Dos Pruebas Elementales del Teorema de Dirichlet en la Tonalidad Polinomia

Harold Gamero Rodríguez

Universidad Nacional de Colombia
Facultad de Ciencias, Departamento de Matemáticas
Bogotá, Colombia

2013

Dos Pruebas Elementales del Teorema de Dirichlet en la Tonalidad Polinomia

Harold Gamero Rodríguez

Trabajo de investigación presentado como requisito parcial para optar al título de Magister en Ciencias Matemáticas

Director:
(Doctor, Matemático) Víctor Samuel Albis González

Linea de Investigación:
Álgebra

Universidad Nacional de Colombia
Facultad de Ciencias, Departamento de Matemáticas
Bogotá, Colombia

2013

Resumen

TDP, dado un cuerpo finito $\mathbb{F}_q$ y polinomios $a, m \in \mathbb{F}_q[t]$ con $(a, m) = 1$, $m \neq 0$, se tiene

$$\sum_{\substack{\pi \equiv a \text{ mód } m \\ \deg \pi \leqslant n}} \frac{\log |\pi|}{|\pi|} = \frac{1}{\varphi(m)} \log q^n + O(1), \text{ para } n \geqslant 0.$$

En otras palabras, TDK, para las mismas condiciones, existe una cantidad infinita de polinomios $\pi \in P(q; T)$, el conjunto de polinomios irreducibles unitarios, tales que $\pi \equiv a$ mód m.

Palabras claves: Teorema de Dirichlet en $\mathbb{F}_q[t]$ según Pollack (TDP); Teorema de Dirichlet en $\mathbb{F}_q[t]$ según Kornblum (TDK).

Abstract

TDP, given a finite field $\mathbb{F}_q$ and polynomials $a, m \in \mathbb{F}_q[t]$ with $(a, m) = 1$, $m \neq 0$, we have the equation

$$\sum_{\substack{\pi \equiv a \text{ mód } m \\ \deg \pi \leqslant n}} \frac{\log |\pi|}{|\pi|} = \frac{1}{\varphi(m)} \log q^n + O(1), \text{ para } n \geqslant 0.$$

In other words, TDK, under these conditions, there is an infinite number of polynomials $\pi \in P(q; T)$, the set of unitary irreductible polynomials, such that $\pi \equiv a$ mód m.

Keywords: Dirichlet's Theorem in $\mathbb{F}_q[t]$ according Pollack (TDP); Dirichlet's Theorem in $\mathbb{F}_q[t]$ according Kornblum (TDK).

Agradecimientos

Quiero expresar mis humildes agradecimientos a Dios por escucharme y darme el valor y la persistencia para seguir adelante en la difícil carrera como son las matemáticas. Gracias a Él he podido finalizar este trabajo.

Igualmente, expresar mis sinceros agradecimientos al Profesor Víctor Albis por la gran dedicación e interés con que ha dirigido este trabajo y, desde luego, por las enseñanzas y formación que he recibido de su parte durante todo este tiempo.

Agradezco enormemente a la Universidad Nacional de Colombia la por brindarme la gran oportunidad de realizar mis estudios de Maestría en Matemáticas; a su departamento de matemáticas por poner a mi disposición los recursos y la infraestructura necesaria para la realización de éste trabajo.

Finalmente, quiero dar las gracias de manera especial a mí familia y a mí esposa por su esfuerzo y apoyo incondicional durante el tiempo que dediqué a los estudios de Maestría.

Contenido.

Introducción

La progresión aritmética de números impares $1, 3, 5, \cdots, 2k+1, \cdots$, contiene infinitos números primos. Es natural preguntar si otras progresiones aritméticas tienen esta propiedad. Una progresión aritmética con el primer término a y diferencia común m consiste de todos los números de la forma

$$a + mk, \quad k = 0, 1, 2, \cdots . \tag{1}$$

Si a y m tienen un factor común d, cada término de la progresión es divisible por d y no puede haber más de un primo en la progresión si $d > 1$. En otras palabras, una condición necesaria para la existencia de infinitos números primos en la progresión aritmética (1) es que $(a, m) = 1$. *Dirichlet* fue el primero en probar que esta condición es también suficiente. Esto es, si $m > 0$ y a son enteros con $(a, m) = 1$, entonces hay un número infinito de primos p en la progresión aritmética (1), es decir, un número infinito de primos p con $p \equiv a \pmod{m}$. Este resultado es conocido como el teorema de *Dirichlet*.
De hecho, *Dirichlet* estableció mucho más:

$$\lim_{s \downarrow 1} \left(\sum_{p \equiv a \pmod{m}} \frac{p^{-s}}{\log\left(\frac{1}{s-1}\right)} \right) = \frac{1}{\varphi(m)}.$$

Ya que $\log\left(\frac{1}{s-1}\right) = \log \xi(s) + O(1) = \sum_p p^{-s} + O(1)$ cuando $s \downarrow 1$, esto muestra que en cierto sentido, los primos se distribuyen por igual en las progresiones.
Recordemos que *Euler* probó la existencia de infinitos números primos mostrando que la serie $\sum_p p^{-1}$, extendida sobre todos los primos, diverge.
La idea de *Dirichlet* era probar una afirmación correspondiente cuando los primos están limitados a estar en la progresión dada en (1). En una memoria famosa [8], publicada en 1837, realizó esta idea por ingeniosos métodos analíticos. Desafortunadamente, esta prueba no puede ser considerada enteramente elemental, pues, para ello utiliza el desarrollo de *Taylor* del logaritmo complejo alrededor de $s = 1$. Además, la prueba de *Dirichlet* de la no anulación de ciertas sumas infinitas (las *series L* correspondientes a los caracteres no principales reales) en $s = 1$, depende de investigaciones difíciles en la teoría de formas cuadráticas binarias. Sin embargo, la prueba fue más tarde simplificada por varios autores. En 1950, *H. N. Shapiro* publicó una prueba elemental del teorema de *Dirichlet* [7]. Esta es elemental, ya que evita el uso del logaritmo complejo y otras herramientas de la teoría de funciones, que establecen la no anulación de las *funciones L* en $s = 1$, y con pocas excepciones sólo usa sumas finitas.
La prueba de *Shapiro* realmente obtiene una estimación para $\sum_p \frac{\log p}{p}$ cuando $(a, m) = 1$, $m > 0$:

$$\sum_{\substack{p \equiv a \pmod{m} \\ p \leqslant x}} \frac{\log p}{p} = \frac{1}{\varphi(m)} \log x + O(1).$$

Nuestro propósito es mostrar el análogo del teorema de *Dirichlet* en el caso de un anillo de polinomios sobre $\mathbb{F}_q$, donde $\mathbb{F}_q$ denota a un cuerpo finito con q elementos y de característica p, con $q = p^k$ donde p es

un entero primo y $k \geqslant 1$. Es decir, que dado un cuerpo finito $\mathbb{F}_q$ y polinomios $a, m \in \mathbb{F}_q[t]$ con $(a, m) = 1$, $m \neq 0$, se tiene que la serie

$$\sum_{\substack{p \in P(q;t) \\ p \equiv a \text{ mód } m}} \frac{\log |p|}{|p|}$$

es divergente, donde $|p|$ es lo que llamaremos, luego, la norma del polinomio p. El primero en realizar dicha prueba fue *Heinrich Kornblum* [5] en 1919. La estructura de esta demostración es en gran parte la misma como en el caso clásico.
También, se mostrará que la prueba de *Shapiro* y su estimación pueden ser adaptadas para el caso de $\mathbb{F}_q[t]$. Esta prueba fue hecha por *Paul Pollack* [2]. Es decir, probar que dado un cuerpo finito $\mathbb{F}_q$ y polinomios $a, m \in \mathbb{F}_q[t]$ con $(a, m) = 1$, $m \neq 0$, se tiene

$$\sum_{\substack{\pi \equiv a \text{ mód } m \\ deg \pi \leqslant n}} \frac{\log |\pi|}{|\pi|} = \frac{1}{\varphi(m)} \log(q^n) + O(1), \text{ para } n \geqslant 0.$$

Para cumplir con los objetivos de este trabajo, se estudiaron las funciones aritméticas definidas sobre el monoide $M(q;t)$. En particular, los análogos en $M(q;t)$ de la función de *von Mangoldt* y de la función de *Möbius* conocidos en $\mathbb{Z}$. Se Emplearon las propiedades de los caracteres de grupos abelianos finitos (caracteres de *Dirichlet* módulo $m(t)$) y sus relaciones de ortogonalidad en el estudio de las funciones L o L-funciones (llamadas series o funciones de *Dirichlet*), $L(s, \chi)$, asociadas con un carácter χ módulo $m(t)$. También, algunas consecuencias que involucran a la función *Zeta de Riemann*, $\zeta(s)$, y algunos productos de *Euler* en el caso polinomial.

Capítulo 1

Preliminares.

1.1. Conceptos básicos.

Definición 1.1. *Si $g(x) > 0$ para todo $x \geqslant a$, escribimos $f(x) = O(g(x))$ (se lee "$f(x)$ es oh grande de $g(x)$") en el sentido de que el cociente $f(x)/g(x)$ es acotado para $x \geqslant a$; es decir, existe una constante $M > 0$ tal que*

$$|f(x)| \leqslant Mg(x) \text{ para toda } x \geqslant a.$$

Una expresión de la forma $f(x) = h(x) + O(g(x))$ significa que $f(x) - h(x) = O(g(x))$.

Notación 1.1. *Usaremos la notación $f(x) \ll g(x)$ para indicar que existe una constante positiva M tal que $f(x) \leqslant Mg(x)$.*

Teorema 1.1. *Sea G un grupo y g un elemento de G. Entonces, si $o((g)) = m$, entonces $(g) = \{1, g, \cdots, g^{m-1}\}$, y $g^n = 1$ si, y sólo si, $m|n$.*

Teorema 1.2 (Algoritmo de la división para enteros)**.** *Si $m, n \in \mathbb{Z}$ y $n > 0$, entonces existe un único par de enteros q y r tales que $m = qn + r$, donde $0 \leqslant r < n$.*

Definición 1.2. *Sea K un campo. Sea $f(t) = a_0 + a_1t + \cdots + a_nt^n$ un polinomio en $K[t]$, con $a_n \neq 0_K$. Entonces, a_n se llama el coeficiente líder de $f(t)$. El grado de $f(t)$ es el entero n, y se denota "$\deg(f(x))$". $f(t)$ es mónico o unitario si $a_n = 1_K$.*

Teorema 1.3 (Algoritmo de la división para polinomios)**.** *Sea K un campo y $f(t), g(t) \in K[t]$ con $g(t) \neq 0_K$. Entonces, existen polinomios únicos $q(t)$ y $r(t)$ tales que*

$$f(t) = g(t)q(t) + r(t),$$

donde o $r(t) = 0_K$ o $deg(r(t)) < deg(g(t))$.

Afirmación 1.1. *Sea K un campo y k, n enteros positivos. Entonces, $x^k - 1_K$ divide a $x^n - 1_K$ en $K[x]$ si, y sólo si, $k|n$ en $\mathbb{Z}$.*

Demostración. Como k y n son enteros con $k > 0$, entonces por *Teorema 1.2* existen enteros únicos q y r tales que $n = kq + r$ y $0 \leqslant r < n$.
Note que $x^n - 1_K = (x^k - 1_K)h(x) + (x^r - 1_K)$, donde $h(x) = x^{n-k} + x^{n-2k} + \cdots + x^{n-qk}$.
Si $x^k - 1_K | x^n - 1_K$, entonces existe $f(x) \in K(x)$ tal que

$$x^n - 1_K = (x^k - 1_K)f(x) + 0.$$

Luego, por *Teorema 1.3* se tiene que $x^r - 1_K = 0$, lo cual obliga a que $r = 0$. Por lo tanto, $n = kq$, es decir, $k|n$.
Recíprocamente, si $k|n$, entonces existe $u \in \mathbb{Z}$ tal que $n = ku$. Luego, por *Teorema 1.2* se tiene que $r = 0$. Por lo tanto,

$$x^n - 1_K = (x^k - 1_K)h(x).$$

Es decir, $x^k - 1_K | x^n - 1_K$. ■

Teorema 1.4 (Factorización única de polinomios)**.** *Sea K un campo. Cada polinomio no constante $f(t)$ en $K[t]$ es un producto de polinomios irreducibles en $K[t]$. Esta factorización es única en el sentido siguiente: Si*

$$f(t) = p_1(t)p_2(t)\cdots p_r(t) \quad y \quad f(t) = q_1(t)q_2(t)\cdots q_s(t)$$

con cada $p_i(t)$ y $q_j(t)$ irreducible, entonces $r = s$. También, los $q_j(t)$ pueden ser reorganizados y reetiquetados de modo que $p_i(t)$ es un asociado de $q_i(t)$, para $i = 1, 2, \cdots$.

Proposición 1.1. *Si K es un cuerpo, entonces $K[t]$ es un dominio euclidiano.*

1.2. Congruencias en $K[t]$ y aritmética de las clases de congruencia.

Definición 1.3. *Sea K un campo y $f(t), m(t) \in K[t]$ con $m(t)$ diferente de cero. La clase de $f(t)$ módulo $m(t)$ se define así*

$$\begin{aligned}\hat{f}(t) &= \{g(t) \mid g(t) \equiv f(t) \text{ mód } m(t)\} \\ &= \{f(t) + h(t)m(t) \mid h(t) \in K[t]\},\end{aligned}$$

y se denota con $\hat{f}(t)$. El conjunto de todas las clases de congruencia módulo $m(t)$ se denota con $K[t]/(m(t))$, la notación análoga de $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

Observación 1.1. *De ahora en adelante, $\mathbb{F}_q$ denota a un cuerpo de característica p y cardinal $q = p^k$, con p un número entero primo y $k \geqslant 1$.*

Teorema 1.5. *$f(t) \equiv g(t)$ mód $p(t)$ si, y sólo si, $\hat{f}(t) = \hat{g}(t)$.*

Corolario 1.1. *Sea K un cuerpo finito con q elementos. Entonces, $K^* = K - \{0\}$ es cíclico de orden $q - 1$. Además, $K = \mathbb{F}_p(\zeta)$, donde ζ es una raíz $(q-1)$-ésima primitiva de la unidad.*

Véase la prueba en [1, Lección I, Corolario 2].

Teorema 1.6. *Sea A un dominio con un número finito de unidades n, y sea u una unidad de A. Entonces, $u^n = 1_A$.*

En particular, como $\mathbb{F}_q$ es un cuerpo con q elementos, es un dominio de integridad que tiene $q - 1$ unidades. Luego, si $a \in \mathbb{F}_q$ con $a \neq 0$, entonces $a^{q-1} = e$, por tanto, $a^q = a$. Esta igualdad vale si $a = 0$.

Corolario 1.2. *Sea K un campo y $p(t)$ un polinomio de grado n en $K[t]$. Sea*

$$S = \{a_0 + a_1 t + \cdots + a_m t^m \mid m < n \text{ y } a_i \in K \text{ con } 0 \leqslant i \leqslant m\}$$

Entonces, toda clase de congruencia módulo $p(t)$ es la clase de algún polinomio en S, y las clases de congruencias de polinomios diferentes en S son distintas. Es decir, $\hat{f}(t) = \hat{h}(t)$ donde $h(t) \in S$, y $\hat{f}(t) \neq \hat{h}(t)$, si $f(t), h(t) \in S$ y $f(t) \neq h(t)$.

Afirmación 1.2. *Si $m(t) \in \mathbb{F}_q[t]$ tiene grado k, entonces hay exactamente q^k clases de congruencias distintas en $\mathbb{F}_q[t]/(m(t))$.*

Demostración. Si $p(t) \in \mathbb{F}_q[t]$ tiene grado k, entonces los posibles residuos en la división por $p(t)$ son de la forma $a_0 + a_1 t + \cdots + a_{k-1}t^{k-1}$ con $a_i \in \mathbb{F}_q$, por el algoritmo de la división. Por otro lado, hay q posibilidades para cada de los k coeficientes $a_0,\ a_1,\ \cdots,\ a_{k-1}$ y, por lo tanto, hay q^k polinomios diferentes de esta forma. Por consiguiente, por *Corolario 1.2*, hay exactamente q^k clases de congruencias distintas en $\mathbb{F}_q[t]/(m(t))$. ■

Proposición 1.2. *El conjunto $U(\mathbb{F}_q[t]/(m(t)))$, con $m(t) \in \mathbb{F}_q[t]$, definido por*

$$U(\mathbb{F}_q[t]/(m(t))) = \{\hat{a} \in \mathbb{F}_q[t]/(m(t)) \mid (a, m) = 1\}$$

es un grupo multiplicativo de orden $\varphi(m)$, donde φ es la función de Euler para los polinomios. En particular, si $m(t)$ es un polinomio primo de grado k, entonces $U(\mathbb{F}_q[t]/(m(t))) = (\mathbb{F}_q[t]/(m(t)))^*$, los elementos no nulos de $\mathbb{F}_q[t]/(m(t))$, es un grupo multiplicativo de orden $\varphi(m) = q^k - 1$.

Teorema 1.7. *Sea K un campo y $p(t)$ un polinomio no constante en $K[t]$. Entonces, $K[t]/(p(t))$ es un anillo conmutativo con identidad que contiene a K.*

Teorema 1.8. *Sea K un campo y $p(t)$ un polinomio no constante en $K[t]$. Entonces, las siguientes afirmaciones son equivalentes:*

(i). $p(t)$ es irreducible en $K[t]$.

(ii). $K[t]/(p(t))$ es un campo.

(iii). $K[t]/(p(t))$ es un dominio de integridad.

Observación 1.2. *$M(q;t)$ denota el monoide de los polinomios unitarios con coeficientes en $\mathbb{F}_q$ y $P(q;t)$ denota el conjunto de los polinomios primos de $\mathbb{F}_q[t]$, es decir, de los polinomios irreducibles unitarios.*

Teorema 1.9 (Análogo del teorema de Euler)**.** *Si $(a, m) = 1$ con $m \in M(q;t)$, entonces*

$$a^{\varphi(m)} \equiv 1 \text{ mód } m.$$

Véase la prueba en [1, Lección II, Sección 4].
Una consecuencia del teorema anterior es el siguiente:

Corolario 1.3 (Análogo del teorema pequeño de Fermat)**.** *Si $p(t) \in P(q;t)$ tiene grado d y $p(t) \nmid a(t)$, entonces*

$$a(t)^{q^d - 1} \equiv 1 \text{ mód } p(t).$$

1.3. Funciones aritméticas.

Definición 1.4. *Una función con valor complejo definida en el monoide $M(q;t)$ se llama una función aritmética. Una función aritmética $f \neq 0$ es multiplicativa si $f(mn) = f(m)f(n)$ siempre que $(m, n) = 1$ y es completamente multiplicativa si $f(mn) = f(m)f(n)$ para todo par $m, n \in M(q;t)$.*

Definición 1.5. *La función aritmética I dada por*

$$I(f) = \begin{cases} 1, & \text{si } f = 1, \\ 0, & \text{si } f \neq 1 \end{cases}$$

se llama la función identidad.

Definición 1.6. *El análogo de la función de Möbius μ está definida por*

$$\mu(f) = \begin{cases} 1, & \text{si } f = 1, \\ 0, & \text{si } \pi^2 | f \text{ para algún } \pi \in P(q;t), \\ (-1)^r, & \text{si } f = \pi_1 \pi_2 \cdots \pi_r, \text{ donde los } \pi_i \in P(q;t) \text{ son mutuamente distintos.} \end{cases}$$

Para $f = 1$, se considera $r = 0$.

Teorema 1.10. *La función de Möbius satisface la relación*

$$\sum_{d|f} \mu(d) = I(f).$$

Véase la prueba en [1, Lección VII, Proposición 6 (a)].

Teorema 1.11. *La función de Möbius μ es multiplicativa.*

Véase la prueba en [1, Lección VII, Proposición 6 (b)].

Afirmación 1.3.

$$\sum_{d|f} \mu(d) = \prod_{\pi|f} (1 + \mu(\pi)), \tag{1.1}$$

si $f = \pi_1^{a_1} \pi_2^{a_2} \cdots \pi_k^{a_k}$, con $\pi_i \in P(q;t)$, $a_i \geqslant 1$.

Demostración. Teniendo en cuenta que μ es multiplicativa, desarrollamos el producto del miembro derecho de la igualdad (1.1), obteniendo

$$\begin{aligned} &\prod_{\pi|f} (1 + \mu(\pi)) \\ &= (1 + \mu(\pi_1))(1 + \mu(\pi_2)) \cdots (1 + \mu(\pi_k))(1 + \mu(\pi_1\pi_2)) \cdots \\ &\quad (1 + \mu(\pi_{k-1}\pi_k)) \cdots (1 + \mu(\pi_1 \pi_2 \cdots \pi_k)) \\ &= 1 + \mu(\pi_1) + \mu(\pi_2) + \cdots + \mu(\pi_k) + \mu(\pi_1\pi_2) + \cdots + \mu(\pi_{k-1}\pi_k) + \cdots + \mu(\pi_1 \pi_2 \cdots \pi_k) \end{aligned}$$

lo cual es igual al miembro izquierdo de (1.1). ■

Definición 1.7. *La norma $|\cdot|$ de un polinomio unitario de $\mathbb{F}_q[t]$ es una función $|\cdot| : M(q;t) \to \mathbb{N}$ tal que $|a(t)| = q^n$ con $n = \deg(a(t))$, para $a(t) \in M(q;t)$. Como tal, esta función tiene las siguientes propiedades:*

(i). $|1| = 1$,

(ii). *si $p(t) \in P(q;t)$, entonces $|p(t)| > 1$, y*

(iii). $|a_1(t)a_2(t)| = |a_1(t)||a_2(t)|$ *para* $a_1(t), a_2(t) \in M(q;t)$.

Proposición 1.3 (Fórmula de la inversión de Möbius)**.** *Sean f y g dos funciones aritméticas. Suponga que para cada $a \in M(q;t)$, la función*

$$g(a) = \sum_{d|a} f(d)$$

es multiplicativa. Entonces,

$$f(a) = \sum_{d|a} \mu(d) g(a/d) = \sum_{d|a} g(d) \mu(a/d)$$

y la función f es multiplicativa.

Véase la prueba en [1, Lección VII, Proposición 9].

Definición 1.8. *El análogo de la función de von Mangoldt está definida por*

$$\Lambda(f) = \begin{cases} \log|\pi|, & \text{si } f = \pi^k, \text{ para algún } \pi \in P(q;t) \text{ y } k \geqslant 1, \\ 0, & \text{de otro modo.} \end{cases}$$

Como $\Lambda(1) = 0$, esta función no es invertible y mucho menos multiplicativa.

1.4. Caracteres de grupos abelianos finitos.

Definición 1.9. *Sea G un grupo abeliano finito, denotado multiplicativamente. Un homomorfismo $f : G \to \mathbb{C}^*$ se llama un carácter de G si f tiene la propiedad multiplicativa*

$$f(g_1 g_2) = f(g_1) f(g_2)$$

para todo g_1, g_2 en G, y $f(1_G) = 1$, donde 1_G es el elemento unidad de G.
El conjunto de todos los caracteres de G se denota con $\widehat{G}$, esto es

$$\widehat{G} = \{f : G \to \mathbb{C}^* \mid f \text{ es un homomorfismo de grupos}\}.$$

Con $\mathcal{T}$ designamos al grupo multiplicativo $\{z \in \mathbb{C}^* \mid |z| = 1\}$ (la circunferencia de radio 1 y centro en el origen). Este grupo es un subgrupo de $\mathbb{C}^*$.

Proposición 1.4. *Si $f \in \widehat{G}$, entonces $f(g) \in \mathcal{T}$, para todo $g \in G$. Es decir, cada función valuada $f(g)$ es una raíz de la unidad. De hecho, si $g^n = 1_G$, entonces $f^n(g) = 1$.*

Véase la prueba en [1, Lección VIII, Proposición 1].

Todo grupo admite, por lo menos, un carácter $f_o(g) := 1$, para todo $g \in G$. A este carácter se le llama principal.
Si $f_1, f_2 \in \widehat{G}$, podemos definir una ley de composición interna sobre $\widehat{G}$, de la siguiente manera:

$$(f_1 f_2)(g) := f_1(g) f_2(g) \tag{1.2}$$

para cualquier g de G. Además, $f_o f = f f_o = f$, para cualquier $f \in \widehat{G}$.

Proposición 1.5. *Sea G un grupo abeliano finito. Con la ley (1.2), $\widehat{G}$ es un grupo abeliano. Además, si $f \in \widehat{G}$, entonces*

$$f^{-1}(g) = \frac{1}{f(g)} = \overline{f(g)}$$

para cada $g \in G$.

Demostración. Los postulados de grupo abeliano son de fácil verificación, usando la definición, por lo tanto, vamos a omitir los detalles. Por otro lado, por la *Proposición 1.4*, $|f(g)| = 1$, para cada $g \in G$. Como $f(g)\overline{f(g)} = |f(g)|^2 = 1$ y $f(g)f^{-1}(g) = 1$, entonces $f^{-1}(g) = \overline{f(g)}$, pues, el inverso multiplicativo en $\mathbb{C}$ es único. Por lo tanto, el recíproco $1/f(g) = f^{-1}(g)$ es igual al conjugado complejo $\overline{f(g)}$, para cualquier $g \in G$. Así, la función definida por $\overline{f(g)} = \bar{f}(g)$, para cada $g \in G$ es, también, un carácter de G. ■

Proposición 1.6. *Si G es un grupo abeliano finito, entonces $G \cong \widehat{G}$. Es decir, $o(G) = o(\widehat{G})$.*

Véase la prueba en [1, Lección VII, Proposición 7] o en [3, Teorema 6.8].

1.5. Caracteres módulo $m(t)$.

Definición 1.10. *Sea $m \in \mathbb{F}_q[t]$ un polinomio no constante fijo. Sea $\chi' : (\mathbb{F}_q[t]/(m(t)))^* \to \mathbb{C}^*$ un homomorfismo. Dado χ', definamos $\chi : \mathbb{F}_q[t] \to \mathbb{C}^*$ de la siguiente forma:*

$$\chi(f) = \begin{cases} 0, & si\ (f,m) \neq 1, \\ \chi'(\hat{f}), & si\ (f,m) = 1. \end{cases}$$

Las funciones χ definidas de esta manera son llamadas caracteres de Dirichlet módulo m. El carácter principal χ_o es el que tiene las propiedades:

$$\chi_o(f) = \begin{cases} 0, & si\ (f,m) \neq 1, \\ 1, & si\ (f,m) = 1. \end{cases}$$

Definición 1.11. *Sea $m \in \mathbb{F}_q[t]$. Una función $\chi : \mathbb{F}_q[t] \to \mathbb{C}^*$ se llama un carácter multiplicativo módulo m si para cada $a, b \in \mathbb{F}_q[t]$ se tiene:*

(i). $\chi(a) = 0$, *si* $(a,m) \neq 1$.

(ii). $\chi(1) \neq 0$.

(iii). $\chi(ab) = \chi(a)\chi(b)$.

(iv). $a \equiv b \bmod m$, *entonces* $\chi(a) = \chi(b)$.

Como es fácil ver, un carácter multiplicativo módulo $m(t)$ es un carácter del grupo $(\mathbb{F}_q[t]/(m(t)))^*$, que se extiende a $\mathbb{F}_q[t]/(m(t))$ haciendo $\chi(\alpha) = 0$ para todo divisor de cero α en este anillo.

Proposición 1.7. *Si χ es un carácter módulo $m(t)$, entonces*

$$\sum_{a \bmod m} \chi(a) = \begin{cases} \varphi(m), & si\ \chi = \chi_o, \\ 0, & si\ \chi \neq \chi_o. \end{cases}$$

Véase la prueba en [1, Lección VIII, Proposición 9].

Proposición 1.8. *Sea $\varphi'(m)$ el número de caracteres módulo $m(t)$ sobre $\mathbb{F}_q[t]$. Entonces*

$$\sum_{\chi} \chi(a) = \begin{cases} \varphi'(m), & si\ a \equiv 1 \bmod m, \\ 0, & si\ a \not\equiv 1 \bmod m. \end{cases}$$

Véase la prueba en [1, Lección VIII, Proposición 11].

Ahora, podemos calcular el número de caracteres distintos módulo $m(t)$ sobre $\mathbb{F}_q[t]$. En efecto, por la *Proposición 1.7* y por la *Proposición 1.8*,

$$\sum_{\chi} \left(\sum_{a \bmod m} \chi(a) \right) = \sum_{a \bmod m} \chi_o(a) + \sum_{a \bmod m} \chi_o(a) \Big|_{\chi \neq \chi_o} = \varphi(m)$$

y

$$\sum_{a \bmod m} \left(\sum_{\chi} \chi(a) \right) = \sum_{\chi} \chi(a) \Big|_{a \equiv 1 \bmod m} + \sum_{\chi} \chi(a) \Big|_{a \not\equiv 1 \bmod m} = \varphi'(m).$$

También,

$$\sum_{\chi}\left(\sum_{a \bmod m}\chi(a)\right)=\sum_{a \bmod m}\left(\sum_{\chi}\chi(a)\right).$$

Por lo tanto, $\varphi(m)=\varphi'(m)$.
Es decir, los caracteres de *Dirichlet* (que están definidos en $\mathbb{F}_q[t]$) inducen y están inducidos por elementos en el grupo de caracteres de $(\mathbb{F}_q[t]/(m(t)))^*$. Por consiguiente, hay exactamente $\varphi(m)$ caracteres de *Dirichlet* módulo $m(t)$.

Los caracteres módulo $m(t)$ de un grupo abeliano finito satisfacen ciertas relaciones de ortogonalidad. Aquí tomamos $G=(\mathbb{F}_q[t]/(m(t)))^*$. Para nosotros, éstas relaciones toman las siguientes formas:

Lema 1.1. *Sean $\chi_1,\cdots,\chi_{o(\widehat{G})}$ caracteres de Dirichlet módulo m (asumiendo χ_1 como el carácter principal) y $u,v\in\mathbb{F}_q[t]$ con $(v,m)=1$. Entonces,*

$$\frac{1}{\varphi(m)}\sum_{\chi}\chi(u)\overline{\chi(v)}=\delta(u,v),$$

donde

$$\delta(u,v)=\begin{cases}1, & \text{si } u\equiv v \bmod m,\\ 0, & \text{de otra manera.}\end{cases}$$

Véase la prueba en [1, Lección VII, Proposición 13] o en [3, Teorema 6.16].

Lema 1.2. *Sean χ, ψ caracteres de Dirichlet módulo m y $u\in\mathbb{F}_q[t]$. Entonces,*

$$\frac{1}{\varphi(m)}\sum_{u \bmod m}\chi(u)\overline{\psi(u)}=\delta(\chi,\psi),$$

donde

$$\delta(\chi,\psi)=\begin{cases}1, & \text{si } \chi=\psi,\\ 0, & \text{de otra manera.}\end{cases}$$

Demostración. Suponga que $\chi(u)=\psi(u)$ para todo $u\in\mathbb{F}_q[t]$ (u mód m). Entonces,

$$\chi(u)\bar{\psi}(u)=\psi(u)\bar{\psi}(u)=\chi_o(u).$$

Por tanto,

$$\begin{aligned}\sum_{u \bmod m}\chi(u)\overline{\psi(u)}&=\sum_{u \bmod m}\chi(u)\bar{\psi}(u)\\ &=\sum_{u \bmod m}\chi_o(u)\\ &=\sum_{\substack{u \bmod m\\(u,m)=1}}\chi_o(u)+\sum_{\substack{u \bmod m\\(u,m)\neq 1}}\chi_o(u)\\ &=\sum_{\substack{u \bmod m\\(u,m)=1}}1=\varphi(m).\end{aligned}$$

Por otro lado, suponga $\chi\neq\psi$. Entonces, $\chi\bar{\psi}\neq\chi_o$, por tanto, existe un $b\in\mathbb{F}_q[t]$ tal que $(\chi\bar{\psi})(b)\neq 1$. Como consecuencia, tenemos

$$\sum_{u \bmod m}\chi(u)\overline{\psi(u)}=\sum_{u \bmod m}(\chi\bar{\psi})(u)=\sum_{u \bmod m}(\chi\bar{\psi})(bu)=(\chi\bar{\psi})(b)\sum_{u \bmod m}(\chi\bar{\psi})(u),$$

y así

$$((\chi\bar{\psi})(b)-1)\sum_{u \bmod m}(\chi\bar{\psi})(u)=0.$$

Ya que, $(\chi\bar{\psi})(b)-1\neq 0$, esto implica que $\sum_{u \bmod m}(\chi\bar{\psi})(u)=0$. ■

Como ejemplo, tomando $\psi=\chi_o$, podemos deducir de la relación de arriba que $\sum_{u \bmod m}\chi(u)=0$ para cualquier carácter no principal χ (si $(u,m)=1$, $\overline{\chi_o(u)}=1=\chi_o(u)$. Por el contrario, si $(u,m)\neq 1$, entonces $\overline{\chi_o(u)}=0=\chi_o(u)$. Es decir, $\overline{\chi_o}=\chi_o$).

Capítulo 2

Teorema de Dirichlet en $\mathbb{F}_q[t]$ según Pollack.

Antes de proceder, introducimos un poco de notación: Para $p \in \mathbb{F}_q[t]$ se define $\varphi(p)$ como el cardinal del grupo de unidades de $\mathbb{F}_q[t]/(p)$. De aquí en adelante, π siempre denota un mónico irreducible de $\mathbb{F}_q[t]$, d, f siempre denotan polinomios mónicos, n siempre denota un entero no negativo. Las sumas de polinomios siempre se entiende que deben tomarse sólo sobre polinomios mónicos.
Con estos acuerdos, podemos expresar uno de nuestros resultados principales como:

Teorema 2.1. *Sean $\mathbb{F}_q$ un cuerpo finito, $a, m \in \mathbb{F}_q[t]$ con $(a, m) = 1$ y $m \neq 0$. Entonces, para $n \geqslant 0$,*

$$\sum_{\substack{\pi \equiv a \bmod m \\ \deg \pi \leqslant n}} \frac{\log |\pi|}{|\pi|} = \frac{1}{\varphi(m)} \log(q^n) + O(1).$$

Corolario 2.1. *Bajo los supuestos del Teorema 2.1, tenemos para $x \geqslant 1$,*

$$\sum_{\substack{\pi \equiv a \bmod m \\ |\pi| \leqslant x}} \frac{\log |\pi|}{|\pi|} = \frac{1}{\varphi(m)} \log x + O(1).$$

Demostración. Para $x = q^n$, donde $0 \leqslant n \in \mathbb{Z}$, la consecuencia es inmediata por *Teorema 2.1.* A saber, para $0 \leqslant n \in \mathbb{Z}$, tenemos

$$\sum_{\substack{\pi \equiv a \bmod m \\ \deg \pi \leqslant n}} \frac{\log |\pi|}{|\pi|} = \frac{1}{\varphi(m)} \log(q^n) + O(1).$$

Además, como $0 < \deg(\pi) \leqslant n$, entonces $q^{\deg(\pi)} \leqslant q^n$. Es decir, $|\pi| \leqslant q^n = x$. Por lo tanto, se concluye la prueba.
Por otro lado, el resultado se sigue para todo $x \geqslant 1$, de la siguiente manera:
Note que si $n = 0$, $1 \leqslant x < q$; si $n = 1$, $q \leqslant x < q^2$; si $n = 2$, $q^2 \leqslant x < q^3$, así, de manera sucesiva, obtenemos que $1 \leqslant q^n \leqslant x < q^{n+1}$, para cualquier $n \geqslant 0$. Por consiguiente,

$$\log(q^n) \leqslant \log x < \log(q^{n+1}). \tag{2.1}$$

Entonces,

$$\log(q^n) + \log(q^{n+1}) \leqslant \log x + \log(q^{n+1})$$

y, además,

$$2\log(q^n) < \log(q^n) + \log(q^{n+1}).$$

Por lo tanto,

$$2\log(q^n) < \log x + \log(q^{n+1}).$$

De aquí, tenemos

$$-[\log(q^{n+1}) - \log(q^n)] = -\log(q^{n+1}) + \log(q^n) < \log x - \log(q^n). \tag{2.2}$$

Por otra parte, de (2.1) se puede concluir

$$0 \leqslant \log x - \log(q^n) < \log(q^{n+1}) - \log(q^n). \tag{2.3}$$

Luego, de (2.2) y (2.3), se tiene

$$|\log x - \log(q^n)| < \log(q^{n+1}) - \log(q^n).$$

Es decir, existe $M = \log(q^{n+1}) - \log(q^n) > 0$, tal que, para todo $x \geqslant 1$, se cumple

$$|\log x - \log(q^n)| \leqslant M \cdot 1.$$

Entonces, $\log x - \log(q^n) = O(1)$, lo que significa

$$\log x = \log(q^n) + O(1).$$

Lo que nos conduce a la siguiente igualdad:

$$\begin{aligned}\frac{1}{\varphi(m)}\log(q^n) + O(1) &= \frac{1}{\varphi(m)}\log x - \frac{1}{\varphi(m)}O(1) + O(1)\\ &= \frac{1}{\varphi(m)}\log x + \left(1 - \frac{1}{\varphi(m)}\right)O(1)\\ &= \frac{1}{\varphi(m)}\log x + O(1).\end{aligned}$$

Ahora, note que $|\pi| = q^{\deg(\pi)} \leqslant q^n \leqslant x$. Finalmente, de lo anterior y por *Teorema 2.1*, se concluye

$$\sum_{\substack{\pi \equiv a \bmod m \\ |\pi| \leqslant x}} \frac{\log|\pi|}{|\pi|} = \frac{1}{\varphi(m)}\log x + O(1)$$

para $x \geqslant 1$. ■

2.1. Algunos resultados preliminares.

En primer lugar demostraremos un análogo de la estimación $\log[x]! = x\log x - x + O(\log x)$.

Lema 2.1. *Para $n \geqslant 0$,*

$$\sum_{\deg(f) \leqslant n} \log|f| = \frac{q^{n+1}}{q-1}\log(q^n) - \left(\frac{q}{q-1}\right)\left(\frac{q^n - 1}{q-1}\right)\log q.$$

Demostración. Sea $S := \sum_{\deg(f)\leqslant n} \log|f|$. Ya que $|f| = q^{\deg(f)}$, entonces

$$\begin{aligned}S = \sum_{\deg(f)\leqslant n} \log|f| &= \sum_{k=0}^{n} \log q \sum_{\deg(f)=k} \deg(f)\\ &= \sum_{k=0}^{n} k\log q \sum_{\deg(f)=k} 1.\end{aligned}$$

Puesto que, $\sum_{\deg(f)=k} 1 = q^k$ para $f(t) \in \mathbb{F}_q[t]$, entonces

$$S = \sum_{k=0}^{n} k \log q \sum_{\deg(f)=k} 1 = \log q \sum_{k=0}^{n} k q^k,$$

por lo tanto,

$$\begin{aligned}
S(1-q) &= \left(\log q \sum_{k=0}^{n} k q^k \right)(1-q) \\
&= \log q \left(\sum_{k=0}^{n} k q^k - q \sum_{k=0}^{n} k q^k \right) \\
&= \log q [0 + q + 2q^2 + 3q^3 + \cdots + nq^n - q(0 + q + 2q^2 + 3q^3 + \cdots + (n-1)q^{n-1} + nq^n)] \\
&= \log q [0 + q + 2q^2 + 3q^3 + \cdots + nq^n - q^2 - 2q^3 - 3q^4 - \cdots - (n-1)q^n - nq^{n+1}] \\
&= \log q (q + q^2 + q^3 + \cdots + q^n - nq^{n+1}) \\
&= \log q \left(-nq^{n+1} + \sum_{k=1}^{n} q^k \right) \\
&= \log q \left[-nq^{n+1} + \frac{q(q^n-1)}{q-1} \right] \\
&= q \log q \left(-nq^n + \frac{q^n - 1}{q-1} \right)
\end{aligned}$$

pues, $\sum_{k=1}^{n} q^k$ es una progresión geométrica. Entonces,

$$\begin{aligned}
S &= -\frac{q \log q}{q-1} \left(-nq^n + \frac{q^n-1}{q-1} \right) \\
&= \frac{nq^{n+1} \log q}{q-1} - \frac{q \log q}{q-1} \cdot \frac{q^n - 1}{q-1} \\
&= \frac{q^{n+1}}{q-1} \log(q^n) - \left(\frac{q}{q-1} \right) \left(\frac{q^n-1}{q-1} \right) \log q.
\end{aligned}$$

■

También necesitaremos algunos resultados elementales sobre la distribución de primos en $\mathbb{F}_q[t]$, los cuales reuniremos aquí. Éstas serán consecuencias sencillas de los siguientes:

Teorema 2.2 (Teorema del número primo para $\mathbb{F}_q[t]$)**.** *Sea $\mathbb{F}_q$ un cuerpo finito. Sea $\nu_q(n)$ que denota el número de polinomios primos (mónicos) de grado n en $\mathbb{F}_q[t]$. Para $n \geqslant 1$, $\sum_{d|n} d\nu_q(d) = q^n$. Así,*

$$\nu_q(n) = \frac{1}{n} \sum_{d|n} q^d \mu(n/d) = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n} \right).$$

Demostración. Consideremos la factorización prima de $t^{q^n} - t$ en $\mathbb{F}_q[t]$. Si $\pi(t)$ es un primo mónico de grado d, con $d|n$, es decir, $n = dk$, para algún $k \in \mathbb{Z}$, entonces

$$t^{q^d} \equiv t \text{ mód } \pi(t) \tag{2.4}$$

por el análogo del teorema pequeño de Fermat. A saber, como $\pi(t)$ es un primo mónico de grado d y $\pi(t) \nmid t$ (en el caso de que $\pi(t) = t$, es fácil notar que $t^q \equiv t$ mód $\pi(t)$, pues $t^q = t + t(t^{q-1} - 1)$), entonces por el

análogo del teorema pequeño de Fermat $t^{q^d-1} \equiv 1$ mód $\pi(t)$, es decir, $t^{q^d} \equiv t$ mód $\pi(t)$.
Elevando reiteradamente ambos lados de (2.4) a la q^d obtenemos:

$$t^{q^d} \equiv t,\ t^{q^{2d}} \equiv t^{q^d},\ t^{q^{3d}} \equiv t^{q^{2d}}, \cdots,\ t^{q^{kd}} \equiv t^{q^{(k-1)d}}$$

para $k \geqslant 1$.
Por consiguiente,

$$t^{q^{kd}} \equiv t^{q^{(k-1)d}} \equiv \cdots \equiv t^{q^{3d}} \equiv t^{q^{2d}} \equiv t^{q^d} \equiv t \text{ mód } \pi(t)$$

para $k \geqslant 1$. De modo que $\pi(t)|(t^{q^{kd}} - t) = (t^{q^n} - t)$.
Recíprocamente, si $\pi(t)|(t^{q^n} - t)$ escogemos $\widehat{g(t)}$ como un generador del grupo multiplicativo $\left(\mathbb{F}_q[t]/(\pi(t))\right)^*$ (ya que, por ser $\mathbb{F}_q[t]/(\pi(t))$ un cuerpo finito, por *Afirmación 1.2* y *Teorema 1.8*, $\left(\mathbb{F}_q[t]/(\pi(t))\right)^*$ es cíclico, por *Corolario 1.1*).
Entonces, ya que, $t^{q^n} \equiv t$ mód $\pi(t)$, tenemos $t^{q^n} = t + h(t)\pi(t)$ con $h(t) \in \mathbb{F}_q[t]$. Si $g(t) = g_0 + g_1 t + \cdots + g_k t^k$ donde cada $g_i \in \mathbb{F}_q$, se tiene:

$$\begin{aligned}
g(t^{q^n}) &= g(t + h(t)\pi(t)) \\
&= g_0 + g_1(t + h(t)\pi(t)) + \cdots + g_k(t + h(t)\pi(t))^k \\
&= g_0 + g_1(t + h(t)\pi(t)) + \cdots + g_k(t^k + kt^{k-1}h(t)\pi(t) + \cdots + h^k(t)\pi^k(t)) \\
&= g_0 + g_1 t + \cdots + g_k t^k + g_1 h(t)\pi(t) + \cdots + g_k(kt^{k-1}h(t)\pi(t) + \cdots + h^k(t)\pi^k(t)) \\
&= g(t) + [g_1 h(t) + \cdots + g_k(kt^{k-1}h(t) + \cdots + h^k(t)\pi^{k-1}(t))]\pi(t).
\end{aligned}$$

Es decir, $g(t^{q^n}) \equiv g(t)$ mód $\pi(t)$. Por otro lado,

$$g(t^{q^n}) = g_0 + g_1 t^{q^n} + \cdots g_k t^{kq^n}$$

y, además, por *Teorema 1.6*

$$\begin{aligned}
g(t)^{q^n} &= (g_0 + g_1 t + \cdots g_k t^k)^{q^n} \\
&= g_0^{q^n} + g_1^{q^n} t^{q^n} + \cdots g_k^{q^n} t^{kq^n} \\
&= g_0 + g_1 t^{q^n} + \cdots g_k t^{kq^n}
\end{aligned}$$

puesto que $\mathbb{F}_q$ es un dominio de integridad con $q-1$ unidades y de característica p.
Entonces,

$$g(t)^{q^n} = g(t^{q^n}) \equiv g(t) \text{ mód } \pi(t)$$

es decir, $\widehat{g(t)^{q^n}} = \widehat{g(t)}$.
Como $\widehat{g(t)} \in \left(\mathbb{F}_q[t]/(\pi(t))\right)^*$, existe $\widehat{g(t)^{-1}} \in \left(\mathbb{F}_q[t]/(\pi(t))\right)^*$ tal que $\widehat{g(t)^{q^n-1}} = \widehat{1}$. Además, puesto que $o(\widehat{g(t)}) = q^d - 1$ (por *Corolario 1.1*, pues, $\mathbb{F}_q[t]/(\pi(t))$ es un cuerpo finito con q^d elementos), entonces, por *Teorema 1.1*, $q^d - 1 | q^n - 1$, lo que obliga a que $d|n$, por *Afirmación 1.1*.
Sea

$$t^{q^n} - t = \pi_1(t)\pi_2(t)\cdots\pi_k(t) \tag{2.5}$$

es la factorización única de $t^{q^n} - t$ en polinomios mónicos irreducibles. Por lo que se probó anteriormente, cada irreducible mónico de grado divisorio de n debe ser o aparece como uno de los π_i, y cada π_i es un irreducible mónico de grado divisorio de n (pues, $\pi_i | t^{q^n} - t$). También, ningún π_i aparece más de una vez, de lo contrario, por la regla del producto, y del hecho de que $\mathbb{F}_q$ es de característica p, π_i divide a la

derivada formal de $t^{q^n}-t$, la cual es -1. Esto es, tomando, en particular, $\pi_1=\pi_2$, y derivando a ambos lados de (2.5), se tiene

$$-1=q^nt^{q^n-1}-1=2\pi_1(t)\pi_1'(t)\Big(\pi_2(t)\cdots\pi_k(t)\Big)+\pi_1(t)\Big(\pi_2(t)\cdots\pi_k(t)\Big)'=\pi_1(t)r(t),$$

donde $r(t)=2\pi_1'(t)\Big(\pi_2(t)\cdots\pi_k(t)\Big)+\Big(\pi_2(t)\cdots\pi_k(t)\Big)'$, es decir, $\pi_1(t)|-1$, lo cual es contradictorio. De lo mostrado anteriormente se deduce que

$$t^{q^n}-t=\prod_{\pi(t):\deg\pi|n}\pi(t).$$

Como

$$t^{q^n}-t=\prod_{\pi(t):\deg\pi|n}\pi(t)=\underbrace{\big(\pi_{11}(t)\pi_{12}(t)\cdots\pi_{1k_1}(t)\big)}_{\substack{\deg\pi_{11}=\cdots=\deg\pi_{1k_1}\\ \deg\pi_{1i}|n}}\underbrace{\big(\pi_{21}(t)\pi_{22}(t)\cdots\pi_{2k_2}(t)\big)}_{\substack{\deg\pi_{21}=\cdots=\deg\pi_{2k_2}\\ \deg\pi_{2i}|n}}\cdots$$
$$\underbrace{\big(\pi_{r1}(t)\pi_{r2}(t)\cdots\pi_{rk_r}(t)\big)}_{\substack{\deg\pi_{r1}=\cdots=\deg\pi_{rk_r}\\ \deg\pi_{ri}|n}}$$

entonces, comparando grados, se tiene

$$\begin{aligned}q^n&=k_1\deg\pi_{1i}|_{\deg\pi_{1i}|n}+k_2\deg\pi_{2i}|_{\deg\pi_{2i}|n}+\cdots+k_r\deg\pi_{ri}|_{\deg\pi_{ri}|n}\\&=\nu_q(d)d|_{\substack{d=\deg\pi_{1i}\\ \deg\pi_{1i}|n}}+\nu_q(d)d|_{\substack{d=\deg\pi_{2i}\\ \deg\pi_{2i}|n}}+\cdots+\nu_q(d)d|_{\substack{d=\deg\pi_{ri}\\ \deg\pi_{ri}|n}}\\&=\sum_{d|n}d\nu_q(d).\end{aligned}$$

La fórmula para $\nu_q(n)$ se sigue de la inversión de Möbius (*Proposición 1.3*), así: colocando $g(n)=q^n$ y $f(d)=d\nu_q(d)$, se tiene

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

entonces

$$n\nu_q(n)=\sum_{d|n}q^d\mu(n/d).$$

Por lo tanto, $\nu_q(n)=\dfrac{1}{n}\displaystyle\sum_{d|n}q^d\mu(n/d)$. Por otro lado, veamos

$$\sum_{d|n}q^d\mu(n/d)=q^n+O(q^{n/2}+nq^{n/3}).\tag{2.6}$$

Si $n=1$, entonces $d=1$. Por lo tanto,

$$\sum_{d|1}q^d\mu(1/d)=q\mu(1)=q.$$

Pero, $q=q+0=q+O(q^{1/2}+q^{1/3})$. Por consiguiente,

$$\sum_{d|n}q^d\mu(n/d)=q^n+O(q^{n/2}+nq^{n/3}),\ \text{si } n=1.$$

Si $n = 2$, entonces $d = 1$ o $d = 2$. Por lo tanto,

$$\begin{aligned}\sum_{d|2} q^d\mu(2/d) &= q\mu(2) + q^2\mu(1)\\ &= q(-1) + q^2\\ &= -q + q^2\end{aligned}$$

Pero, $|-q| = q < q^{2/2} + 2q^{2/3}$. Es decir, $-q = O(q^{2/2} + 2q^{2/3})$. Entonces,

$$\sum_{d|n} q^d\mu(n/d) = q^n + O(q^{n/2} + nq^{n/3}),\ \text{si } n = 2.$$

Si n es un número primo > 2, entonces $d = 1$ o $d = n$. Por lo tanto,

$$\begin{aligned}\sum_{d|n} q^d\mu(n/d) &= q\mu(n) + q^n\mu(1)\\ &= q(-1) + q^n\\ &= -q + q^n\end{aligned}$$

Como $n > 2$, entonces $q^{n/2} > q$, pues $n/2 > 1$. Entonces, $|-q| = q < q^{n/2} < q^{n/2} + nq^{n/3}$. Es decir, $-q = O(q^{n/2} + nq^{n/3})$. Luego, (2.6) se verifica para un primo $n > 2$.
Suponga que n es un número con las siguientes formas:
Si $n = 2t$, con $t = 2, 3, \cdots$, entonces,

$$\sum_{d|n} q^d\mu(n/d) = q^n\mu(1) + q^{n/2}\mu(2) + S$$

donde

$$S := \sum_{\substack{d|n\\ d\leqslant n/4}} q^d\mu(n/d).$$

Por otro lado, como $d \leqslant \frac{n}{4} < \frac{n}{3}$, entonces $q^d < q^{n/3}$ y, además, $|\mu(n/d)| \leqslant 1$, por consiguiente,

$$\begin{aligned}\left|\sum_{\substack{d|n\\ d\leqslant n/4}} q^d\mu(n/d)\right| &\leqslant \sum_{\substack{d|n\\ d\leqslant n/4}} q^d|\mu(n/d)|\\ &= q^{t_1}|\mu(n/t_1)| + q^{t_2}|\mu(n/t_2)| + \cdots + q^{t_r}|\mu(n/t_r)| + q^{n/4}|\mu(4)|\\ &< \underbrace{q^{n/3} + q^{n/3} + \cdots + q^{n/3}}_{r\ \text{términos}}\\ &= rq^{n/3}\\ &< nq^{n/3},\end{aligned}$$

donde $t_1, t_2, \cdots, t_r$ son los divisores de n menores que $n/4$.
Por lo tanto,

$$|-q^{n/2} + S| \leqslant q^{n/2} + |S| < q^{n/2} + nq^{n/3}$$

Entonces,

$$\sum_{d|n} q^d\mu(n/d) = q^n + O(q^{n/2} + nq^{n/3}).$$

Si $n = 3t$, con $t = 2, 3, \cdots$, entonces,

$$\sum_{d|n} q^d \mu(n/d) = q^n \mu(1) + S$$

donde

$$S := \sum_{\substack{d|n \\ d \leqslant n/3}} q^d \mu(n/d).$$

Por otro lado,

$$\begin{aligned}
\left| \sum_{\substack{d|n \\ d \leqslant n/3}} q^d \mu(n/d) \right| &\leqslant \sum_{\substack{d|n \\ d \leqslant n/3}} q^d |\mu(n/d)| \\
&= q^{t_1}|\mu(n/t_1)| + q^{t_2}|\mu(n/t_2)| + \cdots + q^{t_r}|\mu(n/t_r)| + q^{n/3}|\mu(3)| \\
&= q^{t_1} + q^{t_2} + \cdots + q^{t_r} + q^{n/3} \\
&< \underbrace{q^{n/3} + q^{n/3} + \cdots + q^{n/3}}_{r \text{ términos}} + q^{n/2} \\
&= q^{n/2} + rq^{n/3} \\
&< q^{n/2} + nq^{n/3}
\end{aligned}$$

donde $t_1, t_2, \cdots, t_r$ son los divisores de n menores que $n/3$. Así, de esta forma, se verifica (2.6).
Análogamente, (2.6) se verifica si $n = pt$, donde p es un entero primo y $t \in \mathbb{Z}^+$. De acuerdo a lo anterior, (2.6) se cumple para $n \geqslant 1$.
Ya que,

$$\begin{aligned}
\sum_{d|n} q^d \mu(n/d) &= q^n + O(q^{n/2} + nq^{n/3}) \\
&= q^n + O((1 + nq^{-n/6})q^{n/2}) \\
&= q^n + O(q^{n/2})
\end{aligned}$$

la estimación final se sigue. ■

Lema 2.2. *Para cada f,*

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

También,

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

Demostración. Sea $f = \pi_1^{a_1} \pi_2^{a_2} \cdots \pi_k^{a_k}$ con π_i primo, para $1 \leqslant i \leqslant k$. Entonces,

$$|f| = |\pi_1|^{a_1} |\pi_2|^{a_2} \cdots |\pi_k|^{a_k}.$$

Por lo tanto,

$$\begin{aligned}
\log |f| &= \log(|\pi_1|^{a_1} |\pi_2|^{a_2} \cdots |\pi_k|^{a_k}) \\
&= \sum_{i=1}^{k} \log |\pi_i|^{a_i} \\
&= \sum_{i=1}^{k} a_i \log |\pi_i|, \qquad (2.7)
\end{aligned}$$

pues, al ser $|\cdot|$ una función completamente multiplicativa, se tiene

$$\log(|\pi_1|^{a_1}|\pi_2|^{a_2}\cdots|\pi_k|^{a_k}) = \log|\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_k^{a_k}| = \log|f|.$$

Por otro lado, si $d \in \{\pi_1, \pi_1^2, \cdots, \pi_1^{a_1}, \pi_2, \pi_2^2, \cdots, \pi_2^{a_2}, \cdots, \pi_k, \pi_k^2, \cdots, \pi_k^{a_k}\}$, entonces $\Lambda(d) \neq 0$, por lo cual:

$$\begin{aligned}
\sum_{d|f}\Lambda(d) &= \Lambda(\pi_1) + \Lambda(\pi_1^2) + \cdots + \Lambda(\pi_1^{a_1}) \\
&\quad + \Lambda(\pi_2) + \Lambda(\pi_2^2) + \cdots + \Lambda(\pi_2^{a_2}) + \cdots + \Lambda(\pi_k) + \Lambda(\pi_k^2) + \cdots + \Lambda(\pi_k^{a_k}) \\
&= \underbrace{\log|\pi_1| + \log|\pi_1| + \cdots + \log|\pi_1|}_{a_1 \text{ términos}} \\
&\quad + \underbrace{\log|\pi_2| + \log|\pi_2| + \cdots + \log|\pi_2|}_{a_2 \text{ términos}} + \cdots + \underbrace{\log|\pi_k| + \log|\pi_k| + \cdots + \log|\pi_k|}_{a_k \text{ términos}} \\
&= \sum_{i=1}^{k} a_i \log|\pi_i| \\
&= \log|f|
\end{aligned}$$

por (2.7). Luego,

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

La segunda afirmación se sigue por una generalización apropiada de la inversión de Möbius.
Podemos dar una prueba directa de la siguiente manera:
Sea $f = \pi_1^{a_1}\pi_2^{a_2}\cdots\pi_k^{a_k}$ con π_i primo, para $1 \leqslant i \leqslant k$. Para evaluar el lado izquierdo es suficiente restringir la suma a divisores libres de cuadrados d. Expandiendo $\log|d|$ formalmente, tenemos

$$\begin{aligned}
\sum_{d|f}\mu(d)\log|d| &= \mu(\pi_1)\log|\pi_1| + \mu(\pi_2)\log|\pi_2| + \cdots + \mu(\pi_k)\log|\pi_k| \\
&\quad + \mu(\pi_1\pi_2)\log|\pi_1\pi_2| + \cdots + \mu(\pi_{k-1}\pi_k)\log|\pi_{k-1}\pi_k| + \cdots \\
&\quad + \mu(\pi_1\pi_2\cdots\pi_k)\log|\pi_1\pi_2\cdots\pi_k| \\
&= \mu(\pi_1)\log|\pi_1| + \mu(\pi_2)\log|\pi_2| + \cdots + \mu(\pi_k)\log|\pi_k| \\
&\quad + \mu(\pi_1\pi_2)\log|\pi_1| + \mu(\pi_1\pi_2)\log|\pi_2| + \cdots \\
&\quad + \mu(\pi_{k-1}\pi_k)\log|\pi_{k-1}| + \mu(\pi_{k-1}\pi_k)\log|\pi_k| + \cdots \\
&\quad + \mu(\pi_1\pi_2\cdots\pi_k)\log|\pi_1| + \mu(\pi_1\pi_2\cdots\pi_k)\log|\pi_2| + \cdots \\
&\quad + \mu(\pi_1\pi_2\cdots\pi_k)\log|\pi_k| \\
&= \log|\pi_1|(\mu(\pi_1) + \mu(\pi_1\pi_2) + \cdots + \mu(\pi_1\pi_2\cdots\pi_k)) \\
&\quad + \log|\pi_2|(\mu(\pi_2) + \mu(\pi_1\pi_2) + \cdots + \mu(\pi_1\pi_2\cdots\pi_k)) + \cdots \\
&\quad + \log|\pi_k|(\mu(\pi_k) + \mu(\pi_1\pi_k) + \cdots + \mu(\pi_1\pi_2\cdots\pi_k)) \\
&= \log|\pi_1|\left[(-1)^1 + (k-1)(-1)^2 + \cdots + \binom{k-1}{j-1}(-1)^j + \cdots + (-1)^k\right] \\
&\quad + \log|\pi_2|\left[(-1)^1 + (k-1)(-1)^2 + \cdots + \binom{k-1}{j-1}(-1)^j + \cdots + (-1)^k\right] + \cdots \\
&\quad + \log|\pi_k|\left[(-1)^1 + (k-1)(-1)^2 + \cdots + \binom{k-1}{j-1}(-1)^j + \cdots + (-1)^k\right]
\end{aligned}$$

$$
\begin{aligned}
&= \log|\pi_1| \sum_{j=1}^{k} (-1)^j \binom{k-1}{j-1} + \log|\pi_2| \sum_{j=1}^{k} (-1)^j \binom{k-1}{j-1} + \cdots \\
&\quad + \log|\pi_k| \sum_{j=1}^{k} (-1)^j \binom{k-1}{j-1} \\
&= \sum_{\pi|f} \log|\pi| \sum_{j=1}^{k} (-1)^j \binom{k-1}{j-1}
\end{aligned}
$$

donde π son los divisores primos de f distintos mutuamente, y k es el número de divisores primos de f distintos mutuamente. De esta manera,

$$\sum_{d|f} \mu(d) \log|d| = \sum_{\pi|f} \log|\pi| \sum_{j=1}^{k} (-1)^j \binom{k-1}{j-1}.$$

Si $k = 0$ de modo que $f = 1$, la suma de la derecha es vacía. Si $k = 1$, entonces $f = \pi_1^{a_1}$, y el lado derecho se evalúa como $-\log|\pi_1|$. Si $k \geqslant 2$, la suma interior es igual a $-(1-1)^{k-1} = 0$. A saber:

$$
\begin{aligned}
\sum_{j=1}^{k} (-1)^j \binom{k-1}{j-1} &= (-1)^1 \binom{k-1}{0} + (-1)^2 \binom{k-1}{1} + (-1)^3 \binom{k-1}{2} + \cdots \\
&\quad + (-1)^{k-1} \binom{k-1}{k-2} + (-1)^k \binom{k-1}{k-1} \\
&= (-1) \left[(-1)^0 \binom{k-1}{0} + (-1)^1 \binom{k-1}{1} + (-1)^2 \binom{k-1}{2} + \cdots \right. \\
&\quad \left. + (-1)^{k-2} \binom{k-1}{k-2} + (-1)^{k-1} \binom{k-1}{k-1} \right] \\
&= -\sum_{j=0}^{k-1} (-1)^j \binom{k-1}{j} \\
&= -(1-1)^{k-1} \\
&= 0
\end{aligned}
$$

si $k \geqslant 2$. Por lo tanto, en cualquier caso, el resultado se demuestra. ■

Afirmación 2.1. *La suma de los grados de todos los polinomios primos $\pi(t)$ en $\mathbb{F}_q[t]$ que dividen al entero positivo r es q^r. Esto es,*

$$\sum_{\deg(\pi(t))|r} \deg(\pi(t)) = q^r.$$

Demostración. Sea $r = p_1 p_2 \cdots p_k$ donde p_i son números primos, y sea $\nu_q(n)$ que denota el número de polinomios primos (irreducibles unitarios) de grado n, con $n \geqslant 1$. Entonces,

$$
\begin{aligned}
\sum_{\deg(\pi(t))|r} \deg(\pi(t)) &= 1 \cdot \nu_q(1) + p_1 \cdot \nu_q(p_1) + p_2 \cdot \nu_q(p_2) + \cdots + p_k \cdot \nu_q(p_k) + \sum_{P} P \nu_q(P) \\
&= \sum_{d|r} d \nu_q(d) \\
&= q^r
\end{aligned}
$$

por *Teorema 2.2*, donde P son los distintos productos que dividen a r y cuyos factores están en $\{p_1, p_2, \cdots, p_k\}$. ■

Lema 2.3. *Para $n \geqslant 0$,*

$$\psi(n) := \sum_{\deg f \leqslant n} \Lambda(f) = \left(\frac{q^{n+1}-q}{q-1}\right)\log q = O(q^n).$$

Observación 2.1. *Esta es otra forma del teorema del número primo para $\mathbb{F}_q[t]$. Aquí tenemos una fórmula exacta y simple para esta suma.*

Demostración.

$$\begin{aligned}\sum_{\deg f \leqslant n} \Lambda(f) &= \sum_{\substack{\deg f \leqslant n \\ f=\pi^k,\ k\geqslant 1}} \log|\pi| \\ &= \log q \sum_{\substack{k\deg\pi \leqslant n \\ k\geqslant 1}} \deg\pi\end{aligned}$$

pues $\deg \pi^k = k\deg\pi$.
Si $r = k\deg\pi$ con $k \geqslant 1$, entonces $1 \leqslant \deg\pi \leqslant r \leqslant n$. Por lo tanto, por *Afirmación 2.1*, tenemos

$$\begin{aligned}\psi(n) := \sum_{\deg f \leqslant n} \Lambda(f) &= \log q \sum_{\substack{k\deg\pi \leqslant n \\ k\geqslant 1}} \deg\pi \\ &= \log q \sum_{1\leqslant r\leqslant n} \sum_{k\deg\pi = r} \deg\pi \\ &= \log q \sum_{1\leqslant r\leqslant n} \sum_{\deg\pi \mid r} \deg\pi \\ &= \log q \sum_{1\leqslant r\leqslant n} q^r \\ &= \left[\frac{q(q^n-1)}{q-1}\right]\log q \\ &= \left(\frac{q^{n+1}-q}{q-1}\right)\log q.\end{aligned}$$

Por otro lado, como $\log q < q-1$, entonces

$$\left(\frac{q^{n+1}-q}{q-1}\right)\log q < q^{n+1}-q < q^{n+1} = qq^n.$$

Es decir,

$$\left(\frac{q^{n+1}-q}{q-1}\right)\log q = O(q^n).$$

Considerando los resultados anteriores, se sigue la igualdad deseada. ■

Lema 2.4. *Para $n \geqslant 0$,*

$$\begin{aligned}\sum_{\deg f \leqslant n} \frac{\Lambda(f)}{|f|} &= \sum_{\deg\pi\leqslant n} \frac{\log|\pi|}{|\pi|} + \sum_{2\deg\pi\leqslant n} \frac{\log|\pi|}{|\pi|^2} + \cdots \\ &= \sum_{\deg\pi\leqslant n} \frac{\log|\pi|}{|\pi|} + O(1).\end{aligned}$$

También,

$$\sum_{\deg \pi \leqslant n} \frac{\log|\pi|}{|\pi|} = \log(q^n) + O(1).$$

Demostración. La primera igualdad se sigue por la reordenación de la suma, al igual que cuando se prueba la afirmación análoga sobre $\mathbb{Z}$. De esta forma, tenemos

$$\sum_{\deg f \leqslant n} \frac{\Lambda(f)}{|f|} = \sum_{k \geqslant 1} \sum_{k \deg \pi \leqslant n} \frac{\log|\pi|}{|\pi|^k}.$$

Entonces,

$$\sum_{\deg f \leqslant n} \frac{\Lambda(f)}{|f|} - \sum_{\deg \pi \leqslant n} \frac{\log|\pi|}{|\pi|} = \sum_{2 \deg \pi \leqslant n} \frac{\log|\pi|}{|\pi|^2} + \sum_{3 \deg \pi \leqslant n} \frac{\log|\pi|}{|\pi|^3} + \cdots$$

Por otro lado,

$$\begin{aligned}
\sum_{k \geqslant 2} \sum_{2 \deg \pi \leqslant n} \frac{\log|\pi|}{|\pi|^k} &= \sum_{2 \deg \pi \leqslant n} \frac{\log|\pi|}{|\pi|^2} + \sum_{2 \deg \pi \leqslant n} \frac{\log|\pi|}{|\pi|^3} + \cdots \\
&= \sum_{2k \leqslant n} \sum_{\deg \pi = k} \frac{\log|\pi|}{|\pi|^2} + \sum_{2k \leqslant n} \sum_{\deg \pi = k} \frac{\log|\pi|}{|\pi|^3} + \cdots \\
&= \left(\sum_{\deg \pi = 1} \frac{\log|\pi|}{|\pi|^2} + \sum_{\deg \pi = 2} \frac{\log|\pi|}{|\pi|^2} + \cdots + \sum_{\deg \pi = [n/2]} \frac{\log|\pi|}{|\pi|^2} \right) \\
&\quad + \left(\sum_{\deg \pi = 1} \frac{\log|\pi|}{|\pi|^3} + \sum_{\deg \pi = 2} \frac{\log|\pi|}{|\pi|^3} + \cdots + \sum_{\deg \pi = [n/2]} \frac{\log|\pi|}{|\pi|^3} \right) + \cdots \\
&= \sum_{\deg \pi = 1} \log|\pi| \sum_{k \geqslant 2} \frac{1}{|\pi|^k} + \sum_{\deg \pi = 2} \log|\pi| \sum_{k \geqslant 2} \frac{1}{|\pi|^k} + \cdots \\
&\quad + \sum_{\deg \pi = [n/2]} \log|\pi| \sum_{k \geqslant 2} \frac{1}{|\pi|^k} \\
&= \sum_{2 \deg \pi \leqslant n} \log|\pi| \sum_{k \geqslant 2} \frac{1}{|\pi|^k} \\
&= \sum_{2 \deg \pi \leqslant n} \frac{\log|\pi|}{|\pi|(|\pi| - 1)},
\end{aligned}$$

ya que

$$\begin{aligned}
&\sum_{\deg \pi = l} \frac{\log|\pi|}{|\pi|^2} + \sum_{\deg \pi = l} \frac{\log|\pi|}{|\pi|^3} + \cdots \\
&= \left(\frac{\log|\pi_1|}{|\pi_1|^2} + \cdots + \frac{\log|\pi_{q^l}|}{|\pi_{q^l}|^2} \right) + \left(\frac{\log|\pi_1|}{|\pi_1|^3} + \cdots + \frac{\log|\pi_{q^l}|}{|\pi_{q^l}|^3} \right) + \cdots \\
&= \log|\pi_1| \left(\frac{1}{|\pi_1|^2} + \frac{1}{|\pi_1|^3} + \cdots \right) + \cdots + \log|\pi_{q^l}| \left(\frac{1}{|\pi_{q^l}|^2} + \frac{1}{|\pi_{q^l}|^3} + \cdots \right)
\end{aligned}$$

$$= \log|\pi_1| \sum_{k\geqslant 2} \frac{1}{|\pi_1|^k} + \cdots + \log|\pi_{q^l}| \sum_{k\geqslant 2} \frac{1}{|\pi_{q^l}|^k}$$
$$= \sum_{\deg \pi = l} \log|\pi| \sum_{k\geqslant 2} \frac{1}{|\pi|^k},$$

para $l \geqslant 1$, y también

$$\sum_{k\geqslant 2} \frac{1}{|\pi|^k} = \sum_{k\geqslant 1} \frac{1}{|\pi|^k} - \frac{1}{|\pi|} = \frac{1}{|\pi|-1} - \frac{1}{|\pi|} = \frac{1}{|\pi|(|\pi|-1)}.$$

Por consiguiente,

$$\sum_{k\geqslant 2} \sum_{2\deg\pi\leqslant n} \frac{\log|\pi|}{|\pi|^k} = \sum_{2\deg\pi\leqslant n} \frac{\log|\pi|}{|\pi|(|\pi|-1)}. \tag{2.8}$$

Para $k \geqslant 2$, note que

$$\frac{1}{q^k} + \frac{2}{q^{2k}} + \cdots + \frac{[n/k]}{q^{[n/k]k}} \leqslant \frac{1}{q^k} + \frac{2}{q^{2k}} + \cdots + \frac{[n/k]}{q^{[n/k]k}} + \cdots + \frac{[n/2]}{q^{[n/2]k}}.$$

Por tanto,

$$\sum_{kr\leqslant n} \frac{r}{q^{kr}} \leqslant \sum_{2r\leqslant n} \frac{r}{q^{kr}}.$$

Entonces, tomando $r = \deg\pi$ y multiplicando ambos lados de la desigualdad anterior por $\log q$, se tiene

$$\sum_{k\deg\pi\leqslant n} \frac{\log|\pi|}{|\pi|^k} \leqslant \sum_{2\deg\pi\leqslant n} \frac{\log|\pi|}{|\pi|^k}, \text{ para } k \geqslant 2.$$

Lo anterior implica que

$$\sum_{2\deg\pi\leqslant n} \frac{\log|\pi|}{|\pi|^2} + \sum_{3\deg\pi\leqslant n} \frac{\log|\pi|}{|\pi|^3} + \cdots \leqslant \sum_{2\deg\pi\leqslant n} \frac{\log|\pi|}{|\pi|^2} + \sum_{2\deg\pi\leqslant n} \frac{\log|\pi|}{|\pi|^3} + \cdots$$

Es decir,

$$\sum_{k\geqslant 2} \sum_{k\deg\pi\leqslant n} \frac{\log|\pi|}{|\pi|^k} \leqslant \sum_{k\geqslant 2} \sum_{2\deg\pi\leqslant n} \frac{\log|\pi|}{|\pi|^k}.$$

Luego, de (2.8), tenemos

$$\sum_{\deg f\leqslant n} \frac{\Lambda(f)}{|f|} - \sum_{\deg\pi\leqslant n} \frac{\log|\pi|}{|\pi|} \leqslant \sum_{k\geqslant 2} \sum_{2\deg\pi\leqslant n} \frac{\log|\pi|}{|\pi|^k}$$
$$= \sum_{2\deg\pi\leqslant n} \frac{\log|\pi|}{|\pi|(|\pi|-1)}.$$

Por otro lado, como $q^k \geqslant q \geqslant 2$ para $k \geqslant 1$, entonces $2q^k \leqslant q^{2k}$. Por lo tanto,

$$q^{2k} + 2q^k \leqslant 2q^{2k}.$$

De esta manera $q^{2k} \leqslant 2(q^{2k} - q^k)$, o

$$\frac{1}{q^{2k} - q^k} \leqslant \frac{2}{q^{2k}}.$$

Por consiguiente,

$$\frac{k\log q}{q^k(q^k-1)} \leqslant 2kq^{-2k}\log q.$$

Si $k = \deg \pi$, tenemos

$$\frac{\log|\pi|}{|\pi|(|\pi|-1)} \leqslant 2(\deg\pi)q^{-2\deg\pi}\log q.$$

Como consecuencia,

$$\begin{aligned}\sum_{2\deg\pi\leqslant n}\frac{\log|\pi|}{|\pi|(|\pi|-1)} &\leqslant 2\log q\sum_{2\deg\pi\leqslant n} q^{-2\deg\pi}\deg\pi\\ &= 2\log q\sum_{2k\leqslant n}\sum_{\deg\pi=k} q^{-2\deg\pi}\deg\pi\\ &= 2\log q\sum_{2k\leqslant n} kq^{-2k}\sum_{\deg\pi=k}1\\ &= 2\log q\sum_{2k\leqslant n} kq^{-k}.\end{aligned}$$

Para $q \geqslant 2$,

$$\sum_k kq^{-k} \leqslant \sum_k k2^{-k}.$$

Además, note que

$$\lim_{n\to\infty}\frac{(n+1)2^{-(n+1)}}{n2^{-n}} = \frac{1}{2}\lim_{n\to\infty}\left(1+\frac{1}{n}\right) = \frac{1}{2} < 1.$$

Por lo tanto, la serie

$$\sum_k kq^{-k}$$

es convergente. Entonces,

$$\sum_{\deg f\leqslant n}\frac{\Lambda(f)}{|f|} - \sum_{\deg\pi\leqslant n}\frac{\log|\pi|}{|\pi|} \leqslant 2\log q\sum_{2k\leqslant n} kq^{-k} < 2\log q\cdot M$$

Pues, al ser la serie convergente, su sucesión de sumas parciales está acotada. Es decir, existe $M > 0$ tal que

$$\sum_{2k\leqslant n} kq^{-k} < M.$$

De la cual se concluye

$$\sum_{\deg f\leqslant n}\frac{\Lambda(f)}{|f|} - \sum_{\deg\pi\leqslant n}\frac{\log|\pi|}{|\pi|} = O(1),\ \text{o}\ \sum_{\deg f\leqslant n}\frac{\Lambda(f)}{|f|} = \sum_{\deg\pi\leqslant n}\frac{\log|\pi|}{|\pi|} + O(1).$$

Finalmente, puesto que

$$\begin{aligned}\sum_{\deg f\leqslant k}\Lambda(f) &= \sum_{\deg f=1}\Lambda(f) + \sum_{\deg f=2}\Lambda(f) + \cdots + \sum_{\deg f=k-1}\Lambda(f) + \sum_{\deg f=k}\Lambda(f)\\ &= \sum_{\deg f\leqslant k-1}\Lambda(f) + \sum_{\deg f=k}\Lambda(f),\end{aligned}$$

entonces,

$$\begin{aligned}\sum_{\deg f=k}\Lambda(f) &= \sum_{\deg f\leqslant k}\Lambda(f) - \sum_{\deg f\leqslant k-1}\Lambda(f)\\ &= \psi(k)-\psi(k-1).\end{aligned}$$

De esta manera, se tiene

$$\sum_{\deg f\leqslant n}\frac{\Lambda(f)}{|f|} = \sum_{k=1}^{n}\sum_{\deg f=k}\frac{\Lambda(f)}{|f|} = \sum_{k=1}^{n}q^{-k}\sum_{\deg f=k}\Lambda(f) = \sum_{k=1}^{n}[\psi(k)-\psi(k-1)]q^{-k}.$$

Por la prueba del *Lema 2.3*, $\psi(k)-\psi(k-1) = q^k\log q$, cuando $k\geqslant 1$, por tanto,

$$\begin{aligned}\sum_{\deg f\leqslant n}\frac{\Lambda(f)}{|f|} &= \sum_{k=1}^{n}[\psi(k)-\psi(k-1)]q^{-k}\\ &= \sum_{k=1}^{n}q^kq^{-k}\log q\\ &= \log q\sum_{k=1}^{n}1\\ &= n\log q = \log(q^n).\end{aligned}$$

Refiriéndonos a la primera parte del lema, tenemos

$$\sum_{\deg \pi\leqslant n}\frac{\log|\pi|}{|\pi|} = \log(q^n)+O(1).$$

■

2.2. Caracteres y Series-L.

Definición 2.1. *Sea $s=\sigma+i\gamma$ un número complejo. Para un carácter no principal χ módulo $m(t)$, con $m(t)\in\mathbb{F}_q[t]$, definamos*

$$L(s,\chi) = \sum_{f\in M(q;t)}\frac{\chi(f)}{|f|^s} \tag{2.9}$$

como la función L asociada a χ.

Definición 2.2. *Para un carácter no principal χ módulo $m(t)$, con $m(t)\in\mathbb{F}_q[t]$, coloquemos*

$$L(\chi) = \sum_{k=0}^{\infty}\sum_{\deg f=k}\frac{\chi(f)}{|f|} = \sum_{k=0}^{\infty}\frac{c_k}{q^k}, \tag{2.10}$$

donde $c_k = \sum_{\deg f=k}\chi(f)$.

Aparentemente, la suma anterior es infinita. Sin embargo, más adelante vamos a demostrar que cuando $k\geqslant\deg m$, $c_k=0$, de manera que en la definición de $L(\chi)$ sólo necesitamos la suma hasta $k=\deg m-1$.

Proposición 2.1. *Para cualquier carácter χ módulo m sobre $\mathbb{F}_q[t]$, la serie*

$$L(s,\chi) = \sum_{f\in M(q;t)} \frac{\chi(f)}{|f|^s}$$

es absolutamente convergente para $\sigma = \Re(s) > 1$.

Demostración. Tomemos $\sigma = \Re(s) > 1$. Como $|f| = q^k$, donde $k = \deg f$, y existen q^k polinomios mónicos de grado k, tenemos, para todo $k = 0, 1, 2, \cdots$, lo siguiente

$$\begin{aligned}
\left| \sum_{\substack{f\in M(q;t)\\ \deg f=k}} \chi(f)|f|^{-s} \right| &\leqslant \sum_{\substack{f\in M(q;t)\\ \deg f=k}} |\chi(f)|f|^{-s}| \\
&= q^{-k\sigma} \sum_{\substack{f\in M(q;t)\\ \deg f=k}} |\chi(f)||q^{-ik\gamma}| \\
&\leqslant q^{-k\sigma} \sum_{\substack{f\in M(q;t)\\ \deg f=k}} 1 \\
&= q^{-k\sigma} q^k \\
&= q^{k(1-\sigma)},
\end{aligned}$$

pues $|q^{ik\gamma}| = |e^{ik\gamma \log q}| = 1$. Luego,

$$\begin{aligned}
\sum_{\deg f\leqslant r} |\chi(f)|f|^{-s}| &= \sum_{k=0}^{r} \sum_{\substack{f\in M(q;t)\\ k=\deg f}} |\chi(f)|f|^{-s}| \\
&= \sum_{k=0}^{r} q^{-k\sigma} \sum_{\substack{f\in M(q;t)\\ \deg f=k}} |\chi(f)| \\
&\leqslant \sum_{k=0}^{r} q^{-k\sigma} \sum_{\substack{f\in M(q;t)\\ \deg f=k}} 1 \\
&= \sum_{k=0}^{r} q^{k(1-\sigma)} \\
&= 1 + \sum_{k=1}^{r} q^{k(1-\sigma)} \\
&= 1 + q^{1-\sigma} \frac{(q^{r(1-\sigma)} - 1)}{q^{1-\sigma} - 1} \\
&= \frac{1 - q^{(1-\sigma)(1+r)}}{1 - q^{1-\sigma}}.
\end{aligned}$$

Por lo tanto,

$$\sum_{\deg f\leqslant r} |\chi(f)|f|^{-s}| \to \frac{1}{1 - q^{1-\sigma}}, \text{ cuando } r \to \infty,$$

pues $\sigma > 1$. ■

Proposición 2.2. *Para todo $\chi \neq \chi_o$ módulo $m(t)$, con $m(t) \in \mathbb{F}_q[t]$, se tiene*

(i). $c_k = 0$, *para todo* $k \geqslant \deg m$, *donde* $c_k = \sum_{\deg f = k} \chi(f)$.

(ii). $L(s,\chi) = \sum_{k=0}^{\deg m - 1} c_k q^{-ks}$.

Demostración.

(i). Sabemos que hay exactamente $q^{\deg m}$ clases módulo m. Éstos representantes, $r_1(t), \cdots, r_{q^{\deg m}}(t)$, pueden tomarse en $M(q;t)$ y todos de grado menor o igual a $\deg m$.
Si $f \in M(q;t)$, existe $Q \in M(q;t)$ tal que $f = mQ + r_n$, donde podemos asumir $r_n = 0$ o $\deg r_n < \deg m$. Cuando $k \geqslant \deg m$, los polinomios f de grado k son exactamente los polinomios $f = mQ + r_n$, donde $Q \in M(q;t)$ es mónico de grado $\deg f - \deg m$, pues

$$\deg f = \text{máx}\{\deg m + \deg Q, \deg r_n\} = \deg m + \deg Q$$

ya que, $\deg r_n < \deg m + \deg Q$.
Por tanto, hay $q^{\deg f - \deg m}$ de tales polinomios para cada clase residual módulo m. Es decir, congruentes con cada $r_n(t)$ hay exactamente $q^{\deg f - \deg m}$ polinomios de grado k. En consecuencia,

$$c_k = \sum_{\deg f = k} \chi(f) = q^{\deg f - \deg m} \sum_{r_n(t) \text{ mód } m(t)} \chi(r_n(t)) = 0$$

en virtud del *Lema 1.2*, tomando $\psi = \chi_o$, porque $\chi \neq \chi_o$.

(ii). Como $L(s,\chi)$ es absolutamente convergente, tenemos

$$\begin{aligned}
L(s,\chi) &= \sum_{k=0}^{\infty} \sum_{\deg f = k} \frac{\chi(f)}{|f|^s} \\
&= \sum_{k=0}^{\infty} \left(\sum_{\deg f = k} \chi(f) \right) \frac{1}{|f|^s} \\
&= \sum_{k=0}^{\infty} c_k \frac{1}{|f|^s} \\
&= \sum_{k=0}^{\infty} c_k \frac{1}{q^{s \deg f}} \\
&= \sum_{k=0}^{\infty} c_k \frac{1}{q^{ks}} \\
&= \sum_{k=0}^{\deg m - 1} c_k q^{-ks}.
\end{aligned}$$

■

Ahora, podemos establecer la no anulación de $L(\chi)$ para χ real no principal.
Considerando que la próxima afirmación es uno de los pasos más difíciles de la prueba del teorema de *Dirichlet* sobre $\mathbb{Z}$, aquí se trabaja un argumento bastante sencillo.

Teorema 2.3. *Si* $\chi \neq \chi_o$ *es un carácter de Dirichlet real módulo* m, *entonces* $L(\chi) \neq 0$.

Demostración. Definamos $F(f) := \sum_{d|f} \chi(d)$ la cual es una función multiplicativa, pues χ es una función multiplicativa. Si $f = \pi_1^{a_1}\pi_2^{a_2}\cdots\pi_k^{a_k}$ es la factorización de f en irreducibles mónicos,

$$F(f) = \prod_{1\leqslant j\leqslant k} F(\pi_j^{a_j}).$$

A saber,

$$\begin{aligned}
F(f) &= \sum_{d|f} \chi(d) \\
&= (\chi(1) + \chi(\pi_1) + \chi(\pi_1^2) + \cdots + \chi(\pi_1^{a_1})) + (\chi(\pi_2) + \chi(\pi_2^2) + \cdots + \chi(\pi_2^{a_2})) \\
&\quad + \cdots + (\chi(\pi_k) + \chi(\pi_k^2) + \cdots + \chi(\pi_k^{a_k})) \\
&\quad + \chi(\pi_1\pi_2) + \cdots + \chi(\pi_{k-1}\pi_k) + \chi(\pi_1\pi_2^2) + \cdots + \chi(\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_k^{a_k}) \\
&= (\chi(1) + \chi(\pi_1) + \cdots + \chi(\pi_1^{a_1}))(\chi(1) + \chi(\pi_2) + \cdots + \chi(\pi_2^{a_2}))\cdots \\
&\quad (\chi(1) + \chi(\pi_k) + \cdots + \chi(\pi_k^{a_k})) \\
&= \sum_{d|\pi_1^{a_1}} \chi(d) \cdot \sum_{d|\pi_2^{a_2}} \chi(d) \cdots \sum_{d|\pi_k^{a_k}} \chi(d) \\
&= F(\pi_1^{a_1}) \cdot F(\pi_2^{a_2}) \cdots F(\pi_k^{a_k}) \\
&= \prod_{1\leqslant j\leqslant k} F(\pi_j^{a_j}).
\end{aligned}$$

Como χ es real, tenemos: si $\chi(\pi) = 0$, entonces $F(\pi^l) = \chi(1) = 1$; si $\chi(\pi) = 1$, entonces

$$\begin{aligned}
F(\pi^l) = \sum_{d|\pi^l} \chi(d) &= \chi(1) + \chi(\pi) + \chi(\pi^2) + \cdots + \chi(\pi^l) \\
&= 1 + \underbrace{1 + \cdots + 1}_{l \text{ veces}} \\
&= 1 + l.
\end{aligned}$$

Finalmente, sea $\chi(\pi) = -1$. Como

$$\begin{aligned}
F(\pi^l) = \sum_{d|\pi^l} \chi(d) &= \chi(1) + \chi(\pi) + \chi(\pi^2) + \cdots + \chi(\pi^l) \\
&= 1 + (-1) + (-1)^2 + \cdots + (-1)^l
\end{aligned}$$

y, además,

$$\sum_{i=0}^{l} (-1)^i = \frac{(-1)^l + 1}{2} = \begin{cases} 0, & \text{si } l \text{ es impar} \\ 1, & \text{si } l \text{ es par} \end{cases},$$

concluimos que

$$F(\pi^l) = \begin{cases} 0, & \text{si } l \text{ es impar} \\ 1, & \text{si } l \text{ es par} \end{cases}.$$

Por lo tanto, siempre se tiene $F(\pi^l) \geqslant 0$, con $F(\pi^l) \geqslant 1$ si l es par. Consecuentemente, siempre se tiene $F(f) \geqslant 0$, y en particular, $F(f) \geqslant 1$ si f es un cuadrado (es decir, f es de la forma π^{2i}, con $i = 0, 1, \cdots$). En la siguiente prueba usaremos la notación $f = \blacksquare$ para indicar que f es el cuadrado de un polinomio.

Para un número natural z, definamos $S(z) := \sum_{\deg f \leqslant z} F(f)$. Entonces,

$$\begin{aligned}
S(z) &= \sum_{\deg f \leqslant z} F(f) \\
&= \sum_{\deg f=0} F(f) + \sum_{\deg f=1} F(f) + \sum_{\deg f=2} F(f) + \cdots + \sum_{\deg f=z} F(f) \\
&\geqslant \sum_{\deg f=0} F(f) + \sum_{\deg f=2} F(f) + \cdots + \sum_{\deg f=2i} F(f),\ 0 \leqslant 2i \leqslant z \\
&\geqslant \sum_{\substack{\deg f=0 \\ f=\blacksquare}} F(f) + \sum_{\substack{\deg f=2 \\ f=\blacksquare}} F(f) + \cdots + \sum_{\substack{\deg f=2i \\ f=\blacksquare}} F(f),\ 0 \leqslant 2i \leqslant z \\
&= \sum_{\substack{\deg f \leqslant z \\ f=\blacksquare}} F(f) \\
&\geqslant \sum_{\substack{\deg f \leqslant z \\ f=g^2}} F(f) \\
&= \sum_{2\deg g \leqslant z} F(g^2) \\
&\geqslant \sum_{\deg g \leqslant z/2} 1 \qquad (2.11) \\
&= \sum_{k \leqslant z/2} \sum_{k=\deg g} 1 = \sum_{0 \leqslant k \leqslant z/2} q^k.
\end{aligned}$$

Note que si g es un unitario no irreducible, la relación (2.11) se cumple, pues $g = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, entonces $F(g^2) = F(p_1^{2a_1}) F(p_2^{2a_2}) \cdots F(p_r^{2a_r}) \geqslant 1$.
Por lo tanto, $S(z) \geqslant \sum_{0 \leqslant k \leqslant z/2} q^k$. Lo cual implica que

$$S(z) \to \infty \text{ cuando } z \to \infty. \qquad (2.12)$$

Por otro lado,

$$\begin{aligned}
S(z) &= \sum_{\deg f \leqslant z} F(f) = \sum_{\deg f \leqslant z} \sum_{d|f} \chi(d) \\
&= \sum_{\deg f=0} \sum_{d|f} \chi(d) + \sum_{\deg f=1} \sum_{d|f} \chi(d) + \cdots + \sum_{\deg f=z-1} \sum_{d|f} \chi(d) + \sum_{\deg f=z} \sum_{d|f} \chi(d) \\
&= \underbrace{\sum_{\substack{d|f \\ \deg d=0}} \chi(d)}_{\deg f=0} + \underbrace{\sum_{\substack{d|f \\ \deg d=0}} \chi(d) + \sum_{\substack{d|f \\ \deg d=1}} \chi(d)}_{\deg f=1} + \cdots \\
&\quad + \underbrace{\sum_{\substack{d|f \\ \deg d=0}} \chi(d) + \sum_{\substack{d|f \\ \deg d=1}} \chi(d) + \cdots + \sum_{\substack{d|f \\ \deg d=z-1}} \chi(d)}_{\deg f=z-1}
\end{aligned}$$

$$
\begin{aligned}
&+ \underbrace{\sum_{\substack{d|f\\ \deg d=0}} \chi(d) + \sum_{\substack{d|f\\ \deg d=1}} \chi(d) + \cdots + \sum_{\substack{d|f\\ \deg d=z-1}} \chi(d) + \sum_{\substack{d|f\\ \deg d=z}} \chi(d)}_{\deg f=z} \\
&= \underbrace{\sum_{\substack{d|f\\ \deg f=0}} \chi(d) + \cdots + \sum_{\substack{d|f\\ \deg f=z}} \chi(d)}_{\deg d=0,\ \text{hay } z+1 \text{ términos}} + \underbrace{\sum_{\substack{d|f\\ \deg f=1}} \chi(d) + \cdots + \sum_{\substack{d|f\\ \deg f=z}} \chi(d)}_{\deg d=1,\ \text{hay } z \text{ términos}} + \cdots \\
&\quad + \underbrace{\sum_{\substack{d|f\\ \deg f=z-1}} \chi(d) + \sum_{\substack{d|f\\ \deg f=z}} \chi(d)}_{\deg d=z-1,\ \text{hay } z-(z-2) \text{ términos}} + \underbrace{\sum_{\substack{d|f\\ \deg f=z}} \chi(d)}_{\deg d=z,\ \text{hay } z-(z-1) \text{ términos}} \\
&= \chi(d)|_{\deg d=0} \sum_{\substack{d|f\\ 0\leqslant \deg f\leqslant z}} 1 + \chi(d)|_{\deg d=1} \sum_{\substack{d|f\\ 1\leqslant \deg f\leqslant z}} 1 + \cdots \\
&\quad + \chi(d)|_{\deg d=z-1} \sum_{\substack{d|f\\ z-1\leqslant \deg f\leqslant z}} 1 + \chi(d)|_{\deg d=z} \sum_{\substack{d|f\\ \deg f=z}} 1 \\
&= \chi(d)|_{\deg d=0} \sum_{\substack{Ed=f\\ \deg E\leqslant z-0}} 1 + \chi(d)|_{\deg d=1} \sum_{\substack{Ed=f\\ \deg E\leqslant z-1}} 1 + \cdots \\
&\quad + \chi(d)|_{\deg d=z-1} \sum_{\substack{Ed=f\\ \deg E\leqslant z-(z-1)}} 1 + \chi(d)|_{\deg d=z} \sum_{\substack{Ed=f\\ \deg E\leqslant z-z}} 1 \\
&= \sum_{\deg d\leqslant z} \chi(d) \sum_{\substack{Ed=f\\ \deg E\leqslant z-\deg d}} 1.
\end{aligned}
$$

Por consiguiente,

$$S(z) = \sum_{\deg f\leqslant z} F(f) = \sum_{\deg d\leqslant z} \chi(d) \sum_{\substack{Ed=f\\ \deg E\leqslant z-\deg d}} 1.$$

Luego, para $z \geqslant \deg m - 1$,

$$
\begin{aligned}
S(z) &= \sum_{\deg d\leqslant z} \chi(d) \sum_{\substack{Ed=f\\ \deg E\leqslant z-\deg d}} 1 \\
&= \sum_{k=0}^{z} \sum_{k=\deg d} \chi(d) \sum_{l=0}^{z-k} \sum_{l=\deg E} 1 \\
&= \sum_{k=0}^{z} c_k \sum_{l=0}^{z-k} q^l \\
&= \sum_{k=0}^{\deg m-1} c_k \left(\frac{q^{z-k+1}-1}{q-1} \right) \\
&= \frac{q^{z+1}}{q-1} L(\chi) + c,
\end{aligned}
$$

donde $c = -\dfrac{1}{q-1} \displaystyle\sum_{k=0}^{\deg m-1} c_k$ es constante. De esta manera, si $L(\chi) = 0$, $S(z) = c$ para $z \geqslant \deg m - 1$,

contradiciendo lo probado en (2.12). Esta contradicción completa la prueba. ■

Ahora, estamos listos para movernos al corazón del argumento: Estudiaremos las funciones $A_\chi(n) := \sum_{\deg f \leqslant n} \chi(f)\Lambda(f)/|f|$.

Teorema 2.4. *Para $n \geqslant 0$, $A_{\chi_o}(n) = \log(q^n) + O(1)$.*

Demostración. Note que, si $(g^k, m) = 1$, para $k \geqslant 1$, con g y m en $M(q;T)$, entonces $(g,m) = 1$. Suponga que $(g,m) = d \neq 1$. Entonces, $d|g$ y $d|m$. Por lo tanto, $g = dh$, lo que implica que $g^k = dhg^{k-1}$, es decir, $d|g^k$. Como d es unitario, entonces, $\deg d \geqslant 1$. Si $(g^k, m) = c$, entonces, $(g^k, m) \neq 1$, tomando $c = d$, de lo contrario, también se llega a la misma conclusión, pues $1 \leqslant \deg d \leqslant \deg c$. De lo anterior, se tiene

$$\begin{aligned} A_{\chi_o}(n) &= \sum_{\substack{\deg f \leqslant n \\ (f,m)=1}} \frac{\Lambda(f)}{|f|} \\ &= \sum_{\substack{k \deg \pi \leqslant n \\ (\pi^k, m)=1}} \frac{\log|\pi|}{|\pi|^k} \\ &= \sum_{\substack{k \deg \pi \leqslant n \\ \pi \nmid m}} \frac{\log|\pi|}{|\pi|^k} \\ &= \sum_{\substack{\deg \pi \leqslant n \\ \pi \nmid m}} \frac{\log|\pi|}{|\pi|} + R(n), \end{aligned}$$

donde

$$R(n) := \sum_{\substack{2 \deg \pi \leqslant n \\ \pi \nmid m}} \frac{\log|\pi|}{|\pi|^2} + \sum_{\substack{3 \deg \pi \leqslant n \\ \pi \nmid m}} \frac{\log|\pi|}{|\pi|^3} + \cdots .$$

Por otro lado, como

$$\sum_{k \deg \pi \leqslant n} \frac{\log|\pi|}{|\pi|^k} = \sum_{\substack{k \deg \pi \leqslant n \\ \pi | m}} \frac{\log|\pi|}{|\pi|^k} + \sum_{\substack{k \deg \pi \leqslant n \\ \pi \nmid m}} \frac{\log|\pi|}{|\pi|^k} \geqslant \sum_{\substack{k \deg \pi \leqslant n \\ \pi \nmid m}} \frac{\log|\pi|}{|\pi|^k},$$

para $k \geqslant 2$, entonces

$$\begin{aligned} R(n) &\leqslant \sum_{2 \deg \pi \leqslant n} \frac{\log|\pi|}{|\pi|^2} + \sum_{3 \deg \pi \leqslant n} \frac{\log|\pi|}{|\pi|^3} + \cdots \\ &= \sum_{\deg f \leqslant n} \frac{\Lambda(f)}{|f|} - \sum_{\deg \pi \leqslant n} \frac{\log|\pi|}{|\pi|} \ll 1, \end{aligned}$$

con la ayuda de la prueba del *Lema 2.4*. Por lo tanto,

$$A_{\chi_o}(n) = \sum_{\substack{\deg \pi \leqslant n \\ \pi \nmid m}} \frac{\log|\pi|}{|\pi|} + O(1) = \sum_{\deg \pi \leqslant n} \frac{\log|\pi|}{|\pi|} + O(1) = \log(q^n) + O(1),$$

por las propiedades de O-grande, y por el *Lema 2.4*. ■

El resto de esta sección está dedicada a mostrar que para $\chi \neq \chi_o$, $A_\chi(n) = O(1)$. El *Teorema 2.1* se seguirá de este resultado, del *Teorema 2.4* y las relaciones de ortogonalidad.

Lema 2.5. *Sea χ un carácter no principal. Para $n \geqslant 0$,*

$$L(\chi) - \sum_{k=0}^{n} \frac{c_k}{q^k} = O(q^{-n}).$$

Demostración. Como se demostró anteriormente, la función de la izquierda se anula para $k \geqslant \deg m$. También se anula para $n \geqslant \deg m - 1$. A saber,

$$L(\chi) = \sum_{k=0}^{\deg m - 1} \frac{c_k}{q^k} + \sum_{k=\deg m}^{\infty} \frac{c_k}{q^k} = \sum_{k=0}^{\deg m - 1} \frac{c_k}{q^k}$$

por la parte *(i)* de la *Proposición 2.2*, por lo cual, tenemos

$$L(\chi) - \sum_{k=0}^{\deg m - 1} \frac{c_k}{q^k} = 0.$$

De tal forma que la conclusión es inmediata. Por otro lado, suponga que $n \leqslant \deg m - 2$. Note que

$$\left| L(\chi) - \sum_{k=0}^{n} \frac{c_k}{q^k} \right| \leqslant \max_{0 \leqslant l \leqslant \deg m - 2} \left| L(\chi) - \sum_{k=0}^{l} \frac{c_k}{q^k} \right|.$$

Además, $1 = q^0 \leqslant q^{\deg m - 2 - n} = q^{\deg m - 2} q^{-n}$. Entonces,

$$\left| L(\chi) - \sum_{k=0}^{n} \frac{c_k}{q^k} \right| \leqslant q^{\deg m - 2} \max_{0 \leqslant l \leqslant \deg m - 2} \left| L(\chi) - \sum_{k=0}^{l} \frac{c_k}{q^k} \right| q^{-n}.$$

Por lo tanto, un valor adecuado para la constante implícita es

$$q^{\deg m - 2} \max_{0 \leqslant l \leqslant \deg m - 2} \left| L(\chi) - \sum_{k=0}^{l} \frac{c_k}{q^k} \right|.$$

por lo que podemos concluir

$$L(\chi) - \sum_{k=0}^{n} \frac{c_k}{q^k} = O(q^{-n}).$$

■

Lema 2.6. *Sea χ un carácter no principal. Para $n \geqslant 0$,*

$$L(\chi) \sum_{\deg f \leqslant n} \frac{\chi(f)\Lambda(f)}{|f|} = O(1).$$

Demostración. Por el *Lema 2.2*,

$$\sum_{\deg f \leqslant n} \frac{\chi(f) \log |f|}{|f|} = \sum_{\deg f \leqslant n} \frac{\chi(f)}{|f|} \sum_{d \mid f} \Lambda(d).$$

Además,

$$\begin{aligned}
&\sum_{\deg f\leqslant n}\frac{\chi(f)}{|f|}\sum_{d|f}\Lambda(d)\\
&=\sum_{\deg f=0}\frac{\chi(f)}{|f|}\sum_{d|f}\Lambda(d)+\sum_{\deg f=1}\frac{\chi(f)}{|f|}\sum_{d|f}\Lambda(d)+\cdots\\
&\quad+\sum_{\deg f=n-1}\frac{\chi(f)}{|f|}\sum_{d|f}\Lambda(d)+\sum_{\deg f=n}\frac{\chi(f)}{|f|}\sum_{d|f}\Lambda(d)\\
&=\left[\sum_{\deg f=0}\frac{\chi(f)}{|f|}+\sum_{\deg f=1}\frac{\chi(f)}{|f|}+\cdots+\sum_{\deg f=n-1}\frac{\chi(f)}{|f|}+\sum_{\deg f=n}\frac{\chi(f)}{|f|}\right]\sum_{\substack{d|f\\ \deg d=0}}\Lambda(d)\\
&\quad+\left[\sum_{\deg f=1}\frac{\chi(f)}{|f|}+\cdots+\sum_{\deg f=n-1}\frac{\chi(f)}{|f|}+\sum_{\deg f=n}\frac{\chi(f)}{|f|}\right]\sum_{\substack{d|f\\ \deg d=1}}\Lambda(d)+\cdots\\
&\quad+\left[\sum_{\deg f=n-1}\frac{\chi(f)}{|f|}+\sum_{\deg f=n}\frac{\chi(f)}{|f|}\right]\sum_{\substack{d|f\\ \deg d=n-1}}\Lambda(d)+\sum_{\deg f=n}\frac{\chi(f)}{|f|}\sum_{\substack{d|f\\ \deg d=n}}\Lambda(d)\\
&=\sum_{0\leqslant\deg f\leqslant n}\frac{\chi(f)}{|f|}\sum_{\substack{d|f\\ \deg d=0}}\Lambda(d)+\sum_{1\leqslant\deg f\leqslant n}\frac{\chi(f)}{|f|}\sum_{\substack{d|f\\ \deg d=1}}\Lambda(d)+\cdots\\
&\quad+\sum_{n-1\leqslant\deg f\leqslant n}\frac{\chi(f)}{|f|}\sum_{\substack{d|f\\ \deg d=n-1}}\Lambda(d)+\sum_{\deg f=n}\frac{\chi(f)}{|f|}\sum_{\substack{d|f\\ \deg d=n}}\Lambda(d)\\
&=\sum_{\deg d=0}\frac{\chi(d)\Lambda(d)}{|d|}\sum_{\deg E\leqslant n-0}\frac{\chi(E)}{|E|}+\sum_{\deg d=1}\frac{\chi(d)\Lambda(d)}{|d|}\sum_{\deg E\leqslant n-1}\frac{\chi(E)}{|E|}+\cdots\\
&\quad+\sum_{\deg d=n-1}\frac{\chi(d)\Lambda(d)}{|d|}\sum_{\deg E\leqslant n-(n-1)}\frac{\chi(E)}{|E|}+\sum_{\deg d=n}\frac{\chi(d)\Lambda(d)}{|d|}\sum_{\deg E\leqslant n-n}\frac{\chi(E)}{|E|}\\
&=\sum_{\deg d\leqslant n}\frac{\chi(d)\Lambda(d)}{|d|}\sum_{\deg E\leqslant n-\deg d}\frac{\chi(E)}{|E|},
\end{aligned}$$

puesto que, para $f=Ed$, $i\leqslant j$ con $0\leqslant i,j\leqslant n$, se tiene

$$\begin{aligned}
\sum_{i\leqslant\deg f\leqslant j}\frac{\chi(f)}{|f|}\sum_{\substack{d|f\\ \deg d=i}}\Lambda(d)&=\sum_{i\leqslant\deg f\leqslant j}\sum_{\substack{d|f\\ \deg d=i}}\frac{\chi(f)}{|f|}\Lambda(d)\\
&=\sum_{\deg E\leqslant j-i}\sum_{d:\ \deg d=i}\frac{\chi(E)\chi(d)}{|E||d|}\Lambda(d)\\
&=\sum_{d:\ \deg d=i}\sum_{\deg E\leqslant j-i}\frac{\chi(d)\Lambda(d)}{|d|}\frac{\chi(E)}{|E|}\\
&=\sum_{d:\ \deg d=i}\frac{\chi(d)\Lambda(d)}{|d|}\sum_{\deg E\leqslant j-i}\frac{\chi(E)}{|E|}.
\end{aligned}$$

Entonces,

$$\sum_{\deg f\leqslant n}\frac{\chi(f)}{|f|}\sum_{d|f}\Lambda(d)=\sum_{\deg d\leqslant n}\frac{\chi(d)\Lambda(d)}{|d|}\sum_{\deg E\leqslant n-\deg d}\frac{\chi(E)}{|E|}, \tag{2.13}$$

donde $f=Ed$.
Ahora, por el *Lema 2.5*,

$$L(\chi)-\sum_{\deg E\leqslant n-\deg d}\frac{\chi(E)}{|E|}=O(q^{\deg d-n}),$$

es decir,

$$\sum_{\deg E\leqslant n-\deg d}\frac{\chi(E)}{|E|}=L(\chi)-O(q^{\deg d-n}).$$

Por lo tanto,

$$\frac{\chi(d)\Lambda(d)}{|d|}\sum_{\deg E\leqslant n-\deg d}\frac{\chi(E)}{|E|}=L(\chi)\frac{\chi(d)\Lambda(d)}{|d|}-\frac{\chi(d)\Lambda(d)}{|d|}O(q^{\deg d-n}).$$

Entonces,

$$\sum_{\deg d\leqslant n}\frac{\chi(d)\Lambda(d)}{|d|}\sum_{\deg E\leqslant n-\deg d}\frac{\chi(E)}{|E|}=L(\chi)\sum_{\deg d\leqslant n}\frac{\chi(d)\Lambda(d)}{|d|}+R(n),$$

donde $R(n):=-\sum_{\deg d\leqslant n}\frac{\chi(d)\Lambda(d)}{|d|}O(q^{\deg d-n})$.

Note que

$$\begin{aligned}\left|-\sum_{\deg d\leqslant n}\frac{\chi(d)\Lambda(d)}{|d|}O(q^{\deg d-n})\right|&\leqslant\sum_{\deg d\leqslant n}\frac{|\chi(d)|\Lambda(d)}{|d|}|O(q^{\deg d-n})|\\&\leqslant\sum_{\deg d\leqslant n}\frac{\Lambda(d)}{|d|}|O(q^{\deg d-n})|\\&\leqslant Mq^{-n}\sum_{\deg d\leqslant n}\frac{\Lambda(d)q^{\deg d}}{|d|}\\&=Mq^{-n}\sum_{\deg d\leqslant n}\Lambda(d),\end{aligned}$$

para $M>0$. O sea, $R(n)=O(q^{-n}\sum_{\deg d\leqslant n}\Lambda(d))=O(q^{-n}q^n)=O(1)$, por *Lema 2.3*.
Puesto que, para $n\geqslant\deg m$, $c_k=0$, por consiguiente,

$$\begin{aligned}\sum_{\deg f\leqslant n}\frac{\chi(f)\log|f|}{|f|}&=\sum_{0\leqslant k\leqslant n}\frac{k\log q}{q^k}\sum_{\deg f=k}\chi(f)\\&=\sum_{0\leqslant k\leqslant n}\frac{k\log q}{q^k}c_k\\&=\log q\sum_{k=0}^{\deg m-1}\frac{k}{q^k}c_k=c,\end{aligned}$$

donde c es una constante.
Entonces,

$$c=L(\chi)\sum_{\deg d\leqslant n}\frac{\chi(d)\Lambda(d)}{|d|}+O(1).$$

Luego,

$$L(\chi)\sum_{\deg d\leqslant n}\frac{\chi(d)\Lambda(d)}{|d|}=c-O(1)=O(1).$$

■

De lo anterior, deducimos inmediatamente,

Corolario 2.2. *Si $L(\chi)\neq 0$ para el carácter no principal χ, entonces $A_\chi(n)=O(1)$.*

Demostración. Del *Lema 2.6*, tenemos, para $n\geqslant 0$,

$$L(\chi)\sum_{\deg f\leqslant n}\frac{\chi(f)\Lambda(f)}{|f|}=O(1)$$

o sea, $L(\chi)A_\chi(n)=O(1)$. Si $L(\chi)\neq 0$, entonces $A_\chi(n)=\dfrac{1}{L(\chi)}O(1)=O(1)$. ■

Lema 2.7. *Sea χ un carácter no principal. Para $n\geqslant 0$,*

$$\log(q^n)+A_\chi(n)=L(\chi)\sum_{\deg f\leqslant n}\frac{\chi(f)\mu(f)}{|f|}\log\frac{q^n}{|f|}+O(1).$$

En particular, si $L(\chi)=0$, $A_\chi(n)=-\log(q^n)+O(1)$.

Demostración. Evaluemos $\sum_{\deg f\leqslant n}\frac{\chi(f)}{|f|}\sum_{d|f}\mu(d)\log\frac{q^n}{|d|}$ de dos maneras diferentes. Note que, por *Lema 2.2*

$$\begin{aligned}\sum_{d|f}\mu(d)\log\frac{q^n}{|d|}&=\sum_{d|f}\mu(d)\log(q^n)-\sum_{d|f}\mu(d)\log|d|\\&=\sum_{d|f}\mu(d)\log(q^n)+\Lambda(f)\\&=\log(q^n)\sum_{d|f}\mu(d)+\Lambda(f),\end{aligned}$$

Por *Teorema 1.10*, se tiene: Si $f=1$, $\sum_{d|f}\mu(d)=1$. Además, $\Lambda(f)=0$. También, Si $f\neq 1$, $\sum_{d|f}\mu(d)=0$. Entonces,

$$\sum_{d|f}\mu(d)\log\frac{q^n}{|d|}=\begin{cases}\log(q^n), & \text{si } f=1\\ \Lambda(f), & \text{si } f\neq 1\end{cases}$$

Luego, por un lado

$$\begin{aligned}\sum_{\deg f\leqslant n}\frac{\chi(f)}{|f|}\sum_{d|f}\mu(d)\log\frac{q^n}{|d|}&=\underbrace{\frac{\chi(f)}{|f|}\sum_{d|f}\mu(d)\log\frac{q^n}{|d|}}_{\deg f=0}+\underbrace{\sum_{\deg f\leqslant n}\frac{\chi(f)}{|f|}\sum_{d|f}\mu(d)\log\frac{q^n}{|d|}}_{0<\deg f\leqslant n}\\&=\log(q^n)+\sum_{\deg f\leqslant n}\frac{\chi(f)}{|f|}\Lambda(f),\end{aligned}$$

pues, $f=1$ cuando $\deg f=0$, y $f\neq 1$ cuando $0<\deg f$.
Por otro lado, invirtiendo el orden de la suma, tenemos

$$\sum_{\deg f\leqslant n}\frac{\chi(f)}{|f|}\sum_{d|f}\mu(d)\log\frac{q^n}{|d|}=\sum_{\deg d\leqslant n}\frac{\chi(d)\mu(d)}{|d|}\log\frac{q^n}{|d|}\sum_{\deg h\leqslant n-\deg d}\frac{\chi(h)}{|h|}.$$

A saber,

$$\begin{aligned}
\sum_{\deg f\leqslant n}\frac{\chi(f)}{|f|}\sum_{d|f}\mu(d)\log\frac{q^n}{|d|} &= \sum_{\deg f=0}\frac{\chi(f)}{|f|}\sum_{d|f}\mu(d)\log\frac{q^n}{|d|}+\sum_{\deg f=1}\frac{\chi(f)}{|f|}\sum_{d|f}\mu(d)\log\frac{q^n}{|d|}+\cdots\\
&+\sum_{\deg f=n-1}\frac{\chi(f)}{|f|}\sum_{d|f}\mu(d)\log\frac{q^n}{|d|}+\sum_{\deg f=n}\frac{\chi(f)}{|f|}\sum_{d|f}\mu(d)\log\frac{q^n}{|d|}\\
&=\sum_{\substack{d|f\\ \deg d=0}}\mu(d)\log\frac{q^n}{|d|}\left[\sum_{\deg f=0}\frac{\chi(f)}{|f|}+\sum_{\deg f=1}\frac{\chi(f)}{|f|}+\cdots+\sum_{\deg f=n-1}\frac{\chi(f)}{|f|}+\sum_{\deg f=n}\frac{\chi(f)}{|f|}\right]\\
&+\sum_{\substack{d|f\\ \deg d=1}}\mu(d)\log\frac{q^n}{|d|}\left[\sum_{\deg f=1}\frac{\chi(f)}{|f|}+\cdots+\sum_{\deg f=n-1}\frac{\chi(f)}{|f|}+\sum_{\deg f=n}\frac{\chi(f)}{|f|}\right]+\cdots\\
&+\sum_{\substack{d|f\\ \deg d=n-1}}\mu(d)\log\frac{q^n}{|d|}\left[\sum_{\deg f=n-1}\frac{\chi(f)}{|f|}+\sum_{\deg f=n}\frac{\chi(f)}{|f|}\right]+\sum_{\substack{d|f\\ \deg d=n}}\mu(d)\log\frac{q^n}{|d|}\sum_{\deg f=n}\frac{\chi(f)}{|f|}\\
&=\sum_{\substack{d|f\\ \deg d=0}}\mu(d)\log\frac{q^n}{|d|}\sum_{0\leqslant\deg f\leqslant n}\frac{\chi(f)}{|f|}+\sum_{\substack{d|f\\ \deg d=1}}\mu(d)\log\frac{q^n}{|d|}\sum_{1\leqslant\deg f\leqslant n}\frac{\chi(f)}{|f|}+\cdots\\
&+\sum_{\substack{d|f\\ \deg d=n-1}}\mu(d)\log\frac{q^n}{|d|}\sum_{n-1\leqslant\deg f\leqslant n}\frac{\chi(f)}{|f|}+\sum_{\substack{d|f\\ \deg d=n}}\mu(d)\log\frac{q^n}{|d|}\sum_{\deg f=n}\frac{\chi(f)}{|f|}\\
&=\sum_{\deg d=0}\frac{\chi(d)\mu(d)}{|d|}\log\frac{q^n}{|d|}\sum_{\deg h\leqslant n-0}\frac{\chi(h)}{|h|}+\sum_{\deg d=1}\frac{\chi(d)\mu(d)}{|d|}\log\frac{q^n}{|d|}\sum_{\deg h\leqslant n-1}\frac{\chi(h)}{|h|}+\cdots\\
&+\sum_{\deg d=n-1}\frac{\chi(d)\mu(d)}{|d|}\log\frac{q^n}{|d|}\sum_{\deg h\leqslant n-(n-1)}\frac{\chi(h)}{|h|}+\sum_{\deg d=n}\frac{\chi(d)\mu(d)}{|d|}\log\frac{q^n}{|d|}\sum_{\deg h\leqslant n-n}\frac{\chi(h)}{|h|}\\
&=\sum_{\deg d\leqslant n}\frac{\chi(d)\mu(d)}{|d|}\log\frac{q^n}{|d|}\sum_{\deg h\leqslant n-\deg d}\frac{\chi(h)}{|h|},
\end{aligned}$$

donde $f=hd$ (prueba análoga a (2.13)). Además, por *Lema 2.5*,

$$L(\chi)-\sum_{\deg h\leqslant n-\deg d}\frac{\chi(h)}{|h|}=O(q^{\deg d-n}).$$

Luego, la expresión que está a la derecha se convierte en

$$\begin{aligned}
\sum_{\deg d\leqslant n}\frac{\chi(d)\mu(d)}{|d|}\log\frac{q^n}{|d|}\sum_{\deg h\leqslant n-\deg d}\frac{\chi(h)}{|h|} &= \sum_{\deg d\leqslant n}\frac{\chi(d)\mu(d)}{|d|}\log\frac{q^n}{|d|}(L(\chi)-O(q^{\deg d-n}))\\
&= L(\chi)\sum_{\deg d\leqslant n}\frac{\chi(d)\mu(d)}{|d|}\log\frac{q^n}{|d|}+R(n),
\end{aligned}$$

donde $R(n):=-q^{-n}\displaystyle\sum_{\deg d\leqslant n}\frac{\chi(d)\mu(d)}{|d|}\log\frac{q^n}{|d|}O(q^{\deg d})$.

Note que

$$\begin{aligned}
|R(n)| &\leqslant q^{-n} \sum_{\deg d \leqslant n} \frac{|\chi(d)||\mu(d)|}{|d|} \left| \log \frac{q^n}{|d|} \right| |O(q^{\deg d})| \\
&\leqslant M q^{-n} \sum_{\deg d \leqslant n} \frac{(\log(q^n) - \log|d|)}{|d|} q^{\deg d} \\
&= M q^{-n} \left[\sum_{\deg d \leqslant n} \log(q^n) - \sum_{\deg d \leqslant n} \log|d| \right] \\
&= M q^{-n} \left[\log(q^n) \sum_{k=0}^{n} \sum_{\deg d = k} 1 - \sum_{\deg d \leqslant n} \log|d| \right] \\
&= M q^{-n} \left[\log(q^n) \sum_{k=0}^{n} q^k - \sum_{\deg d \leqslant n} \log|d| \right],
\end{aligned}$$

para $M > 0$. Después, expandiendo la progresión geométrica y restando la expresión obtenida en el *Lema 2.1*, vemos

$$\begin{aligned}
&\log(q^n) \sum_{k=0}^{n} q^k - \sum_{\deg d \leqslant n} \log|d| \\
&= \log(q^n) \left[1 + \frac{q(q^n - 1)}{q - 1} \right] - \left[\frac{q^{n+1}}{q-1} \log(q^n) - (\log q) \frac{q}{q-1} \cdot \frac{q^n - 1}{q - 1} \right] \\
&= \log(q^n) \left(\frac{q^{n+1} - 1}{q - 1} \right) - \frac{q^{n+1}}{q-1} \log(q^n) + (\log q) \frac{q}{q-1} \cdot \frac{q^n - 1}{q-1} \\
&= \frac{-1}{q-1} \log(q^n) + (\log q) \frac{q}{q-1} \cdot \frac{q^n - 1}{q-1} \\
&\leqslant \frac{1}{q-1} \log(q^n) + 2(\log q) q^n \\
&\leqslant 2(\log q) \log(q^n) + 2(\log q) q^n,
\end{aligned}$$

puesto que, $\dfrac{q}{q-1} = 1 + \dfrac{1}{q-1} \leqslant 2$ y $\dfrac{q^n - 1}{q-1} = \dfrac{q^n}{q-1} - \dfrac{1}{q-1} \leqslant \dfrac{q^n}{q-1} \leqslant q^n$. Es decir,

$$\log(q^n) \sum_{k=0}^{n} q^k - \sum_{\deg d \leqslant n} \log|d| \ll \log(q^n) + q^n \ll q^n.$$

Entonces, $R(n) = O(1)$, pues $|R(n)| \ll q^{-n} q^n = 1$.
Comparando las dos expresiones obtenidas da la afirmación del teorema:

$$\log(q^n) + \sum_{\deg f \leqslant n} \frac{\chi(f)\Lambda(f)}{|f|} = L(\chi) \sum_{\deg d \leqslant n} \frac{\chi(d)\mu(d)}{|d|} \log \frac{q^n}{|d|} + O(1)$$

o

$$\log(q^n) + A_\chi(n) = L(\chi) \sum_{\deg d \leqslant n} \frac{\chi(d)\mu(d)}{|d|} \log \frac{q^n}{|d|} + O(1).$$

■

Colocando juntos este resultado con el del *Corolario 2.2*, vemos que hemos demostrado

Lema 2.8. *Sea χ un carácter no principal. Entonces, para $n \geqslant 0$*

$$A_\chi(n) = O(1) + \log(q^n) \begin{cases} 0, & si\ L(\chi) \neq 0 \\ -1, & si\ L(\chi) = 0 \end{cases}$$

Demostración. Del *Lema 2.7* tenemos, para $n \geqslant 0$

$$A_\chi(n) = L(\chi) \sum_{\deg f \leqslant n} \frac{\chi(f)\mu(f)}{|f|} \log \frac{q^n}{|f|} + O(1) - \log(q^n).$$

Si $L(\chi) = 0$, entonces

$$A_\chi(n) = O(1) + \log(q^n)(-1).$$

Por otro lado, del *Corolario 2.2* tenemos, si $L(\chi) \neq 0$

$$A_\chi(n) = O(1) + \log(q^n)(0).$$

De esta forma concluimos la afirmación del lema. ■

Corolario 2.3 (No anulación de $L(\chi)$ para χ no real)**.** *Si χ es un carácter que toma al menos un valor no real, $L(\chi) \neq 0$.*

Demostración. Por *Lema 1.1*, si $f \equiv 1$ mód m, entonces $\sum_\chi \chi(f) = \varphi(m)$. Además,

$$\begin{aligned} \sum_\chi A_\chi(n) &= A_{\chi_o}(n) + A_{\chi_1}(n) + \cdots + A_{\chi_{k-1}}(n) \\ &= \sum_{\deg f \leqslant n} \frac{\chi_o(f)\Lambda(f)}{|f|} + \sum_{\deg f \leqslant n} \frac{\chi_1(f)\Lambda(f)}{|f|} + \cdots + \sum_{\deg f \leqslant n} \frac{\chi_{k-1}(f)\Lambda(f)}{|f|}, \end{aligned}$$

pues $G \cong \widehat{G}$, tomando $o(G) = k$. Por otra parte,

$$\begin{aligned} &\left(\sum_\chi \chi(f)\right) \sum_{\substack{f \equiv 1 \text{ mód } m \\ \deg f \leqslant n}} \frac{\Lambda(f)}{|f|} \\ &= \left(\sum_\chi \chi(f)\right) \left[\sum_{\deg f = 0} \frac{\Lambda(f)}{|f|} + \sum_{\deg f = 1} \frac{\Lambda(f)}{|f|} + \cdots + \sum_{\deg f = n} \frac{\Lambda(f)}{|f|}\right] \\ &= \sum_{\deg f = 0} \frac{\Lambda(f)}{|f|} \sum_\chi \chi(f) + \sum_{\deg f = 1} \frac{\Lambda(f)}{|f|} \sum_\chi \chi(f) + \cdots + \sum_{\deg f = n} \frac{\Lambda(f)}{|f|} \sum_\chi \chi(f) \\ &= \sum_{\deg f = 0} \frac{\Lambda(f)}{|f|} [\chi_o(f) + \chi_1(f) + \cdots + \chi_{k-1}(f)] \\ &\quad + \sum_{\deg f = 1} \frac{\Lambda(f)}{|f|} [\chi_o(f) + \chi_1(f) + \cdots + \chi_{k-1}(f)] + \cdots \\ &\quad + \sum_{\deg f = n} \frac{\Lambda(f)}{|f|} [\chi_o(f) + \chi_1(f) + \cdots + \chi_{k-1}(f)] \\ &= \sum_{\deg f = 0} \frac{\chi_o(f)\Lambda(f)}{|f|} + \sum_{\deg f = 1} \frac{\chi_o(f)\Lambda(f)}{|f|} + \cdots + \sum_{\deg f = n} \frac{\chi_o(f)\Lambda(f)}{|f|} \\ &\quad + \sum_{\deg f = 0} \frac{\chi_1(f)\Lambda(f)}{|f|} + \sum_{\deg f = 1} \frac{\chi_1(f)\Lambda(f)}{|f|} + \cdots + \sum_{\deg f = n} \frac{\chi_1(f)\Lambda(f)}{|f|} + \cdots \end{aligned}$$

$$
\begin{aligned}
&+ \sum_{\deg f=0} \frac{\chi_{k-1}(f)\Lambda(f)}{|f|} + \sum_{\deg f=1} \frac{\chi_{k-1}(f)\Lambda(f)}{|f|} + \cdots + \sum_{\deg f=n} \frac{\chi_{k-1}(f)\Lambda(f)}{|f|} \\
&= \sum_{\deg f\leqslant n} \frac{\chi_o(f)\Lambda(f)}{|f|} + \sum_{\deg f\leqslant n} \frac{\chi_1(f)\Lambda(f)}{|f|} + \cdots + \sum_{\deg f\leqslant n} \frac{\chi_{k-1}(f)\Lambda(f)}{|f|} \\
&= \sum_{\chi} A_\chi(n).
\end{aligned}
$$

Entonces,

$$
\varphi(m) \sum_{\substack{f\equiv 1 \text{ mód } m \\ \deg f\leqslant n}} \frac{\Lambda(f)}{|f|} = \sum_{\chi} A_\chi(n). \tag{2.14}
$$

Por otro lado, del *Teorema 2.4* y del *Lema 2.8*, tenemos

$$
\begin{aligned}
\sum_{\chi} A_\chi(n) &= A_{\chi_o}(n) + A_{\chi_1}(n) + \cdots + A_{\chi_{k-1}}(n) \\
&= \log(q^n) + O(1) - V\log(q^n) + \underbrace{O(1) + \cdots + O(1)}_{k-1 \text{ veces}} \\
&= (1-V)\log(q^n) + O(1),
\end{aligned}
$$

donde V es el número de caracteres χ tales que $L(\chi) = 0$, es decir, $1 \leqslant V \leqslant k-1$.
Note que $\log|\pi| = \deg\pi \log q > 0$, pues $\log q \geqslant \log 2$ y $\deg\pi \geqslant 1$. Entonces,

$$
\sum_{\substack{f\equiv 1 \text{ mód } m \\ \deg f\leqslant n}} \frac{\Lambda(f)}{|f|} \geqslant 0.
$$

Ya que el lado izquierdo de (2.14) es no negativo para todo n, debemos tener $1 - V \geqslant 0$ o $V \leqslant 1$.
Pero si $L(\chi_1) = 0$ para un carácter no real χ_1, entonces $0 = \overline{L(\chi_1)} = L(\overline{\chi}_1)$. Ya que χ_1 toma, al menos, un valor no real, $\chi_1 \neq \overline{\chi}_1$ y, por tanto, $V \geqslant 2$ o $V > 1$, pues, al menos hay dos caracteres χ diferentes tales que $L(\chi) = 0$, contradiciendo lo anterior. ■

Puesto que por el *Corolario 2.3* y el *Teorema 2.3*, $L(\chi) \neq 0$ para cada χ no principal, el *Corolario 2.2* implica lo presagiado

Corolario 2.4. *Si χ es un carácter no principal, $A_\chi(n) = O(1)$.*

2.3. Prueba del Teorema.

Demostración del Teorema 2.1. Por *Lema 1.1*, *Teorema 2.4*, y *Corolario 2.4*, tenemos:

$$
\varphi(m) \sum_{\substack{\deg f\leqslant n \\ f\equiv a \text{ mód } m}} \frac{\Lambda(f)}{|f|} = \left(\sum_{\chi} \chi(f)\overline{\chi}(a) \right) \sum_{\substack{\deg f\leqslant n \\ f\equiv a \text{ mód } m}} \frac{\Lambda(f)}{|f|}.
$$

Como $G \cong \widehat{G}$, tomando $o(G) = k$, se tiene

$$\begin{aligned}
&\left(\sum_{\chi}\chi(f)\overline{\chi}(a)\right)\sum_{\substack{\deg f\leqslant n\\ f\equiv a \bmod m}}\frac{\Lambda(f)}{|f|}\\
&=\left(\sum_{\chi}\chi(f)\overline{\chi}(a)\right)\left[\sum_{\deg f=0}\frac{\Lambda(f)}{|f|}+\sum_{\deg f=1}\frac{\Lambda(f)}{|f|}+\cdots+\sum_{\deg f=n}\frac{\Lambda(f)}{|f|}\right]\\
&=\sum_{\deg f=0}\frac{\Lambda(f)}{|f|}\sum_{\chi}\chi(f)\overline{\chi}(a)+\sum_{\deg f=1}\frac{\Lambda(f)}{|f|}\sum_{\chi}\chi(f)\overline{\chi}(a)+\cdots+\sum_{\deg f=n}\frac{\Lambda(f)}{|f|}\sum_{\chi}\chi(f)\overline{\chi}(a)\\
&=\sum_{\deg f=0}\frac{\Lambda(f)}{|f|}[\chi_o(f)\overline{\chi}_o(a)+\chi_1(f)\overline{\chi}_1(a)+\cdots+\chi_{k-1}(f)\overline{\chi}_{k-1}(a)]\\
&\quad+\sum_{\deg f=1}\frac{\Lambda(f)}{|f|}[\chi_o(f)\overline{\chi}_o(a)+\chi_1(f)\overline{\chi}_1(a)+\cdots+\chi_{k-1}(f)\overline{\chi}_{k-1}(a)]+\cdots\\
&\quad+\sum_{\deg f=n}\frac{\Lambda(f)}{|f|}[\chi_o(f)\overline{\chi}_o(a)+\chi_1(f)\overline{\chi}_1(a)+\cdots+\chi_{k-1}(f)\overline{\chi}_{k-1}(a)]\\
&=\overline{\chi}_o(a)\sum_{\deg f\leqslant n}\frac{\chi_o(f)\Lambda(f)}{|f|}+\overline{\chi}_1(a)\sum_{\deg f\leqslant n}\frac{\chi_1(f)\Lambda(f)}{|f|}+\cdots+\overline{\chi}_{k-1}(f)\sum_{\deg f\leqslant n}\frac{\chi_{k-1}(f)\Lambda(f)}{|f|}\\
&=\overline{\chi}_o(a)A_{\chi_o}(n)+\overline{\chi}_1(a)A_{\chi_1}(n)+\cdots+\overline{\chi}_{k-1}(a)A_{\chi_{k-1}}(n)\\
&=\sum_{\chi}\overline{\chi}(a)A_{\chi}(n).
\end{aligned}$$

Por otro lado,

$$\begin{aligned}
&\sum_{\chi}\overline{\chi}(a)A_{\chi}(n)\\
&=\overline{\chi}_o(a)A_{\chi_o}(n)+\overline{\chi}_1(a)A_{\chi_1}(n)+\cdots+\overline{\chi}_{k-1}(a)A_{\chi_{k-1}}(n)\\
&=\overline{\chi}_o(a)\log(q^n)+\overline{\chi}_o(a)O(1)+\overline{\chi}_1(a)O(1)+\cdots+\overline{\chi}_{k-1}(a)O(1)\\
&=\overline{\chi}_o(a)\log(q^n)+O(1)\\
&=\log(q^n)+O(1),
\end{aligned}$$

pues $(a,m)=1$. Por lo tanto,

$$\varphi(m)\sum_{\substack{\deg f\leqslant n\\ f\equiv a \bmod m}}\frac{\Lambda(f)}{|f|}=\sum_{\chi}\overline{\chi}(a)A_{\chi}(n)=\log(q^n)+O(1).$$

Ahora,

$$\sum_{\substack{\deg f\leqslant n\\ f\equiv a \bmod m}}\frac{\Lambda(f)}{|f|}=\sum_{\substack{k\deg\pi\leqslant n\\ \pi^k\equiv a \bmod m}}\frac{\log|\pi|}{|\pi|^k}=\sum_{\substack{\deg\pi\leqslant n\\ \pi\equiv a \bmod m}}\frac{\log|\pi|}{|\pi|}+R(n),$$

donde

$$R(n):=\sum_{\substack{2\deg\pi\leqslant n\\ \pi^2\equiv a \bmod m}}\frac{\log|\pi|}{|\pi|^2}+\sum_{\substack{3\deg\pi\leqslant n\\ \pi^3\equiv a \bmod m}}\frac{\log|\pi|}{|\pi|^3}+\cdots$$

Como

$$\begin{aligned}\sum_{\deg f\leqslant n}\frac{\Lambda(f)}{|f|} &= \sum_{k\deg\pi\leqslant n}\frac{\log|\pi|}{|\pi|^k}\\ &= \sum_{\deg\pi\leqslant n}\frac{\log|\pi|}{|\pi|}+\sum_{2\deg\pi\leqslant n}\frac{\log|\pi|}{|\pi|^2}+\sum_{3\deg\pi\leqslant n}\frac{\log|\pi|}{|\pi|^3}+\cdots\\ &= \sum_{\deg\pi\leqslant n}\frac{\log|\pi|}{|\pi|}+R(n)+\sum_{\substack{2\deg\pi\leqslant n\\ \pi^2\not\equiv a\ \mathrm{m\acute{o}d}\ m}}\frac{\log|\pi|}{|\pi|^2}+\sum_{\substack{3\deg\pi\leqslant n\\ \pi^3\not\equiv a\ \mathrm{m\acute{o}d}\ m}}\frac{\log|\pi|}{|\pi|^3}+\cdots\\ &\geqslant \sum_{\deg\pi\leqslant n}\frac{\log|\pi|}{|\pi|}+R(n),\end{aligned}$$

entonces

$$\sum_{\deg f\leqslant n}\frac{\Lambda(f)}{|f|}-\sum_{\deg\pi\leqslant n}\frac{\log|\pi|}{|\pi|}\geqslant R(n)\geqslant 0.$$

Por consiguiente,

$$R(n)=O\bigg(\sum_{\deg f\leqslant n}\frac{\Lambda(f)}{|f|}-\sum_{\deg\pi\leqslant n}\frac{\log|\pi|}{|\pi|}\bigg).$$

Por tanto, como $m\neq 0$,

$$\begin{aligned}\frac{1}{\varphi(m)}\log(q^n)+O(1) &= \frac{1}{\varphi(m)}\log(q^n)+\frac{1}{\varphi(m)}O(1)\\ &= \sum_{\substack{\deg f\leqslant n\\ f\equiv a\ \mathrm{m\acute{o}d}\ m}}\frac{\Lambda(f)}{|f|}\\ &= \sum_{\substack{\deg\pi\leqslant n\\ \pi\equiv a\ \mathrm{m\acute{o}d}\ m}}\frac{\log|\pi|}{|\pi|}+O\bigg(\sum_{\deg f\leqslant n}\frac{\Lambda(f)}{|f|}-\sum_{\deg\pi\leqslant n}\frac{\log|\pi|}{|\pi|}\bigg)\\ &= \sum_{\substack{\deg\pi\leqslant n\\ \pi\equiv a\ \mathrm{m\acute{o}d}\ m}}\frac{\log|\pi|}{|\pi|}+O(1),\end{aligned}$$

por *Lema 2.4*. Reorganizando da el teorema. ■

Capítulo 3

Teorema de Dirichlet en $\mathbb{F}_q[t]$ según Kornblum.

Dirichlet demostró el siguiente teorema para las progresiones aritméticas de números enteros positivos: Si $(a, m) = 1$ con a, m enteros mayores o iguales que uno, entonces existe una cantidad infinita de números primos p tales que $p \equiv a$ mód m. En este capítulo daremos una demostración de su análogo en $\mathbb{F}_q[t]$, véase [5].

Teorema 3.1. *Si $a, m \in \mathbb{F}_q[t]$ con $(a, m) = 1$ y $m \neq 0$, entonces existe una cantidad infinita de polinomios $p \in P(q;t)$ tales que $p \equiv a$* mód m.

3.1. Resultados Preliminares: Productos de Euler.

Proposición 3.1. *Sea $\Re(a_n) > 0$ para todo $n > 0$. Entonces, un producto infinito $\prod_n (1 + a_n)$ de números complejos converge (absolutamente) si, y sólo si, la serie $\sum_n a_n$ converge (absolutamente). En tal caso, la serie $\sum_n \log(1 + a_n)$ converge a un logaritmo del producto.*

Estaremos interesados en productos inducidos por el conjunto $P(q;t)$. Estos productos son llamados productos de *Euler*.

Definición 3.1. *Sea $s = \sigma + i\gamma$ un número complejo. Si colocamos $\chi = \chi_o$ en la ecuación (2.9), obtenemos la función*

$$\zeta(s) = \sum_{f \in M(q;t)} \frac{1}{|f|^s} \tag{3.1}$$

llamada la serie o función zeta de Riemann asociada con $M(q;t)$.

Proposición 3.2. *La función $\zeta(s)$ satisface las siguientes propiedades:*

(i). La suma $\zeta(s)$ es absolutamente convergente para $\sigma = \Re(s) > 1$.

(ii). Para $\sigma > 1$, $\zeta(s) = \sum_{d=0}^{\infty} \frac{1}{q^{d(s-1)}}$.

(iii). Para $\sigma > 1$, $\zeta(s) = \dfrac{1}{1 - 1/q^{s-1}}$.

Demostración.

(i). Tomemos $\sigma = \mathfrak{R}(s) > 1$. Como $|f| = q^k$, donde $k = \deg f$, y existen q^k polinomios mónicos de grado k, tenemos, para todo $k = 0, 1, 2, \cdots$, lo siguiente

$$\begin{aligned}\left| \sum_{\substack{f \in M(q;t) \\ \deg f = k}} |f|^{-s} \right| &\leqslant \sum_{\substack{f \in M(q;t) \\ \deg f = k}} ||f|^{-s}| \\ &= q^{-k\sigma} \sum_{\substack{f \in M(q;t) \\ \deg f = k}} 1 \\ &= q^{-k\sigma} q^k \\ &= q^{k(1-\sigma)}.\end{aligned}$$

Luego,

$$\begin{aligned}\sum_{\deg f \leqslant r} ||f|^{-s}| &= \sum_{k=0}^{r} \sum_{\substack{f \in M(q;t) \\ k = \deg f}} ||f|^{-s}| \\ &= \sum_{k=0}^{r} q^{-k\sigma} \sum_{\substack{f \in M(q;t) \\ \deg f = k}} 1 \\ &= \sum_{k=0}^{r} q^{k(1-\sigma)} \\ &= 1 + \sum_{k=1}^{r} q^{k(1-\sigma)} \\ &= 1 + q^{1-\sigma} \frac{(q^{r(1-\sigma)} - 1)}{q^{1-\sigma} - 1} \\ &= \frac{1 - q^{(1-\sigma)(1+r)}}{1 - q^{1-\sigma}}.\end{aligned}$$

Por lo tanto,

$$\sum_{\deg f \leqslant r} ||f|^{-s}| \to \frac{1}{1 - q^{1-\sigma}}, \text{ cuando } r \to \infty,$$

pues $\sigma > 1$.

(ii). Como $\zeta(s)$ es absolutamente convergente, por *(i)*, tenemos

$$\begin{aligned}\zeta(s) = \sum_{f \in M(q;t)} \frac{1}{|f|^s} &= \underbrace{\frac{1}{|f|^s} + \cdots + \frac{1}{|f|^s}}_{\deg f = 0} + \underbrace{\frac{1}{|f|^s} + \cdots + \frac{1}{|f|^s}}_{\deg f = 1} + \cdots \\ &= \#(\deg f) \left.\frac{1}{|f|^s}\right|_{\deg f = 0} + \#(\deg f) \left.\frac{1}{|f|^s}\right|_{\deg f = 1} + \cdots \\ &= \sum_{\deg f = 0}^{\infty} \frac{\#(\deg f)}{|f|^s}\end{aligned}$$

$$= \sum_{d=0}^{\infty} \frac{\#(d)}{q^{ds}}$$
$$= \sum_{d=0}^{\infty} \frac{q^d}{q^{ds}}$$
$$= \sum_{d=0}^{\infty} \frac{1}{q^{d(s-1)}},$$

tomando $\deg f = d$, y donde $\#(d) = q^d$ es el número de polinomios unitarios de grado d en $\mathbb{F}_q[t]$. Por lo tanto,

$$\zeta(s) = \sum_{\deg d=0}^{\infty} \frac{1}{q^{d(s-1)}}.$$

(iii). Por *(i)* y *(ii)*, tenemos

$$\zeta(s) = \sum_{\deg d=0}^{\infty} \frac{1}{q^{d(s-1)}} = \lim_{n\to\infty} \sum_{d=0}^{n} \frac{1}{q^{d(s-1)}}$$
$$= \lim_{n\to\infty} \left[\frac{\frac{1}{q^{(n+1)(s-1)}} - 1}{\frac{1}{q^{s-1}} - 1} \right]$$
$$= \frac{1}{1 - \frac{1}{q^{s-1}}}.$$

■

Teorema 3.2. *Para cada $\sigma > 1$ se cumple*

$$\zeta(s) = \prod_{p\in P(q;t)} (1 - |p|^{-s})^{-1}.$$

Además, la convergencia del producto es absoluta.

Demostración. Para probar que el producto converge absolutamente, notemos que

$$\prod_{p\in P(q;t)} (1 - |p|^{-s})^{-1} = \prod_{p\in P(q;t)} \frac{1}{1 - \frac{1}{|p|^s}} = \prod_{p\in P(q;t)} \frac{|p|^s}{|p|^s - 1} = \prod_{p\in P(q;t)} \left(1 + \frac{1}{|p|^s - 1}\right)$$

y, además, que la serie $\displaystyle\sum_{p\in P(q;t)} \frac{1}{|p|^s - 1}$ converge absolutamente. A saber,

$$\sum_{p\in P(q;t)} \left| \frac{1}{|p|^s - 1} \right| = \sum_{p\in P(q;t)} \frac{1}{||p|^s - 1|} \leqslant \sum_{p\in P(q;t)} \frac{1}{|p|^\sigma - 1} < \infty,$$

ya que $|p|^\sigma - 1 = ||p|^s| - 1 \leqslant ||p|^s - 1|$ y

$$\lim_{|p|\to\infty} \frac{\frac{1}{|p|^\sigma - 1}}{\frac{1}{|p|^\sigma}} = \lim_{|p|\to\infty} \frac{1}{1 - \frac{1}{|p|^\sigma}} = 1,$$

donde la serie $\displaystyle\sum_{p\in P(q;t)} \frac{1}{|p|^\sigma}$ es convergente para $\sigma > 1$.

Por otro lado, para cada $p \in P(q;t)$ se cumple

$$\frac{1}{1 - \frac{1}{|p|^s}} = \sum_{k=0}^{\infty} \frac{1}{|p|^{ks}} \tag{3.2}$$

donde $\deg p \geqslant 1$, y teniendo en cuenta que la serie es geométrica.
Sea $N \in \mathbb{N}$ y sean $p_1, p_2, \cdots, p_r \in P(q;t)$ tales que $|p_i| \leqslant N$. Entonces, de (3.2) y por el teorema de la factorización única, tenemos

$$\begin{aligned}
P(N) := \prod_{|p|\leqslant N} \frac{1}{1-\frac{1}{|p|^s}} &= \prod_{|p|\leqslant N} \sum_{k=0}^{\infty} \frac{1}{|p|^{ks}} \\
&= \sum_{k=0}^{\infty} \frac{1}{|p_1|^{ks}} \sum_{k=0}^{\infty} \frac{1}{|p_2|^{ks}} \cdots \sum_{k=0}^{\infty} \frac{1}{|p_r|^{ks}} \\
&= \left(1+\frac{1}{|p_1|^s}+\frac{1}{|p_1|^{2s}}+\cdots\right)\left(1+\frac{1}{|p_2|^s}+\frac{1}{|p_2|^{2s}}+\cdots\right)\cdots \\
&\quad \left(1+\frac{1}{|p_r|^s}+\frac{1}{|p_r|^{2s}}+\cdots\right) \\
&= \left(1+\frac{1}{|p_1|^s}+\frac{1}{|p_1^2|^s}+\cdots\right)\left(1+\frac{1}{|p_2|^s}+\frac{1}{|p_2^2|^s}+\cdots\right)\cdots \\
&\quad \left(1+\frac{1}{|p_r|^s}+\frac{1}{|p_r^2|^s}+\cdots\right) \\
&= \sum_{k_1,k_2,\cdots,k_r=0}^{\infty} \frac{1}{|p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}|^s} \\
&= \sum_{f\in A} \frac{1}{|f|^s},
\end{aligned}$$

donde $A \subset M(q;t)$ es el conjunto de los f tales que todos sus factores primos tienen valor absoluto $\leqslant N$. Además, como

$$\zeta(s) = \sum_{f\in A} \frac{1}{|f|^s} + \sum_{f\in B} \frac{1}{|f|^s} = P(N) + S(N) \quad \text{o} \quad \zeta(s) - P(N) = S(N)$$

donde $B \subset M(q;t)$ es el conjunto de los f tales que al menos uno de sus factores primos tiene valor absoluto $> N$, entonces

$$|\zeta(s) - P(N)| = |S(N)| \leqslant \sum_{f\in B} \frac{1}{|f|^\sigma} \to 0$$

cuando $N \to \infty$, ya que, $\displaystyle\sum_{f\in M(q;t)} \frac{1}{|f|^s}$ es convergente. Por lo tanto,

$$\zeta(s) = \prod_{p\in P(q;t)} (1-|p|^{-s})^{-1}.$$

■

Proposición 3.3. *Sea χ un carácter módulo $m(t)$. Entonces, para $\sigma > 1$,*

$$L(s,\chi) = \prod_{p\in P(q;t)} \left(1-\frac{\chi(p)}{|p|^s}\right)^{-1}.$$

En particular,

$$L(s,\chi_o) = \zeta(s) \prod_{\substack{p\in P(q;t)\\ p\mid m}} \left(1-\frac{1}{|p|^s}\right).$$

Demostración. Para probar que el producto converge absolutamente, es suficiente probar que la serie $\sum_{p\in P(q;t)} \frac{\chi(p)}{|p|^s-\chi(p)}$ converge absolutamente. A saber,

$$\sum_{p\in P(q;t)} \left|\frac{\chi(p)}{|p|^s-\chi(p)}\right| \leqslant \sum_{p\in P(q;t)} \frac{1}{||p|^s-\chi(p)|} \leqslant \sum_{p\in P(q;t)} \frac{1}{|p|^\sigma-1} < \infty,$$

ya que $|p|^\sigma - 1 \leqslant ||p|^s| - |\chi(p)| \leqslant ||p|^s - \chi(p)|$ y

$$\lim_{|p|\to\infty} \frac{\frac{1}{|p|^\sigma-1}}{\frac{1}{|p|^\sigma}} = \lim_{|p|\to\infty} \frac{1}{1-\frac{1}{|p|^\sigma}} = 1,$$

donde la serie $\sum_{p\in P(q;t)} \frac{1}{|p|^\sigma}$ es convergente para $\sigma > 1$.
Por otro lado, para cada $p \in P(q;t)$, con $\deg p > 0$, se cumple

$$\frac{1}{1-\frac{\chi(p)}{|p|^s}} = \sum_{k=0}^{\infty} \frac{\chi(p^k)}{|p|^{ks}} \tag{3.3}$$

ya que, $\left|\frac{\chi(p)}{|p|^s}\right| < 1$ y χ es completamente multiplicativa.
Sea $N \in \mathbb{N}$ y sean $p_1, p_2, \cdots, p_r \in P(q;t)$ tales que $|p_i| \leqslant N$. Entonces, de (3.3), y por el teorema de la factorización única, tenemos

$$\begin{aligned}
P(N) := \prod_{|p|\leqslant N} \frac{1}{1-\frac{\chi(p)}{|p|^s}} &= \prod_{|p|\leqslant N} \sum_{k=0}^{\infty} \frac{\chi(p^k)}{|p|^{ks}} \\
&= \sum_{k=0}^{\infty} \frac{\chi(p_1^k)}{|p_1|^{ks}} \sum_{k=0}^{\infty} \frac{\chi(p_2^k)}{|p_2|^{ks}} \cdots \sum_{k=0}^{\infty} \frac{\chi(p_r^k)}{|p_r|^{ks}} \\
&= \left(1+\frac{\chi(p_1)}{|p_1|^s}+\frac{\chi(p_1^2)}{|p_1^2|^s}+\cdots\right)\left(1+\frac{\chi(p_2)}{|p_2|^s}+\frac{\chi(p_2^2)}{|p_2^2|^s}+\cdots\right)\cdots \\
&\quad \left(1+\frac{\chi(p_r)}{|p_r|^s}+\frac{\chi(p_r^2)}{|p_r^2|^s}+\cdots\right) \\
&= \sum_{k_1,k_2,\cdots,k_r=0}^{\infty} \frac{\chi(p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r})}{|p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}|^s} \\
&= \sum_{f\in A} \frac{\chi(f)}{|f|^s},
\end{aligned}$$

donde $A \subset M(q;t)$ es el conjunto de los f tales que todos sus factores primos tienen valor absoluto $\leqslant N$. Además, como

$$L(s,\chi) - P(N) = \sum_{f\in B} \frac{\chi(f)}{|f|^s}$$

donde $B \subset M(q;t)$ es el conjunto de los f tales que al menos uno de sus factores primos tiene valor absoluto $> N$, entonces

$$|L(s,\chi) - P(N)| \leqslant \sum_{f\in B} \frac{1}{|f|^\sigma} \to 0$$

cuando $N \to \infty$, ya que, $\sum_{f \in M(q;t)} \frac{1}{|f|^s}$ es convergente. Por lo tanto,

$$L(s,\chi) = \prod_{p \in P(q;t)} \left(1 - \frac{\chi(p)}{|p|^s}\right)^{-1}.$$

Por otro lado, notemos que

$$\begin{aligned} L(s,\chi_o) &= \prod_{p \in P(q;t)} (1 - \chi_o(p)|p|^{-s})^{-1} \\ &= \prod_{\substack{p \in P(q;t) \\ (p,m)=1}} (1 - \chi_o(p)|p|^{-s})^{-1} \prod_{\substack{p \in P(q;t) \\ (p,m)\neq 1}} (1 - \chi_o(p)|p|^{-s})^{-1} \\ &= \prod_{\substack{p \in P(q;t) \\ (p,m)=1}} (1 - |p|^{-s})^{-1} \\ &= \prod_{\substack{p \in P(q;t) \\ p \nmid m}} (1 - |p|^{-s})^{-1}. \end{aligned}$$

Además,

$$\begin{aligned} &\prod_{p \in P(q;t)} (1 - |p|^{-s})^{-1} \prod_{\substack{p \in P(q;t) \\ p \mid m}} (1 - |p|^{-s}) \\ &= \prod_{\substack{p \in P(q;t) \\ p \nmid m}} (1 - |p|^{-s})^{-1} \prod_{\substack{p \in P(q;t) \\ p \mid m}} (1 - |p|^{-s})^{-1} \prod_{\substack{p \in P(q;t) \\ p \mid m}} (1 - |p|^{-s}) \\ &= \prod_{\substack{p \in P(q;t) \\ p \nmid m}} (1 - |p|^{-s})^{-1}. \end{aligned}$$

Entonces, del *Teorema 3.2*, se tiene

$$\begin{aligned} L(s,\chi_o) &= \prod_{p \in P(q;t)} (1 - |p|^{-s})^{-1} \prod_{\substack{p \in P(q;t) \\ p \mid m}} (1 - |p|^{-s}) \\ &= \zeta(s) \prod_{\substack{p \in P(q;t) \\ p \mid m}} (1 - |p|^{-s}). \end{aligned}$$

■

Corolario 3.1. *Si χ es un carácter módulo $m(t)$, entonces, para $\sigma > 1$, tenemos*

$$L(s,\chi) = \exp\left\{ \sum_{k=1}^{\infty} \sum_{p \in P(q;t)} \frac{\chi(p^k)}{k|p|^{ks}} \right\}.$$

Demostración. Como $L(s,\chi)$ es analítica para $\sigma > 1$, entonces, de la *Proposición 3.3*, tenemos

$$\log L(s,\chi) = \log \prod_{p \in P(q;t)} \left(1 - \frac{\chi(p)}{|p|^s}\right)^{-1} = - \sum_{p \in P(q;t)} \log(1 - \chi(p)|p|^{-s}).$$

Como

$$\left| -\frac{\chi(p)}{|p|^s} \right| = \frac{|\chi(p)|}{|p|^\sigma} \leqslant \frac{1}{|p|^\sigma} < 1,$$

pues, $|p|^\sigma = q^{\sigma \deg p} \geqslant 2^{\sigma \deg p} > 2^{\deg p} > 1$, entonces, usando el desarrollo de *Taylor*

$$\log(1+x) = \sum_{k=1}^{\infty} \frac{(-1)^{k-1} x^k}{k}, \quad \text{para} \quad |x| < 1,$$

obtenemos,

$$\begin{aligned}
\log(1-\chi(p)|p|^{-s}) &= \log[1+(-\chi(p)|p|^{-s})] \\
&= \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} \left(-\frac{\chi(p)}{|p|^s} \right)^k \\
&= \sum_{k=1}^{\infty} \frac{(-1)^{k-1}(-1)^k}{k} \frac{(\chi(p))^k}{|p|^{ks}} \\
&= -\sum_{k=1}^{\infty} \frac{\chi(p^k)}{k|p|^{ks}},
\end{aligned}$$

pues χ es completamente multiplicativa. Por lo tanto,

$$\begin{aligned}
\log L(s,\chi) &= \sum_{p \in P(q;t)} \sum_{k=1}^{\infty} \frac{\chi(p^k)}{k|p|^{ks}} \\
&= \sum_{k=1}^{\infty} \frac{\chi(p_1^k)}{k|p_1|^{ks}} + \sum_{k=1}^{\infty} \frac{\chi(p_2^k)}{k|p_2|^{ks}} + \cdots \\
&= \left(\frac{\chi(p_1)}{|p_1|^s} + \frac{\chi(p_1^2)}{2|p_1|^{2s}} + \cdots \right) + \left(\frac{\chi(p_2)}{|p_2|^s} + \frac{\chi(p_2^2)}{2|p_2|^{2s}} + \cdots \right) + \cdots \\
&= \left(\frac{\chi(p_1)}{|p_1|^s} + \frac{\chi(p_2)}{|p_2|^s} + \cdots \right) + \left(\frac{\chi(p_1^2)}{2|p_1|^{2s}} + \frac{\chi(p_2^2)}{2|p_2|^{2s}} + \cdots \right) + \cdots \\
&= \sum_{p \in P(q;t)} \frac{\chi(p)}{|p|^s} + \sum_{p \in P(q;t)} \frac{\chi(p^2)}{2|p|^{2s}} + \cdots \\
&= \sum_{k=1}^{\infty} \sum_{p \in P(q;t)} \frac{\chi(p^k)}{k|p|^{ks}}.
\end{aligned}$$

De esta forma se concluye la afirmación. ■

Corolario 3.2. *El carácter principal χ_o cumple las siguientes propiedades:*

(i). $\lim\limits_{s \to 1^+} (s-1) L(s,\chi_o) = \dfrac{a(m)}{\log q}$, *donde* $a(m) \in \mathbb{C}$ *es una constante.*

(ii). $\lim\limits_{s \to 1^+} \dfrac{L'(s,\chi_o)}{L(s,\chi_o)} = \infty.$

Demostración.

(i). Puesto que $\zeta(s) = (1-q^{1-s})^{-1}$ cuando $\sigma > 1$, entonces, aplicando *l'Hôpital*, tenemos

$$\lim_{s \to 1^+} (s-1)\zeta(s) = \lim_{s \to 1^+} \frac{s-1}{1-q^{1-s}} = \lim_{s \to 1^+} \frac{1}{q^{1-s} \log q} = \frac{1}{\log q}.$$

Además,

$$\lim_{s\to 1^+}\prod_{p|m}\left(1-\frac{1}{|p|^s}\right)=\prod_{p|m}\left(1-\frac{1}{|p|}\right)=:a(m)\in\mathbb{C}.$$

Por consiguiente, de la *Proposición 3.3*, se concluye que

$$\begin{aligned}\lim_{s\to 1^+}(s-1)L(s,\chi_o)&=\lim_{s\to 1^+}(s-1)\zeta(s)\lim_{s\to 1^+}\prod_{p|m}\left(1-\frac{1}{|p|^s}\right)\\&=\frac{1}{\log q}a(m)\\&=\frac{a(m)}{\log q}.\end{aligned}$$

(ii). Aplicando la derivada de un producto a la igualdad $L(s,\chi_o)=\zeta(s)\prod_{p|m}\left(1-\frac{1}{|p|^s}\right)$, llegamos a

$$L'(s,\chi_o)=\zeta'(s)\prod_{p|m}(1-|p|^{-s})+\zeta(s)\left(\prod_{p|m}(1-|p|^{-s})\right)'.$$

Entonces,

$$\begin{aligned}\lim_{s\to 1^+}\frac{L'(s,\chi_o)}{L(s,\chi_o)}&=\lim_{s\to 1^+}\left[\frac{\zeta'(s)}{\zeta(s)}+\frac{\left(\prod_{p|m}(1-|p|^{-s})\right)'}{\prod_{p|m}(1-|p|^{-s})}\right]\\&=\lim_{s\to 1^+}\frac{\zeta'(s)}{\zeta(s)}+\frac{a'(m)}{a(m)}.\end{aligned}$$

Como

$$\frac{\zeta'(s)}{\zeta(s)}=\frac{(q^{1-s}\log q)/(1-q^{1-s})^2}{(1-q^{1-s})^{-1}}=\frac{q^{1-s}\log q}{1-q^{1-s}},$$

la cual tiende a ∞ cuando $s\to 1^+$, se verifica así la afirmación.

■

3.2. Prueba del Teorema.

Demostración del Teorema 3.1. Del *Corolario 3.1* tenemos

$$\log L(s,\chi)=\sum_{k=1}^{\infty}\sum_{p\in P(q;t)}\frac{\chi(p^k)}{k|p|^{ks}},$$

pues $L(s,\chi)\neq 0$ para cualquier carácter χ, y $\Re(s)=\sigma>1$. Al tomar la derivada logarítmica de $L(s,\chi)$ para $\sigma>1$, tenemos

$$\begin{aligned}\frac{d}{ds}\log L(s,\chi)&=\frac{d}{ds}\left(\sum_{k=1}^{\infty}\sum_{p\in P(q;t)}\frac{\chi(p^k)}{k|p|^{ks}}\right)\\&=\sum_{k=1}^{\infty}\sum_{p\in P(q;t)}\frac{d}{ds}\left(\frac{\chi(p^k)}{k|p|^{ks}}\right)\end{aligned}$$

$$= \sum_{k=1}^{\infty} \sum_{p \in P(q;t)} \Big(- \frac{\chi(p^k) \log |p|}{|p|^{ks}} \Big)$$
$$= - \sum_{k=1}^{\infty} \sum_{p \in P(q;t)} \frac{\chi(p^k) \log |p|}{|p|^{ks}}.$$

Entonces,

$$\frac{L'(s,\chi)}{L(s,\chi)} = - \sum_{k=1}^{\infty} \sum_{p \in P(q;t)} \frac{\chi(p^k) \log |p|}{|p|^{ks}}. \tag{3.4}$$

Si multiplicamos ambos miembros de (3.4) por $\overline{\chi}(a)$ y sumamos sobre todos los χ, obtenemos

$$- \sum_{\chi} \overline{\chi}(a) \frac{L'(s,\chi)}{L(s,\chi)} = \sum_{\chi} \overline{\chi}(a) \sum_{k=1}^{\infty} \sum_{p \in P(q;t)} \frac{\chi(p^k) \log |p|}{|p|^{ks}}.$$

Además, si $o(\widehat{G}) = r$, entonces

$$\begin{aligned}
&\sum_{\chi} \overline{\chi}(a) \sum_{k=1}^{\infty} \sum_{p \in P(q;t)} \frac{\chi(p^k) \log |p|}{|p|^{ks}} \\
&= \overline{\chi}_0(a) \sum_{k=1}^{\infty} \sum_{p \in P(q;t)} \frac{\chi_o(p^k) \log |p|}{|p|^{ks}} + \overline{\chi}_1(a) \sum_{k=1}^{\infty} \sum_{p \in P(q;t)} \frac{\chi_1(p^k) \log |p|}{|p|^{ks}} + \cdots \\
&\quad + \overline{\chi}_{r-1}(a) \sum_{k=1}^{\infty} \sum_{p \in P(q;t)} \frac{\chi_{r-1}(p^k) \log |p|}{|p|^{ks}} \\
&= \overline{\chi}_0(a) \left[\sum_{p \in P(q;t)} \frac{\chi_o(p) \log |p|}{|p|^{s}} + \sum_{p \in P(q;t)} \frac{\chi_o(p^2) \log |p|}{|p|^{2s}} + \cdots \right] \\
&\quad + \overline{\chi}_1(a) \left[\sum_{p \in P(q;t)} \frac{\chi_1(p) \log |p|}{|p|^{s}} + \sum_{p \in P(q;t)} \frac{\chi_1(p^2) \log |p|}{|p|^{2s}} + \cdots \right] + \cdots \\
&\quad + \overline{\chi}_{r-1}(a) \left[\sum_{p \in P(q;t)} \frac{\chi_{r-1}(p) \log |p|}{|p|^{s}} + \sum_{p \in P(q;t)} \frac{\chi_{r-1}(p^2) \log |p|}{|p|^{2s}} + \cdots \right] \\
&= \overline{\chi}_0(a) \left[\left(\frac{\chi_o(p_1) \log |p_1|}{|p_1|^{s}} + \frac{\chi_o(p_2) \log |p_2|}{|p_2|^{s}} + \cdots \right) \right. \\
&\quad \left. + \left(\frac{\chi_o(p_1^2) \log |p_1|}{|p_1|^{2s}} + \frac{\chi_o(p_2^2) \log |p_2|}{|p_2|^{2s}} + \cdots \right) + \cdots \right] \\
&\quad + \overline{\chi}_1(a) \left[\left(\frac{\chi_1(p_1) \log |p_1|}{|p_1|^{s}} + \frac{\chi_1(p_2) \log |p_2|}{|p_2|^{s}} + \cdots \right) \right. \\
&\quad \left. + \left(\frac{\chi_1(p_1^2) \log |p_1|}{|p_1|^{2s}} + \frac{\chi_1(p_2^2) \log |p_2|}{|p_2|^{2s}} + \cdots \right) + \cdots \right] + \cdots \\
&\quad + \overline{\chi}_{r-1}(a) \left[\left(\frac{\chi_{r-1}(p_1) \log |p_1|}{|p_1|^{s}} + \frac{\chi_{r-1}(p_2) \log |p_2|}{|p_2|^{s}} + \cdots \right) \right. \\
&\quad \left. + \left(\frac{\chi_{r-1}(p_1^2) \log |p_1|}{|p_1|^{2s}} + \frac{\chi_{r-1}(p_2^2) \log |p_2|}{|p_2|^{2s}} + \cdots \right) + \cdots \right]
\end{aligned}$$

$$
\begin{aligned}
&= \left[\frac{\log|p_1|}{|p_1|^s}\big(\overline{\chi}_0(a)\chi_0(p_1) + \overline{\chi}_1(a)\chi_1(p_1) + \cdots + \overline{\chi}_{r-1}(a)\chi_r(p_1)\big) \right.\\
&\quad \left. + \frac{\log|p_2|}{|p_2|^s}\big(\overline{\chi}_0(a)\chi_0(p_2) + \overline{\chi}_1(a)\chi_1(p_2) + \cdots + \overline{\chi}_{r-1}(a)\chi_{r-1}(p_2)\big) + \cdots \right]\\
&\quad + \left[\frac{\log|p_1|}{|p_1|^{2s}}\big(\overline{\chi}_0(a)\chi_0(p_1^2) + \overline{\chi}_1(a)\chi_1(p_1^2) + \cdots + \overline{\chi}_{r-1}(a)\chi_r(p_1^2)\big) \right.\\
&\quad \left. + \frac{\log|p_2|}{|p_2|^{2s}}\big(\overline{\chi}_0(a)\chi_0(p_2^2) + \overline{\chi}_1(a)\chi_1(p_2^2) + \cdots + \overline{\chi}_{r-1}(a)\chi_{r-1}(p_2^2)\big) + \cdots \right] + \cdots\\
&= \left(\frac{\log|p_1|}{|p_1|^s}\sum_{\chi}\overline{\chi}(a)\chi(p_1) + \frac{\log|p_2|}{|p_2|^s}\sum_{\chi}\overline{\chi}(a)\chi(p_2) + \cdots \right)\\
&\quad + \left(\frac{\log|p_1|}{|p_1|^{2s}}\sum_{\chi}\overline{\chi}(a)\chi(p_1^2) + \frac{\log|p_2|}{|p_2|^{2s}}\sum_{\chi}\overline{\chi}(a)\chi(p_2^2) + \cdots \right) + \cdots\\
&= \sum_{p\in P(q;t)} \frac{\log|p|}{|p|^s}\sum_{\chi}\overline{\chi}(a)\chi(p) + \sum_{p\in P(q;t)} \frac{\log|p|}{|p|^{2s}}\sum_{\chi}\overline{\chi}(a)\chi(p^2) + \cdots\\
&= \sum_{k=1}^{\infty}\sum_{p\in P(q;t)} \frac{\log|p|}{|p|^{ks}}\sum_{\chi}\overline{\chi}(a)\chi(p^k).
\end{aligned}
$$

Así,

$$
-\sum_{\chi}\overline{\chi}(a)\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{k=1}^{\infty}\sum_{p\in P(q;t)} \frac{\log|p|}{|p|^{ks}}\sum_{\chi}\overline{\chi}(a)\chi(p^k),
$$

de donde, usando el *Lema 1.1*,

$$
-\sum_{\chi}\overline{\chi}(a)\frac{L'(s,\chi)}{L(s,\chi)} = \varphi(m)\sum_{k=1}^{\infty}\sum_{\substack{p\in P(q;t)\\ p^k\equiv a \bmod m}} \frac{\log|p|}{|p|^{ks}}. \tag{3.5}
$$

Como $L(1,\chi)\neq 0$ para todo $\chi\neq\chi_o$ (por *Corolario 2.3* y *Teorema 2.3*), usando el *Corolario 3.2*, parte *(ii)*, y teniendo en cuenta que $L(s,\chi_o)\neq 0$, vemos que el lado izquierdo de (3.5) tiende a ∞ cuando $s\to 1^+$, es decir,

$$
\sum_{k=1}^{\infty}\sum_{\substack{p\in P(q;t)\\ p^k\equiv a \bmod m}} \frac{\log|p|}{|p|^{ks}} \to \infty \quad \text{si} \quad s\to 1^+. \tag{3.6}
$$

Como $s>1$, $|p|^{ks} > |p|^k$, para $k\geqslant 2$, por consiguiente $\dfrac{1}{|p|^k} > \dfrac{1}{|p|^{ks}}$, para $k\geqslant 2$. Por lo tanto,

$$
\sum_{k=2}^{\infty}\sum_{\substack{p\in P(q;t)\\ p^k\equiv a \bmod m}} \frac{\log|p|}{|p|^{ks}} < \sum_{k=2}^{\infty}\sum_{\substack{p\in P(q;t)\\ p^k\equiv a \bmod m}} \frac{\log|p|}{|p|^{k}}.
$$

Por otro lado,

$$
\sum_{p\in P(q;t)} \frac{\log|p|}{|p|^k} = \sum_{\substack{p\in P(q;t)\\ p^k\equiv a \bmod m}} \frac{\log|p|}{|p|^k} + \sum_{\substack{p\in P(q;t)\\ p^k\not\equiv a \bmod m}} \frac{\log|p|}{|p|^k} > \sum_{\substack{p\in P(q;t)\\ p^k\equiv a \bmod m}} \frac{\log|p|}{|p|^k}.
$$

Es decir,

$$\sum_{k=2}^{\infty} \sum_{\substack{p\in P(q;t)\\ p^k\equiv a \text{ mód } m}} \frac{\log|p|}{|p|^{ks}} < \sum_{k=2}^{\infty} \sum_{p\in P(q;t)} \frac{\log|p|}{|p|^{k}}.$$

Entonces,

$$\begin{aligned}
\sum_{k=2}^{\infty} \sum_{\substack{p\in P(q;t)\\ p^k\equiv a \text{ mód } m}} \frac{\log|p|}{|p|^{ks}} &< \sum_{k=2}^{\infty} \sum_{p\in P(q;t)} \frac{\log|p|}{|p|^{k}} \\
&= \sum_{p\in P(q;t)} \frac{\log|p|}{|p|^2} + \sum_{p\in P(q;t)} \frac{\log|p|}{|p|^3} + \cdots \\
&= \left(\frac{\log|p_1|}{|p_1|^2} + \frac{\log|p_2|}{|p_2|^2} + \cdots\right) + \left(\frac{\log|p_1|}{|p_1|^3} + \frac{\log|p_2|}{|p_2|^3} + \cdots\right) + \cdots \\
&= \left(\frac{\log|p_1|}{|p_1|^2} + \frac{\log|p_1|}{|p_1|^3} + \cdots\right) + \left(\frac{\log|p_2|}{|p_2|^2} + \frac{\log|p_2|}{|p_2|^3} + \cdots\right) + \cdots \\
&= \log|p_1| \sum_{k=2}^{\infty} \frac{1}{|p_1|^k} + \log|p_2| \sum_{k=2}^{\infty} \frac{1}{|p_2|^k} + \cdots \\
&= \sum_{p\in P(q;t)} \log|p| \sum_{k=2}^{\infty} \frac{1}{|p|^k} \\
&= \sum_{p\in P(q;t)} \frac{\log|p|}{|p|(|p|-1)},
\end{aligned}$$

ya que,

$$\begin{aligned}
\frac{1}{|p|} + \sum_{k=2}^{\infty} \frac{1}{|p|^k} = \sum_{k=1}^{\infty} \frac{1}{|p|^k} &= \lim_{n\to\infty} \sum_{k=1}^{n} \frac{1}{|p|^k} \\
&= \lim_{n\to\infty} \frac{\frac{1}{|p|}\left(1-\frac{1}{|p|^n}\right)}{1-\frac{1}{|p|}} \\
&= \frac{\frac{1}{|p|}}{1-\frac{1}{|p|}} = \frac{1}{|p|-1},
\end{aligned}$$

o

$$\sum_{k=2}^{\infty} \frac{1}{|p|^k} = \frac{1}{|p|-1} - \frac{1}{|p|} = \frac{1}{|p|(|p|-1)}.$$

De (3.6), de la igualdad

$$\sum_{k=1}^{\infty} \sum_{\substack{p\in P(q;t)\\ p^k\equiv a \text{ mód } m}} \frac{\log|p|}{|p|^{ks}} = \sum_{\substack{p\in P(q;t)\\ p\equiv a \text{ mód } m}} \frac{\log|p|}{|p|^{s}} + \sum_{k=2}^{\infty} \sum_{\substack{p\in P(q;t)\\ p^k\equiv a \text{ mód } m}} \frac{\log|p|}{|p|^{ks}},$$

y como la serie a la derecha de la desigualdad probada anteriormente es absolutamente convergente, usando la serie

$$\sum_{p\in P(q;t)} \frac{\log|p|}{|p|^2}$$

que es convergente por el criterio de la integral, entonces, por fuerza,

$$\sum_{\substack{p\in P(q;t)\\ p\equiv a \text{ mód } m}} \frac{\log|p|}{|p|^s} \to \infty \quad \text{cuando} \quad s \to 1^+,$$

lo cual indica que el número de elementos $p \in P(q;t)$ que cumplen $p \equiv a$ mód m es infinito. ■

Bibliografía

[1] Víctor S. Albis, *Lecciones sobre la Aritmética de Polinomios*, Policopiado, Universidad Nacional de Colombia, 2002.

[2] Paul Pollack, *An Elementary Proof of Dirichlet's Theorem in the Polynomial Setting*, Preimpreso.

[3] Tom M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, New York, 1998.

[4] Kenneth Ireland and Michel Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, New York, 1991.

[5] Heinrich Kornblum, *Über Die Primfunktionen in Einer Arithmetischen Progression*, Mathematische Zeitschrift, 1919.

[6] Michael Rosen, *Number Theory in Function Fields*, Springer-Verlag, New York, New York, 2002.

[7] Harold N. Shapiro, *On Primes in Arithmetic Progression, II*, Annals of Mathematics, 1950.

[8] Dirichlet, P. G. Lejeune (1837) Beweis des Satzes, *dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschlaftichen Factor sind*, unendliche viele Primzahlen enthglt. Abhand. Ak. Wiss. Berlin: 45-81. [Werke, 1: 315-342].

[9] Carlos Ivorra Castillo, *Teoría de Números*, se encuentra en la página http://www.uv.es/ivorra/Libros/Numeros.pdf

[10] Ramanujachary Kumandury, Cristina Romero, *Number Theory With Computer Applications*, Prentice Hall, 1998.

[11] Thomas W. Hungerford, *Abstract Algebra An Introduction*, Saunders College Publishing, 1996.

[12] I. N. Herstein, *Topics in Algebra*, New York, Blaisdell 1964.

[13] J. Rotman, *Advanced Algebra*, Second Printing, Prentice Hall, 2003.