acabar con este capitulo, lo último que tenemos que ver es como Euler demostró que había infinitos primos. Para ello propuso un teorema en 1737, para el cual vamos a tomar el teorema 9.2 del libro de Varona [8].

Teorema 3.3.1. *La serie de los inversos de los primos es divergente, es decir;*

$$\sum_{p} \frac{1}{p} = \infty \tag{3.3.1}$$

Demostración. Para ver la demostración veremos también del libro de Varona [8] el apartado 9.1.1. Para empezar la demostración tomaremos la igualdad:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1} \tag{3.3.2}$$

y tomaremos logaritmos a ambos lados, de modo que en la derecha de la igualdad el menos uno pasará a multiplicar y el producto lo transformaremos a una suma

$$\log\left(\sum_{n=1}^{\infty}\frac{1}{n^s}\right) = -\sum_{p}\log\left(1-\frac{1}{p^s}\right) \tag{3.3.3}$$

con $s > 1$.

Usando la aproximación de Taylor para el logaritmo vamos a tener que:

$$-\log(1-x) = x + R(x) \tag{3.3.4}$$

donde $R(x)$ es una función tal que $|R(x)| \leq x^2$ cuando $0 \leq x \leq \frac{1}{2}$. Y por lo tanto lo que obtenemos aplicando esto es:

$$\log\left(\sum_{n=1}^{\infty}\frac{1}{n^s}\right) = \sum_{p}\frac{1}{p^s} + \sum_{p}R\left(\frac{1}{p^s}\right)$$

y podemos ver que el último sumatorio converge si hacemos tender la s a 1, debido a:

$$\sum_{p}|R\left(p^{-s}\right)| \leq \sum_{p}p^{-2s} \leq \sum_{m=1}^{\infty}m^{-2s} \leq \infty \tag{3.3.5}$$

para cualquier $s > \frac{1}{2}$. Pero como en la igualdad inicial la parte de la izquierda sabemos que tiende a infinito cuando la s tiende a 1 diverge, la única manera de que la igualdad sea cierta es que la serie de los inversos de los primos también diverga. □

Como corolario de este teorema podemos entonces deducir que hay infinitos números primos, pues si los números primos fuesen finitos, tendríamos una suma finita y racional, y hemos demostrado que no es asi.

Además con esto demostramos que si cogemos

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

tenemos:

$$\lim_{s\to 1^+}(P(s)) = \infty \tag{3.3.6}$$

Esto se obtiene juntando dos cosas. En primer lugar, vemos la idea de que $\zeta(1^+) = \infty$, lo cual deducimos de que la función zeta decrece entre el 1 y el ∞ y que para todo $s > 1$ y $x > 0$, tenemos:

$$\zeta(s) \geq \sum_{n\leq x}\frac{1}{n^s} \tag{3.3.7}$$

y tomando $s \to 1$, se queda:

$$\zeta(1^+) \geq \sum_{n\leq x}\frac{1}{n} \tag{3.3.8}$$

y haciendo tender ahora la x a ∞, obtenemos:

$$\zeta(1^+) \geq \sum_{n=1}^{\infty} \frac{1}{n} = \infty \tag{3.3.9}$$

con lo que estaría.

En segundo lugar tomamos la idea de que $P(s)$ aproxima el $\log \zeta(s)$. Pues con lo demostrado en la fórmula del producto tenemos:

$$\log \zeta(s) = \sum_{p} \frac{1}{p^s} + O(1) = P(s) + O(1) \tag{3.3.10}$$

Juntando estas dos ideas obtenemos que efectivamente;

$$\lim_{s \to 1^+} (P(s)) = \infty \tag{3.3.11}$$

Estamos usando la notación «O grande» que en general es de la forma $f = O(g)$ para $s \to s_0$ donde s_0 puede ser infinito, y significa que $|f(s)| \leq M|g(s)|$ para alguna constante M y s lo suficientemente cerca de s_0. Pueden ser complejos o reales, y límites laterales también. En particular $f = O(1)$ significa que $f(s)$ está acotada para s cerca de s_0.

Capítulo 4

Demostración del teorema de Dirichlet

Una vez vista la introducción con el objetivo del trabajo y los inicios históricos del teorema que queremos demostrar, y vistas las ideas de Euler, vamos a centrarnos en la demostración del Teorema de Dirichlet.

4.1. Estrategia

En primer lugar veremos cuales fueron las primeras ideas de Dirichlet, las cuales se planteó a partir de las ideas de Euler que hemos visto anteriormente.

Lo primero que vamos a hacer es tomar un número m fijo y mayor o igual a 2, y tomamos $\mathbb{P}(a, m)$ que definiremos como el conjunto de los números primos p tales que $p \equiv a$ mód m y al igual que hizo Euler, para el conjunto de todos los números, Dirichlet definió la función:

$$P_a(s) = \sum_{p \in \mathbb{P}(a,m)} \frac{1}{p^s} \tag{4.1.1}$$

donde la s es un número que verifica que su parte real es mayor que 1. La idea entonces, al igual que hizo Euler, es demostrar:

$$\lim_{s \to 1^+} P_a(s) = \infty \tag{4.1.2}$$

pues si demostramos esto, habríamos demostrado que hay infinitos primos de la forma $p \equiv a$ mód m pues tenemos:

$$\infty = \lim_{s \to 1^+} \sum_{p \in \mathbb{P}(a,m)} \frac{1}{p^s} \leq \sum_{p \in \mathbb{P}(a,m)} \frac{1}{p} \tag{4.1.3}$$

Podemos observar como ya hemos dicho, el paralelismo que tiene esta idea de la de Euler, donde lo único que cambia es el conjunto en el que estamos trabajando, pues el planteamiento es el mismo, la cuestión es: ¿funcionará el mismo proceso para este nuevo conjunto?

La respuesta para esta pregunta es sencilla, NO, no vale este mismo proceso, pues encontramos algunas dificultades por el camino.

Volviendo atrás, lo primero que hacía Euler era poner la función zeta de Riemann como un producto, lo que hemos visto como la fórmula del producto para la función zeta en este mismo trabajo y es aquí donde encontramos el primer escollo. Si tomamos una estructura similar, tendremos las expresiones:

$$\zeta_a(s) = \sum_{n\in\mathbb{N}(a,m)} \frac{1}{n^s} \tag{4.1.4}$$

$$\prod_{p\in\mathbb{P}(a,m)} \left(1 - \frac{1}{p^s}\right)^{-1} \tag{4.1.5}$$

que son iguales a las de Euler pero transformadas para el conjunto en el que estamos trabajando.

El problema viene porque al igual que antes podíamos establecer una igualdad entre ellas, ahora esto no es así, pues; dadas dos funciones x e y ambas a módulo m, no implica que su producto xy sea a módulo m. De aqui obtenemos que si tomamos la función característica de $\mathbb{N}(a,m)$ para m fijo:

$$1_a(n) = \begin{cases} 1 \ si \ n \equiv a \text{ mód } m \\ \\ 0 \ si \ n \neq a \text{ mód } m \end{cases}$$

esta función no es multiplicativa en general, es decir; $1_a(xy) \neq 1_a(x)1_a(y)$.

Aún pese a ellos estas funciones nos van a permitir sumar sobre todos los naturales y primos:

$$\zeta_a(s) = \sum_{n\in\mathbb{N}(a,m)} \frac{1}{n^s} = \sum_{n=1}^{\infty} \frac{1_a(n)}{n^s} \tag{4.1.6}$$

$$P_a(s) = \sum_{p\in\mathbb{P}(a,m)} \frac{1}{p^s} = \sum_{p\in\mathbb{P}} \frac{1_a(p)}{p^s} \tag{4.1.7}$$

4.2. Productos

En esta sección nos centraremos en los productos.

Ya hemos visto, en la sección de la fórmula del producto en el capitulo de las ideas de Euler, las definiciones de cuando una función era multiplicativa y completamente multiplicativa, en las definiciones 8 y 9.

A parte de esto tenemos que ver el teorema sobre la fórmula del producto para las funciones que son completamente multiplicativas.

Teorema 4.2.1. *Dada una función f desde los naturales hasta los complejos y que sea completamente multiplicativa, se verifica en primer lugar:*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p\in\mathbb{P}} \left(1 - \frac{f(p)}{p^s}\right)^{-1} \tag{4.2.1}$$

si la serie es absolutamente convergente.

En segundo lugar para funciones solamente multiplicativas se verifica:

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p\in\mathbb{P}} \sum_{k=0}^{\infty} \frac{f\left(p^k\right)}{p^{ks}} = \prod_{p\in\mathbb{P}} \left(1 + \frac{f(p)}{p^s} + \frac{f\left(p^2\right)}{p^{2s}} + ...\right) \tag{4.2.2}$$

Demostración. Para ver la primera parte, basta con fijarnos en que es la misma igualdad que en la fórmula del producto para la función ζ, pero sustituyendo el 1 por una función f la cual es completamente multiplicativa.

Lo que hacemos entonces, usando esto y el teorema 4 de este mismo trabajo es tomar la función $f(n)*n^{-s}$ la cual es combinación de dos funciones completamente multiplicativa y por lo tanto es completamente multiplicativa y desarrollamos de la misma manera, de modo que:

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p\in\mathbb{P}} \frac{1}{1 - \frac{f(p)}{p^s}} = \prod_{p\in\mathbb{P}} \left(1 - \frac{f(p)}{p^s}\right)^{-1} \tag{4.2.3}$$

La segunda parte es trivial, pues en la primera igualdad lo que usamos es que todo número n se puede poner como producto de primos con sus respectivas multiplicidades, y en la segunda igualdad lo único que hacemos es extender el sumatorio. □

4.3. Caracteres

En primer lugar vamos a ver la definición de carácter, para posteriormente entrar en la definición de carácter de Dirichlet. Recordamos que las clases de restos módulo m son un anillo conmutativo $\mathbb{Z}_m$, y por tanto sus unidades $\mathbb{U}_m$ son un grupo abeliano.

Definición 4.3.1. *Un carácter módulo m es un morfismo de grupos $\chi : \mathbb{U}_m \to \mathbb{C}^*$.*

Dirichlet se basó para su demostración en lo que llamamos caracteres de Dirichlet. Veamos entonces que son y como obtenerlos. Dando por conocidas las definiciones y propiedades más básicas de los grupos, así como definiciones como la de grupo abeliano, pasemos primeramente a ver que es un carácter de un grupo y un grupo de caracteres.

Definición 4.3.2. *Sea G un grupo abeliano finito. Una función de valores complejos f definida en G se llama carácter de G si f verifica:*

1. *$f(ab) = f(a)f(b)$ para todo a y b de G.*
2. *Para algún c de G, $f(c)$ es no nulo.*

*Los caracteres, que son entonces los morfismos de G a $\mathbb{C}^*$, forman el **grupo dual** $\widehat{G}$.*

Veamos ahora la definición de carácter de Dirichlet.

Definición 4.3.3. *Dado un carácter f del grupo $\mathbb{U}_m$ de unidades módulo m, vamos a definir una función aritmética $\chi = \chi_f$ de la siguiente manera:*

$$\chi(n) = \begin{cases} f([n]) & si\ (n,m) = 1, \\ \\ 0 & si\ (n,m) > 1 \end{cases}$$

*Las funciones χ obtenidas asó son llamadas caracteres de Dirichlet de módulo m. El carácter **principal** módulo m, denotado por χ_1, es el que viene del carácter unidad, con valor 1, de $\mathbb{U}_m$:*

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

Una vez vista la definición de carácter de Dirichlet, vamos a ver un teorema que nos va a dar dos características principales de estos caracteres, en concreto que son multiplicativos y son periódicos de periodo m, para ello tomemos como referencia el teorema 6.15 de Apostol [2] para ver estas dos propiedades y la demostración de porque es así.

Teorema 4.3.4. *Hay $\phi(m)$ caracteres de Dirichlet modulo m, cada uno de los cuales es completamente multiplicativo y periódico de periodo m. Esto es, nosotros tenemos:*

1. *Para todo a y b*
$$\chi(ab) = \chi(a)\chi(b) \tag{4.3.1}$$
2. *Para todo n*
$$\chi(n+m) = \chi(n) \tag{4.3.2}$$
3. *Por el contrario, si χ es completamente multiplicativa y periódica con periodo m, y si $\chi(n) = 0$ si $(n,m) > 1$, entonces χ es uno de los caracteres de Dirichlet modulo m.*

Demostración.

1. Hay $\phi(m)$ caracteres f para el grupo G de clases de residuos reducidos modulo m, por lo que hay $\phi(m)$ caracteres χ_f mód m. La propiedad multiplicativa de χ_f se consigue de la f cuando a y b son relativamente primos con m. Si uno de los dos, a ó b, no son relativamente primos a m, entonces tampoco lo es ab, y por lo tanto ambos términos de la propiedad 1 del enunciado son 0.

2. La propiedad de la periodicidad se consigue del hecho que $\chi_f([n]) = \chi(n)$ y que $a \equiv b$ mód m implica que $(a,m) = (b,m)$.

3. Vamos a tomar la función f definida en el grupo G por la ecuación:
$$\chi(n) = f([n])\ si\ (n,m) = 1 \tag{4.3.3}$$
es un carácter de G, así χ es un carácter de Dirichlet modulo m.

□

Veamos ahora algunos ejemplos sencillos sobre los caracteres de Dirichlet para los casos más sencillos, tomando como referencia el libro de Apóstol capitulo 6 [2], así como los apuntes de Rafael Parra Machío sobre funciones especiales y caracteres de Dirichlet [7].

Ejemplo 4.3.5. *Los dos casos más sencillos son cuando m toma los valores 1 y 2, donde $\phi(m)$ es 1 siempre, y por lo tanto únicamente hay un carácter de Dirichlet, que es el carácter principal χ_1. Cuando m toma valores mayores o iguales a 3, entonces $\phi(m)$ siempre será mayor o igual que dos, sabiendo que cuanto mayor sea, $\phi(m)$ no tiene porque ser mayor, es decir, el aumento de una no implica el del otro. Por ejemplo, para $m = 5$, la $\phi(m)$ toma valor 4, pero cuando $m = 6$, la $\phi(m)$ es 2.*

Lo siguiente que vamos a ver son una tablas que tienen $\phi(m)$ filas, es decir, cada fila representa un carácter de Dirichlet, y m columnas. Veamos como crearlas y luego las iremos poniendo.

Para $m = 3$ y $m = 4$ vamos a tener que $\phi(m)$ es igual a 2 en ambos casos y lo que usaremos es $\chi(n)^{\phi(m)} = 1$ siempre que $(n, m) = 1$, y por lo tanto $\chi(n)$ es una raíz $\phi(m)$-ésima de la unidad. Además podemos observar que si χ es un carácter modulo m, también lo será el conjugado complejo $\overline{\chi}$. Con esto es suficiente para estas dos tablas

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

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

Cuando la m es igual a 5, tenemos que $\phi(m)$ es 4, y por lo tanto cuando $(n, 5) = 1$, $\chi(n)$ puede tomar como valores el $+1, -1, +i, -i$.

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

Como ya hemos dicho arriba que aumente la m no quiere decir que aumente el número de caracteres, ni la dificultad de la tabla por ejemplo cogamos un m mas grande que los anteriores, por ejemplo $m = 8$. Con este m, tenemos que $\phi(m)$ es igual a 4 y la tabla será la siguiente:

n	1	3	5	7
$\chi_1(n)$	1	1	1	1
$\chi_2(n)$	1	1	-1	-1
$\chi_3(n)$	1	-1	1	-1
$\chi_4(n)$	1	-1	-1	1

Pero esto no es caso particular, podemos seguir aumentando la m y que la tabla siga teniendo pocos caracteres, como el caso de m igual a 10 o a 12, donde el número de caracteres sigue siendo 4.

Llegamos a un resultado clave para la demostración, que es la ortogonalidad de los caracteres. Lo ponemos para un grupo abeliano finito en general.

Veamos ahora la definición de un producto que vamos a utilizar.

Definición 4.3.6. *Sea G un grupo abeliano finito y f y g dos funciones que van de este grupo G a los complejos. Definimos su producto por*

$$\langle f, g\rangle = \frac{1}{\#G}\sum_{a\in G} f(a)\overline{g(a)}. \tag{4.3.4}$$

Lema 4.3.7. *Se verifica que el producto definido por* (4.3.4) *es un producto hermítico en el $\mathbb{C}$-espacio vectorial $\mathbb{C}^G$ de funciones de G en $\mathbb{C}$.*

Demostración. Es claramente aditivo y sesquilineal. Se tiene

$$\langle f, f\rangle = (1/\#G)\sum_{a\in G} |f(a)|^2 \geq 0,$$

con igualdad si y sólo si cada $|f(a)| = 0$, o sea $f = 0$. □

Teorema 4.3.8 (Ortogonalidad de los caracteres)**.** *Sea G un grupo abeliano finito. Entonces los caracteres de G son una base ortonormal respecto al producto hermítico* (4.3.4)*.*

Demostración. Sea $n = \#G$. Empezamos observando que si $f : G \to \mathbb{C}^*$ es un carácter entonces f valora en las raíces n-ésimas de la unidad, pues $f(a)^n = f(a^n) = f(1) = 1$. En particular $|f(a)| = 1$. Entonces

$$\langle f, f\rangle = \frac{1}{n}\sum_{a\in G} |f(a)|^2 = \frac{1}{n}\sum_{a\in G} 1 = 1.$$

Ahora sean f, g dos caracteres distintos. Entonces hay un $b \in G$ con $f(b) \neq g(b)$, y como hemos visto que los caracteres tienen módulo 1,

$$f(b)/g(b) = f(b)g(b)^{-1} = f(b)\overline{g(b)} \neq 1$$

Multiplicando la definición del producto $\langle f, g\rangle$ por $\lambda = f(b)\overline{f(b)}$ queda, por ser caracteres

$$\lambda\langle f, g\rangle = \frac{1}{n}\sum_{a\in G} f(a)f(b)\overline{g(a)g(b)} = \frac{1}{n}\sum_{a\in G} f(ab)\overline{g(ab)},$$

y como G es un grupo, $c = ab$ recorre todos los elementos de G cuando a lo hace. Entonces

$$\lambda\langle f, g\rangle = \frac{1}{n}\sum_{c\in G} f(c)\overline{g(c)} = \langle f, g\rangle$$

con lo cual

$$(1 - \lambda)\langle f, g\rangle = 0$$

y como $\lambda \neq 1$ concluimos que $\langle f, g\rangle = 0$.

Para ver que los caracteres son una base necesitamos el resultado que dice que para un grupo abeliano finito hay tantos caracteres como elementos del grupo. De hecho el

grupo G y el grupo dual $\widehat{G}$ son **isomorfos**. Esto se deduce del teorema de clasificación de grupos abelianos finitos, descomponiendo en factores cíclicos y para cíclicos eligiendo un generador se puede comprobar. Entonces el conjunto ortonormal de caracteres tiene n elementos, y n es también la dimensión del espacio de funciones $\dim_{\mathbb{C}} \mathbb{C}^G = \dim_{\mathbb{C}} \mathbb{C}^n = n$ por tanto son una base.

□

Por lo tanto, para una función $f : G \to \mathbb{C}$ tenemos que, por ser los caracteres base ortonormal, se verifica:

$$f = \sum_{\chi \in \widehat{G}} \langle f, \chi \rangle \chi \tag{4.3.5}$$

Ahora sustituiremos la función f por la función característica 1_a, de modo que obtenemos:

$$1_a = \sum_{\chi \in \widehat{G}} \langle 1_a, \chi \rangle \chi \tag{4.3.6}$$

Calculemos ahora el producto 1_a y χ.

$$\langle 1_a, \chi \rangle = \frac{1}{\#G} \sum_{b \in G} 1_a(b) \overline{\chi(b)} \tag{4.3.7}$$

donde la función característica aplicada a b va a ser 0 siempre que a y b sean distintos y 1 cuando a es igual a b, con lo que queda:

$$\frac{1}{\#G} \sum_{b \in G} 1_a(b) \overline{\chi(b)} = \frac{1}{\#G} 1_a(a) \overline{\chi(a)} \tag{4.3.8}$$

Y tenemos que $1_a(a) = 1$, con lo que obtenemos:

$$\frac{1}{\#G} 1_a(a) \overline{\chi(a)} = \frac{\overline{\chi(a)}}{\#G} \tag{4.3.9}$$

Sustituyendo esto en la fórmula de la función característica anterior y tomando la definición del producto hermítico obtenemos:

$$1_a = \frac{1}{\#G} \sum_{\chi \in \widehat{G}} \overline{\chi(a)} \chi \tag{4.3.10}$$

Por último, aplicamos al caso $G = \mathbb{U}_m$ y por lo visto anteriormente sabemos que el tamaño de este grupo será $\phi(m)$ y obtenemos:

$$1_a = \frac{1}{\phi(m)} \sum_{\chi \in \widehat{\mathbb{U}}_m} \overline{\chi(a)} \chi \tag{4.3.11}$$

Y así obtenemos la expresión de las funciones características en función de los caracteres, lo cual usaremos para seguir con nuestra demostración.

4.4. Series

Retomamos la demostración del teorema de Dirichlet de infinitud de primos en una progresión aritmética $\mathbb{P}(a,m)$ con $(a,m)=1$.

En este apartado tomaremos $P_a(s)$ la cual ya habíamos definido y tenemos:

$$P_a(s)=\sum_{p\in\mathbb{P}}\frac{1_a(s)}{p^s} \tag{4.4.1}$$

y sustituyendo la fórmula obtenida en el apartado anterior para la función característica tenemos:

$$P_a(s)=\frac{1}{\phi(m)}\sum_{\chi\in\widehat{\mathbb{U}}_m}\overline{\chi(a)}\sum_{p\in\mathbb{P}}\frac{\chi(p)}{p^s} \tag{4.4.2}$$

y si llamamos $\sum_{p\in\mathbb{P}}\frac{\chi(p)}{p^s}=P(\chi,s)$ tenemos:

$$P_a(s)=\frac{1}{\phi(m)}\sum_{\chi\in\widehat{\mathbb{U}}_m}\overline{\chi(a)}P(\chi,s) \tag{4.4.3}$$

Una vez visto esto, volveremos a nuestro objetivo final, el cual es demostrar que:

$$\lim_{s\to 1^+}P_a(s)=\infty \tag{4.4.4}$$

Para ello veremos primero la definición de L-función/L-serie de Dirichlet.

Definición 4.4.1 (L-series de Dirichlet)**.** *La L-función/L-serie de Dirichlet para un carácter de Dirichlet χ módulo m es*

$$L(\chi,s)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s} \tag{4.4.5}$$

para todo s cuya parte real sea mayor que 1.

Como hemos dicho la idea es imitar la demostración de infinitud de Euler, tomando ahora $L(\chi,s)$ y $P(\chi,s)$ como $\zeta(s)$ y $P(s)$, esto nos da un mejor resultado que con $\zeta_a(s)$ y $P_a(s)$ pues como ya hemos visto los caracteres de Dirichlet son completamente multiplicativos.

Y ahora con esto ya podemos seguir el desarrollo seguido por Euler pero con estas nuevas funciones.

Para ello, al igual que teníamos la definición de la zeta de Riemman como producto, y hemos dicho que $\zeta(s)=L(\chi,s)$, se cumple que para todo s tal que su parte real sea mayor que 1:

$$L(\chi,s)=\prod_{p\in\mathbb{P}}\left(1-\frac{\chi(p)}{p^s}\right)^{-1} \tag{4.4.6}$$

Al igual que hicimos ya en Euler, tomaremos logaritmos a ambos lados de la igualdad, sabiendo que al lado derecho de esta el exponente baja y el producto pasa a un sumatorio,

de modo que queda:

$$\log(L(\chi, s)) = -\sum_{p\in\mathbb{P}} \log\left(1 - \frac{\chi(p)}{p^s}\right) \tag{4.4.7}$$

Y usando la aproximación de Taylor para el logaritmo que ya usamos anteriormente, $-\log(1-x) = x + O(x^2)$ queda:

$$\log(L(\chi, s)) = P(\chi, s) + O(1) \tag{4.4.8}$$

para $s \to 1^+$ y donde recordemos que $P(\chi, s) = \sum_{p\in\mathbb{P}} \frac{\chi(p)}{p^s}$ y $O(1)$ representa una función holomorfa para todo s cuya parte real sea mayor que $\frac{1}{2}$.

4.5. Relación fundamental

Una vez acabada la parte de series, y como enlace para empezar a ver el carácter principal, vamos a ver la relación que hay entre la suma sobre los primos y las L-funciones antes definidas.

Para ver este apartado, vamos a tomar dos de las fórmulas anteriores y luego las juntaremos.

En primer lugar, la última fórmula vista:

$$\log(L(\chi, s)) = P(\chi, s) + O(1) \tag{4.5.1}$$

y en segundo lugar, la última definición que vimos de $P_a(s)$:

$$P_a(s) = \frac{1}{\phi(m)} \sum_{\chi\in\widehat{\mathbb{U}}_m} \overline{\chi(a)} \sum_{p\in\mathbb{P}} \frac{\chi(p)}{p^s} \tag{4.5.2}$$

Juntando estas dos, obtenemos que para todo número s cuya parte real sea mayor que 1:

$$P_a(s) = \frac{1}{\phi(m)} \sum_{\chi\in\widehat{\mathbb{U}}_m} \overline{\chi(a)} \log(L(\chi, s)) + O(1) \tag{4.5.3}$$

Para obtener la demostración deseada, tenemos que ver, como ya hemos dicho antes, que $\lim_{s\to 1^+}(P_a(s)) = \infty$.

Usando la fórmula vista en este apartado, únicamente tendremos que trabajar la parte de las L-funciones, es decir; $L(\chi, s)$, aunque esto no es del todo trivial y lo primero que haremos será separar el carácter principal del resto de caracteres.

4.6. Carácter Principal

En la sección de caracteres ya vimos como llegar a la definición de estos y lo que eran. Entre ellos podemos diferenciar uno de ellos, al que vamos a llamar carácter principal y denotaremos χ_1, de modo que va a ser el elemento unidad del grupo en el que estamos trabajando.

Recordamos que el carácter principal módulo m, que es la unidad en $\widehat{\mathbb{U}}_m$, se define como:

$$\chi_1(n) = \begin{cases} 1 \ si \ (n,m) = 1 \\ \\ 0 \ si \ (n,m) > 1 \end{cases} \tag{4.6.1}$$

De modo que vamos a estudiar la L-función para dicho carácter. Lo que queremos demostrar en este caso es:

$$L(\chi_1, s) = \zeta(s) \prod_{p|m} \left(1 - \frac{1}{p^s}\right) \tag{4.6.2}$$

Tenemos que para cualquier carácter χ se cumple:

$$L(\chi, s) = \prod_{p \in \mathbb{P}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \tag{4.6.3}$$

y tenemos que cuando p divide a m,su máximo común divisor es > 1 y por lo tanto $\chi(p) = 0$ y nos quedaría la multiplicación por 1 y por lo tanto podrían quitarse dichos términos y dejar el producto en función de aquellos p que no dividen a m.

$$L(\chi, s) = \prod_{p \nmid m} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \tag{4.6.4}$$

y por definición sabemos que:

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \sum_{(n,m)=1} \frac{\chi(n)}{n^s} \tag{4.6.5}$$

Por lo tanto, hasta aquí, tenemos:

$$L(\chi, s) = \sum_{(n,m)=1} \frac{\chi(n)}{n^s} = \prod_{p \in \mathbb{P}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \prod_{p \nmid m} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \tag{4.6.6}$$

Además $\zeta(s) = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1}$, tomando $\chi = \chi_1$ y siguiendo las definiciones anteriores nos queda:

$$L(\chi_1, s) = \prod_{p \nmid m} \left(1 - \frac{1}{p^s}\right)^{-1} \tag{4.6.7}$$

Por lo tanto, si tomamos $\zeta(s)$ y lo multiplicamos por $\prod_{p|m} \left(1 - \frac{1}{p^s}\right)$ obtenemos:

$$\zeta(s) \prod_{p|m} \left(1 - \frac{1}{p^s}\right) = \prod_{p \nmid m} \left(1 - \frac{1}{p^s}\right)^{-1} \tag{4.6.8}$$

con lo que concluimos.

Por tanto si aquí hacemos tender la s al 1 por el lado positivo tenemos que el

$$\lim_{s\to 1^+}(L(\chi_1,s))=\infty \tag{4.6.9}$$

ya que el límite de la función zeta en este caso es infinito.

Por lo tanto volviendo a la fórmula de la sección anterior:

$$P_a(s)=\frac{1}{\phi(m)}\sum_{\chi\in\widehat{\mathbb{U}}_m}\overline{\chi(a)}\log(L(\chi,s))+O(1) \tag{4.6.10}$$

acabamos de ver que el término principal es infinito para $s=1$.

Con esto daríamos finalizada esta sección y nos quedaría un último paso para acabar la demostración, que sería estudiar que pasa en aquellos caracteres que NO son el principal.

4.7. Caracteres no principales

En este apartado veremos una introducción a la siguiente sección, la cual es la última y con la cual concluiremos la demostración.

En primer lugar, cabe destacar que para cualquier carácter $\chi\neq\chi_1$, la serie $\sum_{n=1}^{\infty}\chi(n)n^{-s}$ no converge absolutamente. Aunque dicha serie si tendrá una convergencia uniforme en aquellos compactos cuya parte real de s sea mayor que cero. (Véase demostración en el apéndice 1).

En segundo lugar, $L(\chi,s)$ prolonga a una función holomorfa en el semiplano tal que la parte real s sea mayor que 0 y en particular cuando s tiende a 1^+ tenemos que $L(\chi,s)=O(1)$.

Con esto habríamos acabado en caso de que en la fórmula apareciera $L(\chi,s)$ pero en la fórmula aparece el logaritmo de esto.

Por lo tanto, lo queremos ver es que cuando s tiende a 1^+ tengamos que $\log(L(\chi,s))=O(1)$ y para ello vamos a hacer él último paso de la demostración.

Recordemos que lo que queríamos ver para acabar la demostración era que $\lim_{s\to 1^+}(P_a(s))=\infty$ para lo cual bastaría con saber que $L(\chi,s)\neq 0$ o lo que es lo mismo que sea el término principal el que se hace infinito y los demás no.

Pero esto NO es trivial.

4.8. $L(\chi,1)\neq 0$ para caracteres no principales

Vista la sección anterior, para concluir la demostración, como ya hemos dicho y como indica el nombre de esta última sección, lo único que nos queda por demostrar es que $L(\chi,1)\neq 0$ si χ es cualquier carácter de Dirichlet no principal, para lo cual vamos a usar lo que se conoce como la función zeta de Dedekind, así como la expresión del producto para esta y el teorema de Landau.

Definición 4.8.1. *La función zeta de Dedekind para el módulo m es:*

$$\zeta_m(s)=\prod_{\chi\in\widehat{\mathbb{U}}_m}L(\chi,s) \tag{4.8.1}$$

La función zeta de Dedekind es meromorfa en el semiplano tal que la parte real de s sea mayor que 0 pues cada factor lo es.

De los apartados anteriores sabemos dos cosas ya que usaremos ahora:

En primer lugar, $L(\chi, s)$ con $\chi \neq \chi_1$ es holomorfa para el semiplano donde la parte real de s es mayor que 0.

Y en segundo lugar, $L(\chi_1, s)$ tiene solo un polo simple y este está en $s = 1$.

Y por tanto, juntando estos dos, tenemos como corolario, que la zeta de Dedekind tendrá un único polo simple en $s = 1$ salvo que se cancele con algún 0 de alguna de las $L(\chi, s)$ con caracteres distintos del carácter principal, (pues la zeta de Dedekind es el producto de estas L-funciones).

Como ya hemos dicho la idea que tenemos que demostrar para acabar es que $L(\chi, s) \neq 0$ para cualquier carácter distinto del principal y esto va a ocurrir si y solo si $\zeta_m(s)$ tiene un polo en $s = 1$, por lo tanto el objetivo que vamos a seguir ahora es ver esto.

Para ello veremos como expresar esta zeta de Dedekind como producto.

Teorema 4.8.2.

$$\zeta_m(s) = \prod_{p \nmid m} \left(1 - \frac{1}{p^{f(p)s}}\right)^{-g(p)} \tag{4.8.2}$$

donde $f(p)$ es el orden de p módulo m y $g(p) = \frac{\phi(m)}{f(p)}$.

Demostración. Tomamos p un primo, tal que $p \in \mathbb{U}_m$, y por lo tanto p no será divisible por ningún m. Además llamamos G_p al grupo generado por p, es decir; $G_p = \langle [p] \rangle \subseteq \mathbb{U}_m$ y hemos definido en el enunciado $f(p)$ como el orden de p módulo m, y por lo tanto; por definición, tenemos que $f(p)$ será el mínimo n tal que $p^n \equiv 1$ mód m. De aquí deducimos por definición que $f(p) = \#G_p$ y por lo tanto tenemos que este grupo G_p es cíclico de orden $f(p)$. Y por lo tanto:

$$G_p = 1, [p], [p^2], ..., [p^{f(p)-1}] \tag{4.8.3}$$

Y por lo tanto tenemos, como hemos enunciado que $g(p) = [\mathbb{U}_m : G_p] = \frac{\phi(m)}{f(p)}$.

Ahora cogemos un carácter, distinto al principal, tal que $\chi \in \widehat{G_p}$.

Además tenemos que cada carácter va a valorar para el primo p, de modo que tenemos, $\chi \to \chi(p)$ donde $\chi(p)$ va a pertenecer al conjunto de las raíces de la unidad de orden $f(p)$, conjunto al que llamaremos $\mu_{f(p)}$. Y por lo tanto tendremos una aplicación entre dos grupos cíclicos:

$$\widehat{G_p} \to \mu_{f(p)} \tag{4.8.4}$$

Y necesitamos ver que es biyectiva, pero al ser los dos cíclicos tenemos que *inyectiva* $\leftrightarrow$ *epiyectiva* $\leftrightarrow$ *biyectiva* y por lo tanto veremos la inyectividad.

Para esto calculamos el núcleo y sabemos que este será todo carácter de $\widehat{G_p}$ tal que $\chi(p) = 1$ y como p es el generador de G_p tenemos que $\chi(p^n) = \chi(p)^n = 1$ para todo n, y por lo tanto el núcleo es el 1, y es inyectiva.

Por todo lo anterior, podemos usar la factorización y nos queda:

$$1 - T^n = \prod_{w^{f(p)}=1} (1 - wT) = \prod_{\chi \in \widehat{G_p}} (1 - \chi(p)T) \tag{4.8.5}$$

Además cada $\chi \in \widehat{G_p}$ tiene $g(p)$ extensiones a $\mathbb{U}_m$. (Véase demostración de esto en el Apéndice 2). Debido a estos obtenemos que el producto anterior, aplicado a $\mathbb{U}_m$ nos queda como $g(p)$ veces lo mismo y por lo tanto:

$$\prod_{\chi \in \widehat{\mathbb{U}_m}} (1 - \chi(p)T) = \left(1 - T^{f(p)}\right)^{g(p)} \tag{4.8.6}$$

Deshaciendo el cambio $T = \frac{1}{p^s}$ y multiplicando los productos para las L-funciones $L(\chi, s)$ queda:

$$\zeta_m(s) = \prod_{p \nmid m} \prod_{\chi \in \widehat{\mathbb{U}_m}} \left(1 - \left(\frac{\chi(p)}{p^s}\right)^{f(p)}\right)^{-1} = \prod_{p \nmid m} \left(1 - \frac{1}{p^{f(p)s}}\right)^{-g(p)} \tag{4.8.7}$$

□

Y como corolario de esto tenemos que para todo s cuya parte real sea mayor que 1:

Corolario 4.8.3. *La función zeta de Dedekind se puede expresar como una serie*

$$\zeta_m(s) = \sum_{n=1}^{\infty} f(n) n^{-s} \tag{4.8.8}$$

con $f(n) \geq 0$.

Demostración. Además lo que podemos hacer es desarrollar la parte de dentro del producto, y se quedará una suma, pues lo desarrollamos como una serie geométrica:

$$\left(1 - \frac{1}{p^{f(p)s}}\right)^{-g(p)} = \left(1 + \frac{1}{p^{f(p)s}} + \frac{1}{p^{2f(p)s}} + \frac{1}{p^{3f(p)s}} + ...\right)^{g(p)} \tag{4.8.9}$$

□

La idea es que usando esta expresión para la zeta de Dedekind, y usando lo que se conoce como el teorema de Landau podemos llegar a demostrar lo que nos queda del teorema de Dirichlet, que recordemos ; nos queda ver $s = 1$ es un polo para dicha zeta.

Teorema 4.8.4 (Teorema de Landau)**.** *Si* $\sum_{n=1}^{\infty} f(n) n^{-s}$ *con* $f(n) \neq 0$ *converge para* $\operatorname{Re} s > \sigma_0$ *y la función suma prolonga al punto* $s = \sigma_0$*, entonces para algún* $\epsilon > 0$*, la serie converge para* $\operatorname{Re} s > \sigma_0 - \epsilon$.

La demostración de este teorema es muy extensa, debido a que necesitamos varios teoremas y lemas previos, por lo que la dejaremos para el apéndice 3.

Y continuaremos viendo el teorema de Landau pero aplicado a la zeta de Dedekind.

Es obvio que la serie $\zeta_m(s)$ converge para todo s cuya parte real es mayor que 1 y queremos ver que tiene un polo en $s = 1$, para lo cual vamos a actuar por reducción al absurdo suponiendo lo contrario, por lo tanto; suponemos que $\zeta_m(s)$ no tiene un polo en $s = 1$.

Y suponiendo esto por el teorema de Landau tendríamos que la serie convergería en $\operatorname{Re} s > 1 - \epsilon$ y $\zeta_m(s)$ sería holomorfa para parte real de s mayor que 0. En efecto si la serie converge para parte real de s mayor que un sigma tal que $0 < \sigma < 1$ entonces por

el Teorema de Landau, converge para $\operatorname{Re} s > \sigma - \epsilon$ con $\epsilon > 0$ suficientemente pequeño y entonces como conclusión sería que la serie convergería para parte real de $s > 0$.

Pero vamos a ver que la serie $\zeta_m(s)$ no converge para $\sigma = \operatorname{Re} s > 0$ tomando la igualdad conseguida como corolario de la expresión de Dedekind:

$$\begin{aligned}\left(1 - \frac{1}{p^{f(p)\sigma}}\right)^{-g(p)} &= \left(1 + \frac{1}{p^{f(p)\sigma}} + \frac{1}{p^{2f(p)\sigma}} + \frac{1}{p^{3f(p)\sigma}} + ...\right)^{g(p)} \\ &\geq 1 + \frac{1}{p^{f(p)g(p)\sigma}} + \frac{1}{p^{2f(p)g(p)\sigma}} + \frac{1}{p^{3f(p)g(p)\sigma}} + ... \\ = 1 + \frac{1}{p^{\phi(m)\sigma}} + \frac{1}{p^{2\phi(m)\sigma}} + \frac{1}{p^{3\phi(m)\sigma}} + ... &= \left(1 - \frac{1}{p^{\phi(m)\sigma}}\right)^{-1} \end{aligned} \tag{4.8.10}$$

Y por lo tanto tenemos:

$$\zeta_m(\sigma) \geq \prod_{p \nmid m} \left(1 - \frac{1}{p^{\phi(m)\sigma}}\right)^{-1} = \sum_{mcd(n,m)=1} \frac{1}{n^{\phi(m)\sigma}} \tag{4.8.11}$$

Pero si evaluamos para $\sigma = \frac{1}{\phi(m)}$ resulta una serie divergente, pues tenemos:

$$\sum_{mcd(n,m)=1} \frac{1}{n} \geq \sum_{n \equiv 1 \text{ mód } m} \frac{1}{n} = \sum_{k=1}^{\infty} \frac{1}{mk+1} = \infty \tag{4.8.12}$$

Por lo tanto llegamos a una contradicción y de aquí resulta que $s = 1$ es un polo de la zeta de Dedekind, que es lo que buscabamos.

Por tanto, a partir de esto ya sabemos que $L(\chi, s) \neq 0$ para $\chi \neq \chi_1$ y volviendo a la relación fundamental:

$$P_a(s) = \sum_{p \equiv a \text{ mód } m} \frac{1}{p^s} = \frac{1}{\phi(m)} \sum_{\chi \in \widehat{\mathbb{U}_m}} \overline{\chi(a)} \log L(\chi, s) + O(1) \tag{4.8.13}$$

se obtiene que cuando tomamos el límite cuando $s \to 1^+$ de $P_a(s)$ es infinito, pues en 1 tenemos que se hace infinito cuando $\chi = \chi_1$ y para el resto son distintos de 0.

Finalmente, sabemos que queríamos demostrar esto para acabar el Teorema de Dirichlet y por lo tanto con esto hemos demostrado que:

$$\sum_{p \equiv a \text{ mód } m} \frac{1}{p} = \infty \tag{4.8.14}$$

luego hay infinitos primos en una progresión aritmética, y con esto acabamos la demostración del Teorema de Dirichlet.

Apéndice A

Apéndices

A.1. Apéndice 1

En el apartado de caracteres no principales, dijimos que la serie $\sum_{n=1}^{\infty} \chi(n)n^{-s}$ no converge absolutamente, pero si uniformemente, y dejamos la demostración de esto para este apéndice.

En primer lugar, tenemos que ver la demostración de la versión de convergencia uniforme del Criterio de Dirichlet para series de funciones, para lo cual veremos antes un lema, que será el de la suma por partes de Abel, para la cual nos basaremos en la proposición 9.39 de los apuntes de Fernando Chamizo sobre series numéricas [4].

Lema A.1.1 (Suma por partes)**.** *Dadas dos sucesiones a_n y b_n y definimos que $A_p = \sum_{j=1}^{p} a_j$. Tenemos entonces que:*

$$\sum_{k=1}^{n} a_k b_k = \sum_{k=1}^{n} A_k(b_k - b_{k+1}) + A_n b_{n+1} \tag{A.1.1}$$

Demostración. Por facilidad suponemos que $A_0 = 0$ y por lo tanto, para todo $k \in \mathbb{N}$ se verifica $a_k = A_k - A_{k-1}$ y se verifica:

$$\begin{aligned}\sum_{k=1}^{n} a_k b_k = \sum_{k=1}^{n} (A_k - A_{k-1})b_k &= \sum_{k=1}^{n} A_k b_k - \sum_{k=2}^{n} A_{k-1} b_k \\ &= \sum_{k=1}^{n} A_k b_k - \sum_{k=1}^{n} A_k b_{k+1} + A_n b_{n+1} \\ &= \sum_{k=1}^{n} A_k(b_k - b_{k+1}) + A_n b_{n+1} \end{aligned} \tag{A.1.2}$$

con lo que concluimos este lema. □

Y ahora visto este lema, veamos la versión uniforme del Criterio de Dirichlet para series de funciones, para lo cual vamos a ver la proposición 10.13 de los apuntes de Fernando, [5] sobre sucesiones y series de funciones.

Teorema A.1.2. *Sea a_n una sucesión numérica y $\sum_{n\geq 1} f_n$ una serie de funciones definidas en un conjunto A. Supongamos que:*

1. *a_n es una sucesión de números reales monótona y convergente a 0*

2. *La serie $\sum_{n\geq 1} f_n$ tiene sumas parciales uniformemente acotadas en A, es decir, hay un número $M > 0$ tal que para todo $x \in A$ y para todo $n \in \mathbb{N}$ se verifica que $|\sum_{k=1}^{\infty} f_k(x)| \leq M$.*

Entonces la serie de funciones $\sum_{n\geq 1} a_n f_n$ converge uniformemente en A.

Demostración. Supongamos que $F_n = \sum_{k=1}^{n} f_k$. De la fórmula del lema anterior sobre la suma por partes de Abel se deduce que:

$$\sum_{k=1}^{p} a_{n+k} f_{n+k}(x) = \sum_{k=1}^{p} F_{n+k}(x)(a_{n+k} - a_{n+k+1}) + F_{n+p}(x)a_{n+p+1} - F_n(x)a_{n+1} \tag{A.1.3}$$

Igualdad que se cumple para todo n mayor o igual que 1 y menor que p y para todo $x \in A$. Si tomamos valores absolutos en la igualdad anterior, teniendo en cuenta que para todo $n \in \mathbb{N}$ se cumple $|F_n(x)| \leq M$ y suponemos que a_n es decreciente en cuyo caso será $a_n > 0$, obtenemos:

$$\begin{aligned} |\sum_{k=1}^{p} a_{n+k} f_{n+k}(x)| &\leq M \sum_{k=1}^{\infty} (a_{n+k} - a_{n+k+1}) + Ma_{n+p+1} - Ma_{n+1} \\ &= M(a_{n+1} - a_{n+p+1}) + Ma_{n+p+1} - Ma_{n+1} = 2Ma_{n+1} \end{aligned} \tag{A.1.4}$$

Tomemos ahora un $\epsilon > 0$, como suponemos que $a_n \to 0$, hay un n_0 tal que para todo $n \geq n_0$ se verifica que $a_n \leq \frac{\epsilon}{2M}$ y por lo tanto deducimos que para todo n entre p y n_0, ambos incluidos; y para todo $x \in A$ se verifica que:

$$|\sum_{k=1}^{p} a_k f_k(x) - \sum_{k=1}^{n} a_k f_k(x)| = |\sum_{k=1}^{p} a_{n+k} f_{n+k}(x)| \leq 2Ma_{n+1} \leq \epsilon \tag{A.1.5}$$

Así queda demostrado $\sum_{n\geq 1} a_n f_n$ verifica la condición de Cauchy para la convergencia uniforme en A. □

Lo que tenemos que demostrar ahora es lo que hemos supuesto en el enunciado, recordando que nuestro ejemplo es $\sum_{n=1}^{\infty} \chi(n)n^{-s}$. Por lo tanto, nuestro a_n será $\sum_{n=1}^{\infty} \frac{1}{n^s}$ y la f_n serían los caracteres.

En primer lugar, la a_n, es decir, $\sum_{n=1}^{\infty} \frac{1}{n^s}$ para $s > 0$, que es el caso en el que estamos, y sabemos que es monótona, pues es decreciente y cuando n tiende a infinito converge a 0.

En segundo lugar tenemos que ver que $\sum_{n=1}^{\infty} \chi(n)$ tiene sumas parciales uniformemente acotada o lo que es lo mismo que existirá una constante M tal que $|\sum_{n=1}^{N} \chi(n)| \leq M$ para todo N, y por lo tanto con demostrar esto acabaríamos la demostración de este apéndice.

Para ver esto vamos a usar algo lo cual ya hemos visto, y además de que sabemos que estamos con caracteres distintos al principal. La ortogonalidad de los caracteres implica que si χ no es principal, entonces

$$0 = \langle \chi, \chi_1 \rangle = \frac{1}{\phi(m)} \sum_{a} \chi(a)\overline{\chi_1(a)} = \frac{1}{\phi(m)} \sum_{a=0}^{m-1} \chi(a)$$

pues por definición $\chi_1(a) = 0$ si $(a, m) \neq 1$ y 1 si $(a, m) = 1$.

De aquí deducimos que, excepto para el carácter principal, el cual no esta incluido en este caso en nuestro estudio, para la suma parcial hasta N, si escribimos $N = mq + r$ con resto $0 \leq r < m$, tenemos por la periodicidad que vimos antes $\chi(n) = \chi(n + m)$, que la suma es

$$\sum_{n=0}^{N} \chi(n) = \sum_{n=0}^{m-1} \chi(n) + \sum_{n=m}^{2m-1} \chi(n) + \cdots + \sum_{n=(q-1)m}^{qm-1} \chi(n) + \sum_{n=qm}^{qm+r} \chi(n)$$

y en cada bloque de longitud m la suma es nula por periodicidad y la última es la suma parcial hasta el resto r

$$\sum_{n=0}^{N} \chi(n) = 0 + 0 + \cdots + 0 + \sum_{n=0}^{r} \chi(n)$$

Entonces las sumas parciales van repitiendo el número finito de valores de las sumas parciales hasta $m - 1$. Como es un conjunto finito de números, está acotado.

A.2. Apéndice 2

Durante la demostración de la expresión de la zeta de Dedekind en la ultima sección del capítulo cuatro de dicho TFG, hicimos referencia a que cada carácter $\chi \in \widehat{G_p}$ tiene $g(p)$ extensiones a $\mathbb{U}_m$.

Para demostrar esto nos basta ver el lema 3.2 y los teoremas 3.3 y 3.4 de los apuntes *Characters of Finite Abelian Groups* del autor Keith Conrad [6].

Lema A.2.1. *Sea G un grupo abeliano finito, H un subgrupo de este y definamos $\chi : H \to S^1$ un carácter de H. Para cada $g \in G - H$, hay una extensión de χ a un carácter de $\langle H, g\rangle$.*

Demostración. Lo que queremos hacer es extender un carácter χ a otro $\widehat{\chi}$ de $\langle H, g\rangle$.

En primer lugar, tenemos que para un g no pertenciente a H, $\widehat{\chi}(g)$ no esta inicialmente definido pero alguna potencia no nula de g esta en H, y en esta potencias el carácter χ si que esta definido. Tomamos un $d \geq 1$ con $g^d \in H$, es decir, d va a ser el orden de g en G/H, asi $d = [\langle H, g\rangle : H]$.

Si hay un carácter $\widehat{\chi}$ en $\langle H, g\rangle$ que extiende a χ en H entonces $\widehat{\chi}(g)$ debe ser una raíz d-esima de $\chi(g^d)$ entonces debemos tener que $\widehat{\chi}(g)^d = \widehat{\chi}(g^d) = \chi(g^d)$ y esta es nuestra clave: definir $\widehat{\chi}(g) \in S^1$ para que sea una solución para $z^d = \chi(g^d)$, y por lo tanto:

$$\widehat{\chi}(g)^d = \chi(g^d) \tag{A.2.1}$$

Una vez que eligimos $\widehat{\chi}(g)$ para que satisfaga la igualdad anterior, definimos $\widehat{\chi}$ en $\langle H, g\rangle$ como:

$$\widehat{\chi}(hg^i) := \chi(h)\widehat{\chi}(g)^i \tag{A.2.2}$$

Esta fórmula contiene a todos los posibles elementos de $\langle H, g\rangle$, pero ahora tendríamos que ver que este carácter $\widehat{\chi}$ esta bien definido.

Quizás H y $\langle g\rangle$ se superpongan de manera no trivial, así la expresión de un elemento de $\langle H, g\rangle$ en la forma hg^i no es única. Y lo que tenemos que demostrar es que esto no lleva a ninguna contradicción en el valor de $\widehat{\chi}$ en la última igualdad.

Para ello, vamos a suponer que $hg^i = h'g^{i'}$ y por lo tanto $g^{i-i'} \in H$, lo que implica $i' \equiv i$ mód d entonces d es el orden de g en G/H.

Escribimos $i' = i + dd'$, así $h = h'a^{i'-i} = h'g^{dd'}$ y los términos h,h' y g^d están en H, asique:

$$\chi(h')\widehat{\chi}(g)^{i'} = \chi(h')\widehat{\chi}(g)\widehat{\chi}(g)^{dd'} = \chi(h')\widehat{\chi}(g)\widehat{\chi}(g^d)^{d'} \tag{A.2.3}$$

y como sabemos de antes que $\widehat{\chi}(g)^d = \chi(g^d)$ se queda:

$$= \chi(h'g^{dd'})\widehat{\chi}(g)^i = \chi(h)\widehat{\chi}(g)^i \tag{A.2.4}$$

Por lo tanto; $\widehat{\chi} : \langle H, g\rangle \to S^1$ esta bien definida como función y es fácil comprobar que es un homomorfismo. □

Visto este lema, vamos a ver el teorema 3.3 de los apuntes antes mencionados donde veremos que cada carécter de un subgrupo puede extenderse al grupo original si este es finito y abeliano.

Teorema A.2.2. *Para un grupo finito y abeliano G y un subgrupo H, cada carácter de H puede ser extendido a un carácter de G.*

Demostración. Sea $\chi : H \to S^1$ un carácter de H.

Como sabemos que por definición G es finito, este tiene un conjunto generador finito, $g_1, ..., g_k$. Así podemos construir una torre de subgrupos de H a G añadiendo los elementos generadores uno a uno, de modo que:

$$H \subset \langle H, g_1\rangle \subset \langle H, g_1, g_2\rangle \subset ... \subset \langle H, g_1, ..., g_k\rangle = G \tag{A.2.5}$$

Cada paso de esta torre tiene la forma $H_i \subset \langle H_i, g_i\rangle$ donde $H_0 = H$ y aplicando el lema anterior en cada paso de esta torre, χ puede ser extendido de H a H_1 a H_2 y así hasta que lleguemos a $H_k = G$, con lo que concluímos. □

Una vez visto que efectivamente, podemos extender estos caracteres vamos a ver lo que queríamos demostrar en este apéndice, y es que el número de extensiones de estos caracteres existentes, para lo cual veremos el teorema 3.4 de los apuntes ya dichos.

Teorema A.2.3. *Para un grupo finito abeliano G y un subgrupo H, cada carácter de H puede ser extendido a un carácter de G en $[G : H]$ maneras.*

Demostración. Vamos a hacer inducción sobre el índice $[G : H]$.

En primer lugar, cuando $[G : H] = 1$ tenemos que $H = G$, por lo tanto supondremos que $[G : H] > 1$ y el teorema será cierto para los caracteres en subgrupos de indice menor que $[G : H]$.

Tomemos ahora $g \in G$ pero no contenido en H, así tenemos:

$$H \subset \langle H, g\rangle \subset G \tag{A.2.6}$$

Para extender un carácter $\chi : H \to S^1$ a G necesitamos por lo menos poder extender χ a un carácter $\widehat{\chi}$ en $\langle H, g\rangle$, cosa que ya sabemos que se puede.

El siguiente paso sería contar el número de maneras para hacer esto, que es lo queremos saber y que haremos por inducción.

Tomamos d el positivo mas pequeño tal que $g^d \in H$. Una extensión de χ en H a un carácter $\widehat{\chi}$ en $\langle H, g\rangle$ esta determinado por $\widehat{\chi}(g)$, y este valor tiene que cumplir la condición $\widehat{\chi}(g)^d = \chi(g^d)$.

Cada número en S^1 tiene d diferentes raíces d-esimas en S^1, así hay d valores potenciales para $\widehat{\chi}(g)$, y por el lema visto en esta sección sabemos que todos ellos son válidos.

El número de opciones de extender χ a $\widehat{\chi}$ coincide el número de opciones para $\widehat{\chi}(g)$, el cual es $d = [\langle H, g\rangle : H]$.

Entonces tenemos que $[G : \langle H, g\rangle] < [G : H]$, y por inducción sobre el índice hay $[G : \langle H, g\rangle]$ extensiones para cada $\widehat{\chi}$ a un carácter de G, por lo tanto el número de extensiones de un carácter de H a un carácter de G es $[G : \langle H, g\rangle][\langle H, g\rangle : H] = [G : H]$, con lo que concluimos la demostración de este teorema y con ello el segundo apéndice. □

A.3. Apéndice 3

Dentro de la última sección del capítulo de la demostración del teorema vimos un teorema, el Teorema de Landau, el cual usamos posteriormente para acabar la demostración del teorema de Dirichlet.

La demostración de este teorema la dejamos para verla en un apéndice, pues teníamos que demostrar varios teoremas y lemas previos, y podríamos salirnos del tema principal del TFG.

En primer lugar veremos la identidad de Abel (aunque ya la vimos en el apéndice 1, la volveremos a ver pues es otra versión), la cual llamaremos teorema 3.1, al ser el primer teorema del apéndice 3, y la notación será similar para el resto.

Basándonos en el teorema 4.2 de Apostol [2] tenemos:

Teorema A.3.1. *Para una función aritmética $a(n)$*

$$A(x) = \sum_{n \leq x} a(n) \tag{A.3.1}$$

donde $A(x) = 0$ si $x < 1$ y suponiendo que f tiene una derivada continua en el intervalo $[y, x]$, donde $0 < y < x$. Entonces tenemos:

$$\sum_{y < n \leq x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_x^y A(t)f'(t)\,dt \tag{A.3.2}$$

Demostración. Sea $k = [x]$ y $m = [y]$, tal que $A(x) = A(k)$ y $A(y) = A(m)$. Entonces tenemos:

$$\sum_{y < n \leq x} a(n)f(n) = \sum_{n=m+1}^{k} a(n)f(n) = \sum_{n=m+1}^{k} \{A(n) - A(n-1)\} f(n)$$

$$= \sum_{n=m+1}^{k} A(n)f(n) - \sum_{n=m}^{k-1} A(n)f(n+1)$$

$$= \sum_{n=m+1}^{k-1} A(n)\{f(n) - f(n+1)\} + A(k)f(k) - A(m)f(m+1)$$

$$= -\sum_{n=m+1}^{k-1} A(n)\int_{n}^{n+1} f'(t)\,dt + A(k)f(k) - A(m)f(m+1)$$

$$= -\sum_{n=m+1}^{k-1} \int_{n}^{n+1} A(t)f'(t)\,dt + A(k)f(k) - A(m)f(m+1)$$

$$= -\int_{m+1}^{k} A(t)f'(t)\,dt + A(x)f(x) - \int_{k}^{x} A(t)f'(t)\,dt - A(y)f(y) - \int_{y}^{m+1} A(t)f'(t)\,dt$$

$$= A(x)f(x) - A(y)f(y) - \int_{x}^{y} A(t)f'(t)\,dt \tag{A.3.3}$$

□

Con esto quedaría demostrada esta identidad de Abel, lo cual usaremos para demostrar el primer lema, el cual seguiremos por el lema 2 del tema 11 del Libro de Apostol [2], el cual dice:

Lema A.3.2. *Sea $s_0 = \sigma_0 + it_0$ y asumimos que la serie de Dirichlet $\sum f(n)n^{-s_0}$ tiene sumas parciales acotadas, es decir:*

$$|\sum_{n\leq x} f(n)n^{-s_0}| \leq M \tag{A.3.4}$$

para todo $x \geq 1$. Entonces para cada s con $\sigma > \sigma_0$ nosotros tenemos:

$$|\sum_{a<n\leq b} f(n)n^{-s}| \leq 2Ma^{\sigma_0-\sigma}\left(1 + \frac{|s-s_0|}{\sigma-\sigma_0}\right) \tag{A.3.5}$$

Demostración. Veamos la demostración de este teorema siguiendo la demostración de Apostol.

Sea $a(n) = f(n)n^{-s_0}$ y tomamos $A(x) = \sum_{n\leq x} a(n)$. Entonces tenemos $= f(n)n^{-s} = a(n)n^{s_0-s}$ y podemos aplicar la identidad de Abel, que es el teorema visto anteriormente y así obtenemos:

$$\sum_{a<n\leq b} f(n)n^{-s} = A(a)a^{s_0-s} + (s-s_0)\int_{a}^{b} A(t)t^{s_0-s-1}dt \tag{A.3.6}$$

Entonces $|A(x)| \leq M$ y con esto obtenemos:

$$|\sum_{a<n\leq b} f(n)n^{-s}| \leq Mb^{\sigma_0-\sigma} + Ma^{\sigma_0-\sigma} + |s-s_0|M\int_{a}^{b} t^{\sigma_0-\sigma-1}dt$$

$$\leq 2Ma^{\sigma_0-\sigma} + |s-s_0|M|\frac{b^{\sigma_0-\sigma}-a^{\sigma_0-\sigma}}{\sigma_0-\sigma}|$$

$$\leq 2Ma^{\sigma_0-\sigma}\left(1+\frac{|s-s_0|}{\sigma-\sigma_0}\right) \tag{A.3.7}$$

y con esto queda demostrado. □

Pasemos a ver el siguiente teorema, en cuya demostración utilizaremos el lema que acabamos de demostrar. Para ver este teorema vamos a seguir el teorema 11,11 del Ápostol [2].

Teorema A.3.3. *Una serie de Dirichlet $\sum f(n)n^{-s}$ converge uniformemente en todo subconjunto compacto que se encuentra en el interior para el semiplano de convergencia $\sigma > \sigma_c$.*

Demostración. Nos va a ser suficiente con demostrar que $\sum f(n)n^{-s}$ converge uniformemente en todo rectángulo compacto $R = [\alpha, \beta]x[c, d]$ con $\alpha > \sigma_c$ y para esto usaremos lo demostrado en el lema anterior:

$$|\sum_{a<n\leq b} f(n)n^{-s}| \leq 2Ma^{\sigma_0-\sigma}\left(1+\frac{|s-s_0|}{\sigma-\sigma_0}\right) \tag{A.3.8}$$

donde $s_0 = \sigma_0 + it_0$ es algún punto en el semiplano $\sigma > \sigma_c$ y s es un punto con $\sigma > \sigma_0$ y vamos a elegir $s_0 = \sigma_0$ donde $\sigma_c < \sigma_0 < \alpha$.

Entonces si $s \in R$ tenemos $\sigma - \sigma_0 \geq \alpha - \sigma_0$ y $|s_0 - s| < C$, donde definimos C como una constante dependiendo en s_0 y R pero no de s, entonces usando el lema anterior tenemos:

$$|\sum_{a<n\leq b} f(n)n^{-s}| \leq 2Ma^{\sigma_0-\alpha}\left(1+\frac{C}{\sigma-\sigma_0}\right) = Ba^{\sigma_0-\alpha} \tag{A.3.9}$$

donde B es independiente de s. Entonces cuando hacemos tender la a a infinito $a^{\sigma_0-\alpha} \to 0$ y la condición de Cauchy para la convergencia uniforme es satisfecha con lo cual acabamos. □

Recordamos el teorema de Weierstrass que es un resultado básico de Análisis Complejo. Suponemos conocidas las definiciones de función analítica compleja y la convergencia uniforme en compactos.

Teorema A.3.4 (Teorema de Weierstrass)**.** *Tomemos f_n una sucesión de funciones analíticas en un subconjunto abierto del plano complejo, S y asumimos que f_n converge uniformemente para todo subconjunto compacto de S a una función límite f. Entonces f es analítica en S y la sucesión de las derivadas f_n' converge uniformemente en todo subconjunto compacto de S a la derivada de f.*

Vamos a demostrar otro teorema que se va a basar en el teorema 11.12 de Apostol, [2].

Teorema A.3.5. *La función suma $F(s) = \sum f(n)n^{-s}$ de una serie de Dirichlet es analítica en el semiplano de convergencia con $\sigma > \sigma_c$ y su derivada esta representada en el semiplano por la serie de Dirichlet siguiente:*

$$F'(s) = -\sum_{n=1}^{\infty} \frac{f(n)\log n}{n^s} \tag{A.3.10}$$

la cual se obtiene derivando término a término.

Demostración. La demostración de este teorema no es más que la aplicación del los teoremas anteriores a la serie de Dirichlet. □

Una vez vista esta serie de teoremas, lemas y definiciones, por último podemos ver el teorema cuya demostración era el objetivo de este apéndice, que es el teorema de Landau.

Teorema A.3.6. *Sea $F(s)$ una función representada en el semiplano con $\sigma > c$ por la serie de Dirichlet:*

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^{-s}} \tag{A.3.11}$$

donde c es finito, $f(n) \geq 0$ para todo $n \geq n_0$. Si $F(s)$ es analítica en un disco sobre el punto $s = c$, entonces la serie de Dirichlet converge en el semiplano $\sigma > c - \epsilon$ para algún $\epsilon > 0$ y por lo tanto; si la serie de Dirichlet tiene una abscisa finita de convergencia σ_c, entonces $F(s)$ tiene una singularidad en el eje real en el punto $s = \sigma_c$.

Demostración. Sea $a = 1 + c$. Entonces si F es analítica en a se puede representar por una expansión de la serie de potencias absolutamente convergente sobre a, tal que:

$$F(s) = \sum_{k=0}^{\infty} \frac{F^{(k)}(a)}{k!}(s-a)^k \tag{A.3.12}$$

y el radio de convergencia de esta serie de potencias es superior a 1 ya que F es analítica en c. Usando ahora el teorema anterior, el teorema 3.3 de este apéndice, podemos calcular la derivada k-esima de F en a haciendo la diferenciación repetida de la definición de $F(s)$ del enunciado, de modo que obtenemos:

$$F^{(k)}(a) = (-1)^k \sum_{n=1}^{\infty} f(n)(\log n)^k n^{-a} \tag{A.3.13}$$

y juntando las dos últimas fórmulas tenemos:

$$F(s) = \sum_{k=0}^{\infty}\sum_{n=1}^{\infty} \frac{(a-s)^k}{k!} f(n)(\log n)^k n^{-a} \tag{A.3.14}$$

Y entonces el radio de convergencia supera 1 y esta fórmula es válida para algún valor real $s = c - \epsilon$ donde $\epsilon > 0$. Entonces $a - s = 1 + \epsilon$ para ese valor de s y el doble sumatorio en la última fórmula tiene términos no negativos para $n \geq n_0$. Y podemos intercambiar el orden de los sumatorios obtenemos:

$$F(c-\epsilon) = \sum_{n=1}^{\infty} \frac{f(n)}{n^a} \sum_{k=0}^{\infty} \frac{(1+\epsilon)\log n^k}{k!} = \sum_{n=1}^{\infty} \frac{f(n)}{n^a} e^{(1+\epsilon)\log n} = \sum_{n=1}^{\infty} \frac{f(n)}{n^{c-\epsilon}} \tag{A.3.15}$$

En otras palabras, la serie de Dirichlet $\sum f(n)n^{-s}$ converge para $s = c - \epsilon$, y por lo tanto converge en el semiplano $\sigma > c - \epsilon$. □

Con esto queda demostrado el Teorema de Landau, y con ello acabamos este tercer apéndice.

Bibliografía

[1] Alaca, S. y William, K.S., Introdutory Algebraic Number Theory, Cambrige University Press (2004)

[2] Apostol, T.M., Introduction to Analytic Number Theory, Springer Verlag (1976)

[3] Castillo, C.I., Teoría Analítica de Números, http://www.uv.es/~ivorra/Libros/TAn.pdf

[4] Chamizo, F., Series Numéricas, http://matematicas.uam.es/~fernando.chamizo/asignaturas/calc1inf1011/apjperez/calculo_cap09.pdf

[5] Chamizo, F., Sucesiones y Series de Funciones, http://matematicas.uam.es/~fernando.chamizo/asignaturas/calc1inf1011/apjperez/calculo_cap10.pdf

[6] Conrad, K., Character Of Finite Abelian Group, https://kconrad.math.uconn.edu/blurbs/grouptheory/charthy.pdf

[7] Machío R.P., Funciones Especiales y Caracteres de Dirichlet, http://hojamat.es/parra/funesp.pdf

[8] Varona, J.L., Recorridos por la teoría de números, E-lecto Libris, segunda edición (2019)