UNIVERSIDAD DE PANAMÁ
VICERRECTORÍA DE INVESTIGACIÓN Y POSTGRADO
PROGRAMA DE MAESTRÍA EN MATEMÁTICA

ESTUDIO DE LAS FUNCIONES ARITMÉTICAS SOBRE EL MONOIDE DE LOS POLINOMIOS

POR:

FELICIANO BATISTA G.

TESIS PRESENTADA COMO UNO DE LOS REQUISITOS PARA OPTAR AL GRADO DE MAESTRO EN CIENCIAS CON ESPECIALIZACIÓN EN MATEMÁTICA.

PANAMÁ, REPÚBLICA DE PANAMÁ

1993

UNIVERSIDAD DE PANAMA

ULTAD DE CIENCIAS NATURALES Y EXACTAS

Panamá, ____________________

Aprobado por:

Director de Tesis *Jorge Hernández*
JORGE HERNANDEZ Ph.D.

Miembro del Jurado *Evangelista González*
EVANGELISTA GONZALEZ M.Sc.

Miembro del Jurado *Josué Ortiz Gutiérrez*
JOSUE ORTIZ M.Sc.

Fecha: *23 de Abril de 1993.*

DEDICATORIA

A mis hijos, FELIX ORLANDO
y MELVA JARISSA.

FELICIANO

AGRADECIMIENTO

Al Doctor VICTOR ALBIS, por su
apoyo y asesoría.
A todos mis compañeros, en
especial, a JAIME GUTIERREZ por
su valiosa colaboración.

CONTENIDO

CONTENIDO

INTRODUCCIÓN

INTRODUCCION

En el presente trabajo estudiaremos las funciones aritméticas sobre el monoide de los polinomios mónicos, en la indeterminada X sobre un cuerpo finito $\mathbb{F}_q$, comparando algunos resultados aquí obtenidos, con aquellos que les son análogos en el monoide $\mathbb{N}^*$.

El objeto fundamental de este trabajo es el de encontrar expresiones y Ordenes promedios para algunas funciones aritméticas en el monoide $\mathbb{M}(q;X)$. Para ello necesitaremos primero establecer un isomorfismo entre el álgebra de Dirichlet (Dir $(\mathbb{M})$) y el álgebra de las series formales, el cual nos permitirá escribir algunas funciones aritméticas como producto de funciones ζ-de Riemann, obteniendo así expresiones para los coeficientes q^{-kz} a partir de los cuales analizaremos el comportamiento de estas funciones.

Nuestra obra consta de tres capítulos los cuales detallaremos a continuación:

El primer capítulo, en su primera parte, recoge el álgebra de las funciones aritméticas, determinando el inverso de una función aritmética, funciones multiplicativas y completamente multiplicativas, estableciendo condiciones que nos permiten analizar el comportamiento de éstas sobre las potencias de primos de $\mathbb{P}$ en $\mathbb{M}$. Además se estudian algunas funciones aritméticas en especial ($u, \mu, d, d_r\ \sigma_t, \lambda, \Lambda, \phi$ etc.), dando condiciones necesarias y suficientes con la utilización de la fórmula de Inversión y el Teorema de Möbius para determinar cuando una función es multiplicativa o completamente multiplicativa.

En la segunda parte del primer capítulo establecemos un *isomorfismo* entre el álgebra de Dirichlet ($Dir(\mathbb{M})$) y el álgebra de las series formales, el cual será herramienta de gran utilidad en el descubrimiento de nuestros resultados finales. Definimos también, en esta sección una norma ($\|\ \|$) en $Dir(\mathbb{M})$ y estudiamos algunas propiedades topológicas de $Dir(\mathbb{M})$.

En el segundo capítulo hacemos un estudio de las funciones ζ-de Riemann la que tiene como expresión la serie formal $\zeta(z) = \sum_{K=0}^{\infty} (\sum_{|A|=k} 1) q^{-kz} = \tilde{u}(z)$. Analizamos además las funciones *Primo Independiente Multiplicativa*, esto con la escritura de ζ en serie formal nos ayudará a escribir algunas funciones aritméticas como producto de funciones ζ, los que nos permitirán encontrar expresiones para los coeficientes q^{-kz}. Finalmente exhibiremos condiciones necesarias y suficientes para expresar una función aritmética como producto finito o infinito de funciones ζ-de Riemann. Es, pues, en este capítulo donde damos las bases necesarias para satisfacer el objetivo fundamental.

En el tercer capítulo analizamos el comportamiento de algunas funciones aritméticas para valores relativamente grandes de $|A(X)|$; éste se analiza comparando el comportamiento de la función con el comportamiento de una función conocida, y así obtenemos el orden promedio de algunas funciones aritméticas cuyas expresiones para los coeficientes q^{-kz} en $\mathbb{M}(q,X)$ han sido estudiadas en el segundo capítulo. Además estudiamos algunas conjeturas (Mestens, Turán, Pólya) comparando su comportamiento en $\mathbb{M}(q;X)$ con su comportamiento en $\mathbb{N}^*$.

Esperamos que este trabajo incentive a la investigación del comportamiento de las funciones aritméticas en cualquier otro monoide.

CAPÍTULO I

EL ÁLGEBRA DE LAS FUNCIONES ARITMÉTICAS

CAPITULO I

EL ALGEBRA DE LAS FUNCIONES ARITMETICAS

I.1 CONCEPTOS FUNDAMENTALES.

Las "funciones aritméticas" que estudiaremos aquí son generalizaciones de las funciones aritméticas de la teoría clásica de los números. Estas últimas están definidas en el monoide $\mathbb{N}$ de los números enteros ≥ 1 y la generalización que haremos aquí, empieza por sustituir este monoide por otros, cuyas estructuras le son semejantes.

Para nosotros un monoide o semigrupo conmutativo $\mathbb{M}$ es un conjunto provisto de una ley de composición $.(A,B) \longrightarrow AB$ que es asociativa y conmutativa. Además supondremos que $\mathbb{M}$ es unitario, es decir, que existe $1 \in \mathbb{M}$ tal que $A1 = A$ para todo $A \in \mathbb{M}$.

Para mantener la analogía con $\mathbb{N}$ supondremos también que $\mathbb{M}$ tiene un subconjunto $\mathbb{P}$ (llamado el conjunto de los elementos primos de $\mathbb{M}$) tal que todo elemento $A \in \mathbb{M}$, $A \neq 1$ se escribe de manera única en la forma

$$A = p_1^{\alpha_1} . p_2^{\alpha_2} \dots p_k^{\alpha_k} \ ; \ P_i \in \mathbb{P}, \quad \alpha_i \text{ entero } \geq 0$$

Es decir, $\mathbb{M}$ es un monoide factorial o con factorización única (en sus elementos primos).

A partir de este momento, todos los monoides considerados en este trabajo serán monoides factoriales.

Definición 1.1.1: Si existe una aplicación norma $|\ |. \mathbb{M} \longrightarrow \mathbb{Z}$, es decir, tal que

(i) $|1| = 1$; $|P| > 1$ para $p \in \mathbb{P}$,

(ii) $|AB| = |A||B|$, para $A,B \in \mathbb{M}$,

(iii) $G(n) = \sum_{\substack{A \in \mathbb{M} \\ |A|=n}} 1 < \infty$ $(n = 1,2,3, \ldots)$

decimos que $(\mathbb{M}, |\ |)$ es un semigrupo aritmético.

Definición 1.1.2: Si existe una aplicación grado $\partial : \mathbb{M} \longrightarrow \mathbb{Z}$, es decir, tal que:

(i') $\partial(1) = 0$; $\partial(P) > 0$ para $P \in \mathbb{P}$,

(ii') $\partial(AB) = \partial(A) + \partial(B)$ para $A,B \in \mathbb{M}$,

(iii') $\hat{G}(n) = \sum_{\substack{A \in \mathbb{M} \\ \partial(A) = n}} 1 < \infty$ $(n = 1,2,3,\ldots)$

decimos que $(\mathbb{M}, \partial)$ es un semigrupo aritmético aditivo.

Proposición 1.1.1: Todo semigrupo aritmético aditivo es un semigrupo aritmético.

Prueba: Sea q un número real >1. Haciendo $|A| = q^{\partial(A)}$ verificamos que $|\ |$ es una función norma. En efecto, por definición $|1| = q^{\partial(1)} = q^0 = 1$; además, si $P \in \mathbb{P}$, $|P| = q^{\partial(P)} > 1$ pues $\partial(P) > 0$. Esto verifica (i). La relación $|AB| = q^{\partial(AB)} = q^{\partial(A)+\partial(B)} = |A||B|$, no es otra cosa que (ii). Finalmente, sea $n \in \mathbb{N}$; si $n \neq q^m (m=1,2,\ldots)$, entonces

$$G(n) = \sum_{\substack{A \in \mathbb{M} \\ |A|=n}} 1 = \sum_{\substack{A \in \mathbb{M} \\ q^{\partial(A)} = n}} 1 = 0$$

Ahora bién si $n = q^m$ para algún $m = 1,2,\ldots$, entonces

$$G(n) = \sum_{\substack{A \in \mathbb{M} \\ |A|=n}} 1 = \sum_{\substack{A \in \mathbb{M} \\ q^{\partial(A)} = q^m}} 1 = \sum_{\substack{A \in \mathbb{M} \\ \partial(A)=m}} 1 = \hat{G}(m) < \infty$$

Luego en cualquier circunstancia $G(n) < \infty$

Ejemplos:

(1-) Sean $\mathbb{M} = \mathbb{N}$ y $\mathbb{P} = \{$números primos $> 1\}$. Si $|n| = n$ para $n \in \mathbb{N}$, todos sabemos que $(\mathbb{N}, |\,|)$ es un semigrupo aritmético y $G(n)=1$.

(2-) Si $\mathbb{M} = \mathbb{M}(q,X)$ es el conjunto de todos los polinomios unitarios (es decir, de coeficiente director igual a uno) en la indeterminada X y con coeficientes en un cuerpo finito $\mathbb{F}_q$ de q elementos, un conocido teorema (si $\mathbb{K}$ es un cuerpo, el anillo $\mathbb{K}[X]$ es factorial) nos dice que todo elemento $A(X) \in \mathbb{M}$ puede escribirse de manera única así:

$$A(X) = P_1(X)^{\alpha_1} \dots P_k(X)^{\alpha_k} \; ; \; (\alpha_i \geqslant 1),$$

donde cada $P_i(X) \in \mathbb{P} = \mathbb{P}(q;X) = \{$ polinomios irreducibles unitarios $\}$. Denotando con $\partial(A(X)) = \partial(A)$ al grado del polinomio $A(X)$, propiedades elementales y bien conocidas de los polinomios nos dicen que $(\mathbb{M}(q;X), \partial)$ es un semigrupo aritmético aditivo, pues, también se tiene

$$\hat{G}(n) = \sum_{\substack{A(X) \in \mathbb{M}(q;X) \\ \partial(A) = n}} 1 = q^n < \infty$$

El valor $|A(X)| = n(A) = q^{\partial(A)}$ se conoce en la literatura como la <u>norma del polinomio $A(X)$</u>. Claramente, $(\mathbb{M}(q,X), |\,|)$ es un semigrupo aritmético.

Observemos que en un monoide factorial $\mathbb{M}$ existe una <u>relación de divisibilidad</u> definida así:

$A|B$ si existe $C \in \mathbb{M}$ tal que $B = AC$,

que satisface además las siguientes propiedades.

(D1) $A|A$ para todo A.

(D2) Si $A|B$ y $B|C$, entonces $A|C$.

(D3) Si $A|B$ y $B|A$, entonces $A = B$

Si $A|B$ decimos que A es un divisor de B. El elemento $C \in \mathbb{M}$ tal que $B = AC$ se escribe $C = B/A$. También tenemos la noción de máximo común divisor (A,B) de dos elementos $A,B \in \mathbb{M}$, definida de manera obvia. Dualmente, tenemos la de mínimo común múltiplo $[A,B]$, y, en general todas aquellas propiedades de $\mathbb{N}$ que dependen unicamente de la factorización única.

Definición 1.1.3: Sean $\mathbb{M}$ un semigrupo aritmético y $\mathbb{C}$ el cuerpo de los números complejos. Toda función $f:\mathbb{M} \longrightarrow \mathbb{C}$ se llama una función aritmética. Al conjunto de todas estas funciones se le denota con $\mathrm{Dir}(\mathbb{M})$.

En $\mathrm{Dir}(\mathbb{M})$ podemos definir una suma, así:

$(f+g)(A) = f(A) + g(A)$, para $A \in \mathbb{M}$, $f,g \in \mathrm{Dir}(\mathbb{M})$ un producto por escalares así:

$(\lambda f)(A) = \lambda(f(A))$ para $A \in \mathbb{M}$, $f \in \mathrm{Dir}(\mathbb{M})$, $\lambda \in \mathbb{C}$

y un producto $*$ entre funciones aritméticas, así:

$$(f * g)(A) = \sum_{D|A} f(D)g(A/D)$$

Este producto $*$ se suele llamar convolución de Dirichlet.

Proposición 1.1.2: $\mathrm{Dir}(\mathbb{M})$ con las operaciones anteriores conforma una $\mathbb{C}$-álgebra conmutativa unitaria, que llamaremos el álgebra de Dirichlet de $\mathbb{M}$.

Prueba Que $\mathrm{Dir}(\mathbb{M})$ es un $\mathbb{C}$-espacio vectorial, resulta de un hecho general muy conocido. Pasemos, pues, a verificar que es un $\mathbb{C}$-álgebra conmutativa. En efecto, si $f,g \in Dir(\mathbb{M})$ y $A \in \mathbb{M}$, entonces

$$\begin{aligned}(f*g)(A) &= \sum_{D|A} f(D)g(A/D) = \sum_{DC=A} f(D)g(C) \\ &= \sum_{DC=A} g(C)f(D) = \sum_{C|A} g(C)f(A/C) \\ &= (g*f)(A)\end{aligned}$$

lo que muestra que $*$ es conmutativo. Veamos que $*$ es asociativo.

Sean, $f,g,h \in Dir(\mathbb{M})$, $A \in \mathbb{M}$, de modo que

$$\begin{aligned}[f*(g*h)](A) &= \sum_{D|A} f(D)(g*h)(A/D) \\ &= \sum_{CD=A} f(D)\Big(\sum_{C=EF} g(E)h(F)\Big) \\ &= \sum_{DEF=A} f(D)g(E)h(F)\end{aligned}$$

De manera análoga se desarrolla $[(f*g)*h](A)$ y se verificará que es igual al último miembro derecho de las anteriores igualdades. Verifiquemos ahora que el producto $*$ distribuye respecto a la suma. Sean, pues, $f,g,h \in Dir(\mathbb{M})$; $A \in \mathbb{M}$; entonces

$$\begin{aligned}[(f+g)*h](A) &= \sum_{D|A} (f+g)(D)h(A/D) \\ &= \sum_{D|A} (f(D)+g(D))h(A/D) \\ &= \sum_{D|A} f(D)h(A/D) + \sum_{D|A} g(D)h(A/D) \\ &= (f*h)(A) + (g*h)(A)\end{aligned}$$

Enseguida, mostraremos que $(\lambda f)*g = f*(\lambda g) = \lambda(f*g)$. En efecto, sean $f,g \in Dir(\mathbb{M})$, $\lambda \in \mathbb{C}$, $A \in \mathbb{M}$; entonces

$$\begin{aligned}
[(\lambda f)*g](A) &= \sum_{D|A} (\lambda f)(D)g(A/D) \\
&= \sum_{D|A} \lambda f(D)g(A/D) \\
&= \sum_{D|A} f(D)\,[\lambda g(A/D)] \\
&= [f*(\lambda g)](A) \\
&= \lambda \sum_{D|A} f(D)g(A/D) \\
&= [\lambda(f*g)](A)
\end{aligned}$$

Finalmente, $Dir(\mathbb{M})$ es unitaria pues la función aritmética.

$$I(A) = \begin{cases} 1 & \text{si } A = 1 \\ 0 & \text{si } |A| > 1 \end{cases}$$

satisface

$$(f*I)(A) = \sum_{D|A} f(D)I(A/D) = f(A)$$

es decir, $f*I = f$, para toda $f \in Dir(\mathbb{M})$ lo que indica que I es la unidad para el producto.

Pasaremos ahora a determinar los elementos invertibles de $Dir(\mathbb{M})$. Para ello tomemos $f \in Dir(\mathbb{M})$, $f \neq \theta$ y tal que $f(1) \neq 0$. Queremos determinar $f^{-1} \in Dir(\mathbb{M})$ tal que $f^{-1}*f = f*f^{-1} = I$; para ello basta determinar $f^{-1}(A)$ para cada $A \in \mathbb{M}$. Procederemos por inducción sobre $|A|$. Si $A = 1$ entonces

$$(f*f^{-1})(1) = f(1)f^{-1}(1) = 1;$$

de donde $f^{-1}(1) = \dfrac{1}{f(1)}$. Supongamos ahora que $f^{-1}(A)$ ha sido determinado para todos los $A \in \mathbb{M}$ que cumplen $|A| < n$. Si tomamos $B \in \mathbb{M}$ tal que $|B| = n$, tenemos

$$0 = I(B) = (f*f^{-1})(B) = \sum_{D|B} f(B/D)f^{-1}(D)$$

$$= f(1)f^{-1}(B) + \sum_{\substack{D|B \\ 0<|D|<n}} f(B/D)f^{-1}(D)$$

como para $|D| < n$, $f^{-1}(D)$ esta ya determinado, por hipótesis de inducción, vemos que $f^{-1}(B)$ queda determinado por

$$f^{-1}(B) = -\frac{1}{f(1)} \sum_{\substack{D|B \\ |D|<n}} f(B/D)f^{-1}(D)$$

Recíprocamente, si f^{-1} existe, entonces de $f*f^{-1} = I$, resulta inmediatamente que $f(1)f^{-1}(1) = 1$, es decir, $f(1) \neq 0$. Hemos, pues, demostrado la siguiente·

Proposición 1.1.3: Los elementos $f \in Dir(\mathbb{M})$ que son invertibles son precisamente aquellos que cumplen $f(1) \neq 0$.

Por la construcción inductiva hecha en la demostración de esta proposición, resulta claro que f^{-1} es único. El conjunto $\{ f \in Dir(\mathbb{M}),\ f(1) \neq 0 \}$ es, pues, un grupo para la multiplicación y se le denota con $Dir^{x}(\mathbb{M})$.

Definición 1.1.4: Sea f una función aritmética $f \neq 0$. Decimos que f es multiplicativa si $f(AB) = f(A)f(B)$ cada vez que $(A,B) = 1$. Si $f(AB) = f(A)f(B)$ para todo par de elementos A y B en $\mathbb{M}$, decimos que f es completamente multiplicativa.

Es claro que toda función completamente multiplicativa es multiplicativa. Por otra parte, como $(A,1) = 1$ y

$$f(A) = f(A.1) = f(A)f(1),$$

si f es multiplicativa, vemos que $f(1) = 1$. Por lo tanto, toda función multiplicativa es invertible.

Las siguientes funciones son completamente multiplicativas $|A|^{\alpha}$, $\alpha\in\mathbb{C}$, en particular $\mathcal{U}(A) = |A|^{0} = 1$, para todo $A\in\mathbb{M}$. También lo es la función unidad $I(A)$. Como veremos luego no toda función multiplicativa es completamente multiplicativa.

Proposición 1.1.4: Las funciones multiplicativas conforman un subgrupo de $\mathrm{Dir}^{X}(\mathbb{M})$.

Prueba: Sean f y g dos funciones multiplicativas (ya hemos visto que estas son invertibles). Si A y $B\in\mathbb{M}$ son tales que $(A,B) = 1$, entonces

$$\begin{aligned}(f*g)(AB) &= \sum_{D|AB} f(D)g(AB/D)\\ &= \sum_{\substack{M|A\\ N|B}} f(MN)g(AB/MN)\\ &= \sum_{\substack{M|A\\ N|B}} f(M)f(N)g(A/M)g(A/N)\\ &= \left[\sum_{M|A} f(M)g(A/M)\right]\left[\sum_{N|B} f(N)g(B/N)\right]\\ &= \left[(f*g)(A)\right]\left[(f*g)(B)\right],\end{aligned}$$

donde hemos usado el hecho que si $(A,B) = 1$ y $D|AB$, entonces $D = MN$, $M|A$, $N|B$ y $(A/M, B/N) = 1$. Luego el producto de dos funciones multiplicativas es una función multiplicativa. Veamos finalmente que el inverso de una función multiplicativa f también lo es. Como en este caso $f(1) = 1$ tenemos que $f^{-1}(1) = 1$. Si $P \in \mathbb{P}$ y $e \geqslant 1$ tenemos que

$$0 = I(P^e) = (f*f^{-1})(P^e)$$

Consideremos la única función multiplicativa h tal que $f^{-1}(P^e) = h(P^e)$, para todo $P \in \mathbb{P}$ y todo $e \geqslant 1$ entonces $(f*h)(P^e) = I(P^e)$ para todo $P \in \mathbb{P}$ y $e \geqslant 1$. Como tanto f como h son multiplicativas; vemos que $f*h$ es multiplicativa y, por tanto,

$$(f*h)(A) = I(A) = (f*f^{-1})(A), \text{ para todo } A \in \mathbb{M}; \text{ es}$$

decir, $f*h = f*f^{-1} = I$. La unicidad del inverso nos dice ahora que $h = f^{-1}$, lo que exige que f^{-1} sea multiplicativa.

<u>Corolario</u>: <u>Si f y g son funciones multiplicativas, entonces</u> $h(A) = \sum_{D|A} f(D)g(A/D) = (f*g)(A)$ <u>es multiplicativa</u>

<u>Proposición 1.1.5</u>: <u>Sea $f \in Dir^X(\mathbb{M})$ con</u> $f(1) = 1$ <u>entonces</u>

(a) <u>f es multiplicativa si, y solo si,</u>

$$f(P_1^{e_1} \ldots P_k^{e_k}) = f(P_1^{e_1}) \ldots f(P_k^{e_k})$$

<u>para todo $P_i \in \mathbb{P}$ y todo</u> $e_i \geqslant 1$.

(b) <u>Si f es multiplicativa, entonces f es completamente multiplicativa si, y solo si,</u>

$$f(P^e) = f(P)^e$$

para todo $P \in \mathbb{P}$ y todo entero $e \geqslant 1$.

Prueba: (a) Supongamos primero que f es multiplicativa y tomemos $P_1^{e_1}\ldots P_k^{e_k}$, $P_i \in \mathbb{P}$, $e_i \geqslant 1$. Entonces

$$f(P_1^{e_1}\ldots P_k^{e_k}) = f(P_1^{e_1})f(P_2^{e_2}\ldots P_k^{e_k}),$$

pues $(P_1^{e_1},\ldots,P_k^{e_k}) = 1$. De manera recurrente, obtenemos $f(P_1^{e_1}\ldots P_k^{e_k}) = f(P_1^{e_1})\ldots f(P_k^{e_k})$. Recíprocamente, si $(A,B) = 1$, entonces $A = P_1^{e_1}\ldots P_k^{e_k}$ y $B = Q_1^{f_1}\ldots Q_s^{f_s}$, donde los P_i, y los Q_j son mutuamente distintos y $e_i, f_j \geqslant 1$. Entonces, por hipótesis

$$\begin{aligned} f(AB) &= f(P_1^{e_1}\ldots P_k^{e_k}.Q_1^{f_1}\ldots Q_s^{f_s}) \\ &= f(P_1^{e_1})\ldots f(P_k^{e_k}).f(Q_1^{f_1})\ldots f(Q_s^{f_s}) \\ &= f(P_1^{e_1}\ldots P_k^{e_k})f(Q_1^{f_1}\ldots Q_s^{f_s}) \\ &= f(A)f(B) \end{aligned}$$

(b) Si f es completamente multiplicativa, es claro que $f(P^e)=f(P)^e$. Recíprocamente, sean $A = P_1^{e_1}\ldots P_k^{e_k}$, $B = P_1^{f_1}\ldots P_k^{f_k}$ donde $e_i, f_i \geqslant 0$. Entonces $AB = P_1^{e_1+f_1}\ P_2^{e_2+f_2}\ldots P_k^{e_k+f_k}$ y como f es multiplicativa, por hipótesis tenemos

$$\begin{aligned} f(AB) &= f(P_1^{e_1+f_1})\ldots f(P_k^{e_k+f_k}) \\ &= f(P_1)^{e_1+f_1}\ldots f(P_k)^{e_k+f_k} \\ &= f(P_1)^{e_1}\ldots f(P_k)^{e_k}\, f(P_1)^{f_1}\ldots f(P_k)^{f_k} \\ &= f(P_1^{e_1}\ldots P_k^{e_k})f(P_1^{f_1}\ldots P_k^{f_k}) \\ &= f(A)\, f(B) \end{aligned}$$

donde hemos usado la hipótesis $f(P^e) = f(P)^e$ repetidas veces.

Proposición 1.1.6: Si f es multiplicativa entonces

$$\sum_{D|A} f(D) = \prod_{j=1}^{k} \Big[\sum_{i=1}^{e_j} f(P_j^i) \Big]$$

donde $A = P_1^{e_1} \ldots P_k^{e_k}$, $e_i \geq 1$.

Prueba: Desarrollando el producto del miembro derecho tenemos

$$\prod_{j=1}^{k} \Big(\sum_{i=0}^{e_j} f(P_j^i) \Big) = (1+f(P_1)+\ldots+f(P_1^{e_1}))\times(1+f(P_2)+\ldots+f(P_2^{e_2}))\ldots (1+f(P_k)+ \ldots f(P_k^{e_k}))$$

$$= 1+f(P_1)f(P_2)+\ldots+f(P_1)f(P_k)+\ldots+f(P_1^{e_1})f(P_2^{e_2})\ldots f(P_k^{e_k})$$

$$= 1+f(P_1P_2)+\ldots+f(P_1P_k)+\ldots+f(P_1^{e_1}\ldots P_k^{e_k})$$

lo cual nos da el miembro izquierdo.

I-2 DEFINICIONES Y ESTUDIO ELEMENTAL DE ALGUNAS FUNCIONES ARITMETICAS.

La función definida por

$$\mu(A) = \begin{cases} 1 & \text{si } A = 1 \\ (-1)^k & \text{si } A = P_1\ldots P_k \text{ donde los } P_i \text{ son todos distintos} \\ 0 & \text{si existe } P \in \mathbb{P} \text{ tal que } P^2 | A. \end{cases}$$

se llama función Möbius del monoide factorial $\mathbb{M}$. Como en el caso del monoide $\mathbb{N}$, esta función tiene un carácter combinatorio en todo monoide factorial. Veámoslo

Proposición 1.2.1.

(1) $\sum_{D|A} \mu(D) = I(A)$

Prueba: Sea $A = P_1^{e_1} \ldots P_k^{e_k}$, donde $P_i \in \mathbb{P}$, $e_i \geqslant 1$. Entonces

$$\sum_{D|A} \mu(D) = \mu(1) + \mu(P_1) + \ldots \mu(P_k) + \mu(P_1P_2) + \ldots + \mu(P_1P_k) +$$

$$\ldots + \mu(P_{k-1}P_k) + \ldots + \mu(P_1 \ldots P_k)$$

$$= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \ldots + \binom{k}{k}(-1)^k$$

$$= (1-1)^k = 0$$

si $A \neq 1$

Observemos que (1) significa que $U * \mu = \mu * U = I$. Es decir $\mu = U^{-1}$. De aquí resulta fácilmente que μ es la única función que satisface (1).

Proposición 1.2.2: La función μ de Möbius es multiplicativa.

Prueba Como U es multiplicativa su inversa $U^{-1} = \mu$ es multiplicativa en virtud de la proposición 1.1.4.

La función μ no es completamente multiplicativa, pues $0 = \mu(P^2) \neq \mu(P)\mu(P) = 1$.

Proposición 1.2.3: Si f es multiplicativa y $A = P_1^{e_1} \ldots P_k^{e_k}$, donde $P_i \in \mathbb{P}$ y $e_i \geqslant 1$ entonces.

$$\sum_{D|A} \mu(D)f(D) = \prod_{j=1}^{k} (1-f(P_j)) = \prod_{\substack{P \in \mathbb{P} \\ P|A}} (1-f(P))$$

Prueba La función definida por $\mu(A)f(A)$ es multiplicativa, pues, si $(A,B) = 1$ entonces

$\mu(AB)f(AB) = \mu(A)\mu(B)f(A)f(B) = [\mu(A)f(A)][\mu(B)f(B)]$. Luego, por la proposición 1.1.6,

$$\sum_{D|A} \mu(D)f(D) = \prod_{j=1}^{k} \left(\sum_{i=1}^{e_j} \mu(P_j^i)f(P_j^i)\right),$$

pero $\sum_{i=0}^{e_j} \mu(P_j^i)f(P_j^i) = \mu(1)f(1) + \mu(P_j)f(P_j) = 1-f(P_j)$, de donde resulta la proposición.

<u>Corolario</u>: <u>Si</u> $A = P_1^{e_1} \ldots P_k^{e_k}$, <u>entonces</u>

$$\sum_{D|A} \frac{\mu(D)}{|D|} = \prod_{j=1}^{k} (1-|P_j|^{-1}) = \prod_{P|A} (1-|P|^{-1})$$

<u>Prueba</u>: Como $f(A) = |A|^{-1}$ es multiplicativa el corolario es una consecuencia inmediata de la proposición.

<u>Proposición 1.2.4</u>: <u>Sea</u> f <u>una función multiplicativa</u>. <u>Entonces</u> f <u>es completamente multiplicativa si, sólo sí,</u>

$$f^{-1}(A) = \mu(A)f(A)$$

para todo $A \in \mathbb{M}$.

<u>Prueba</u>: Supongamos que f es completamente multiplicativa y hagamos $h(A) = \mu(A)f(A)$. Entonces

$$(h*f)(A) = \sum_{D|A} h(D)f(A/D) = \sum_{D|A} \mu(D)f(D)f(A/D)$$

$$= \sum_{D|A} \mu(D)f(A) = f(A)\sum_{D|A} \mu(D)$$

$$= f(A)I(A) = I(A)$$

es decir, $h = f^{-1}$. Recíprocamente, si $f^{-1}(A) = \mu(A)f(A)$, vamos a utilizar la proposición 1.1.5(b) para probar que f es completamente multiplicativa. en efecto, si $P \in \mathbb{P}$ y $e \geqslant 1$ vemos que

$$0 = I(P^e) = \sum_{i=0}^{e} \mu(P^i)f(P^i)f(P^{e-i})$$

$$= \mu(1)f(1)f(P^e) + \mu(P)f(P)f(P^{e-1})$$

de donde $f(P^e) = f(P)f(P^{e-1})$. Luego como $f(P) = f(1)f(P)$, una inducción sobre el exponente e nos da el resultado.

Proposición 1.2.5: (Fórmula de inversión de Möbius). Sean f y g funciones aritméticas. Entonces para todo $A \in \mathbb{M}$,

$$f(A) = \sum_{D|A} g(A) \text{ si, y sólo si, } g(A) = \sum_{D|A} f(D)\, \mu(A/D)$$

Además, si f es multiplicativa g también lo es y recíprocamente.

Prueba: La parte izquierda de esta equivalencia significa que $f = g*u$; luego $f*\mu = (g*u)*\mu = g*(u*\mu) = g*I = g$, es decir, la parte derecha. Recíprocamente, el miembro derecho significa que $g = f*\mu$, de donde·

$g*u = (f*\mu)*u = f*(\mu*u) = f*I = f$; es decir, el miembro izquierdo.
El resto de la proposición resulta del corolario de la proposición 1.1.4.

Corolario: μ es la única función aritmética con la propiedad de inversión.

Prueba: Si existe $\alpha \in Dir(\mathbb{M})$ tal que si $f = g*u$ implica que $f*\alpha = g$ entonces $f*\alpha = (g*u)*\alpha = g*(u*\alpha) = g$, para toda $g \in Dir(M)$, pero esto implica que $u*\alpha = I$ si $g(1) \neq 0$ de donde $\alpha = u^{-1} = \mu$

Proposición 1.2.6. (Teorema de Möbius) Sean $\{(D_j, \alpha_j), D_j \in \mathbb{M}, \alpha_j \in \mathbb{C}, 1 \leq j \leq n\}$; $S(M) = \sum_{M|D_j} \alpha_j$ y $S' = \sum_{D_j=1} \alpha_j$ entonces

$$S' = \sum_{M \in \mathbb{M}} \mu(M)S(M)$$

Prueba:

$$\sum_{M \in \mathbb{M}} \mu(M)S(M) = \sum_{M \in \mathbb{M}} \mu(M) \sum_{M|D_J} \alpha_J = \sum_{J=1} \alpha_J \left(\sum_{M|D_J} \mu(M)\right)$$

$$= \sum_{D_J=1} \alpha_J = S';$$

en virtud de la proposición 1.2.1.

Corolario 1. Sean $A_1, \ldots, A_n \in \mathbb{M}$, y sea $F: \{A_1, \ldots, A_n\} \longrightarrow \mathbb{C}$ una función arbitraria. Entonces para cada $A \in \mathbb{M}$, se tiene

$$\sum_{(A_J, A)=1} F(A_J) = \sum_{D|A} \mu(D)S(D)$$

donde $S(D) = \sum_{D|A_J} F(A_J)$

Prueba: Tomemos $D_J = (A_J, A)$ y $\alpha_J = F(A_J)$; entonces $S' = \sum_{(A_J,A)=1} F(A_J)$ y $S(D) = \sum_{D|(A_J,A)} F(A_J)$; como $S(D) = 0$, si $D \not| A$, el corolario resulta de la proposición.

Corolario 2: Sean k un entero $\geqslant 1$ y

$\mathcal{A} = \left\{(A_1^{(J)} \ldots A_k^{(J)});\ A_1^{(J)}, \ldots, A_k^{(J)} \in \mathbb{M},\ 1 \leqslant J \leqslant n\right\}$ Si $F: \mathcal{A} \longrightarrow \mathbb{C}$ es una función arbitraria, entonces,

$$\sum F(A_1^{(J)} \ldots A_k^{(J)}) = \sum_{D|M} \mu(D)S(D)$$

donde la suma de la izquierda se toma sobre todas las k-plas que cumplen

m.c.d$(-_1^{(J)}, \ldots, A_k^{(J)}) = 1$ y

$$S(D) = \sum_{D \mid m.c.d(A_1^{(j)},\ldots,A_k^{(j)})} F(A_1^{(j)},\ldots,A_k^{(j)})$$

Prueba: Tomando $D_j = m.c.d\ (A_1^{(j)},\ldots,A_k^{(j)})$ y $\alpha_j = F(A_1^{(j)},\ldots,A_k^{(j)})$, el resultado se obtiene de la proposición anterior.

Otros ejemplos de funciones aritméticas son los siguientes, donde tomamos $A = P_1^{e_1}\ldots P_k^{e_k}$, $P_j \in \mathbb{P}$ y $e_j \geq 1$.

(i) $$\omega(A) = \begin{cases} 0 & \text{si } A = 1, \\ k & \text{si } A \neq 1 \end{cases}$$

Si A no tiene factores cuadráticos $\mu(A) = (-1)^{\omega(A)}$.

(ii) $$\Omega(A) = \begin{cases} 0 & \text{si } A = 1, \\ e_1+e_2+\ldots+e_k & \text{si } A \neq 1 \end{cases}$$

(iii) $$\beta(A) = \begin{cases} 1 & \text{si } A = 1; \\ e_1.e_2 \ldots e_k & \text{si } A \neq 1 \end{cases}$$

(iv) Las funciones indicatrices de tipo euleriano.

$$\phi(A) = \sum_{\substack{(A,B)=1 \\ |B| \leq |A|}} 1 \ ;$$

Para cada $r = 1,2,\ldots,$

$$\phi_r(A) = \sum_{\substack{(A,B)=1 \\ |B|=r}} 1$$

(v) Las análogas a las funciones de Jordan.

$$J_r(A) = |A|^r \prod_{P|A} (1-|P|^{-1}),$$

$r = 1,2,3,\ldots.$

(vi) El análogo de la función de Liouville.

$$\lambda(A) = \begin{cases} 1 & \text{si } A = 1, \\ (-1)^{\Omega(A)} & \text{si } A \neq 1 \end{cases}$$

Dado que $\Omega(AB) = \Omega(A) + \Omega(B)$; es claro que esta función es multiplicativa.

(vii) La función que indica el número de divisores

$$\tau(A) = \sum_{D|A} 1$$

O, más generalmente, para $r = 2,3,\ldots$

$$d_r(A) = \sum_{(B_1,\ldots,B_r),\, B_1\cdots B_r = A} 1$$

es decir, $d_r(A)$ designa el número de soluciones en $\mathbb{M}$ de $X_1\cdots X_r = A$. Es obvio que $\tau = d_2$.

(viii) $\sigma(A) = \sum_{D|A} |D|$ o, más generalmente, para $t \in \mathbb{C}$

$$\sigma_t(A) = \sum_{D|A} |D|^t = (|\,|^t * u)(A)$$

Es evidente que $\sigma_1(A) = \sigma(A)$ y que $\sigma_0(A) = \tau(A)$. Como $|A|$ es multiplicativa, resulta del corolario de la proposición 1.1.4 que todas las funciones $\sigma_t(A)$ son multiplicativas; en particular $\tau(A)$ es multiplicativa.

(ix) La función análoga a la de Mangoldt.

$$\Lambda(A) = \begin{cases} \log|P| \text{ si } A = P^e, \ P \in \mathbb{P}, \ e \geqslant 1, \\ \\ 0 \text{ en la alternativa} \end{cases}$$

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

supongamos ahora que estamos en un semigrupo aritmético aditivo $(\mathbb{M}, \partial)$, definamos para $r = 1,2,\ldots$, las funciones

$$\hat{\phi}_r(A) = \sum_{\substack{(A,B)=1 \\ \partial(B)=r}} 1$$

Para el semigrupo asociado $(\mathbb{M}, |\,|)$; $|A| = q^{\partial(A)}$ tenemos también una función $\phi_r(A)$ definida en (IV), que cumple $\phi_r(A) = 0$ si r no es una potencia de q, sin que se tenga $\hat{\phi}_r(A) = 0$. Por supuesto, siempre tendremos $\phi_r(A) \leqslant \hat{\phi}_r(A)$. Esto muestra que debemos distinguir entre las funciones definidas seccionalmente en r. Cuando consideramos $(\mathbb{M}, \partial)$, y las análogas definidas seccionalmente en r cuando consideramos $(\mathbb{M}, |\,|)$.

Por ejemplo, si estamos en un semigrupo aritmético $(\mathbb{M}, |\,|)$ es conveniente considerar las siguientes funciones

$$P(r) = \sum_{\substack{P \in \mathbb{P} \\ |P|=r}} 1,$$

$$N(X) = \sum_{|A|\leq x} 1 = \sum_{r\leq X} G(r) = \sum_{r\leq X} \sum_{|A|=r} 1;$$

$$\pi(X) = \sum_{\substack{P\in\mathbb{P} \\ |P|\leq r}} 1 = \sum_{r\leq X} P(r)$$

Mas si estamos en un semigrupo aritmético aditivo, es mejor considerar, además de $\hat{G}(r)$, las siguientes funciones.

$$\hat{P}(r) = \sum_{\substack{P\in\mathbb{P} \\ \partial(P)=r}} 1,$$

$$\hat{N}(X) = \sum_{\partial(A)\leq X} \hat{G}(r) = \sum_{r\leq X} \sum_{\partial(A)=r} 1 \ ;$$

$$\hat{\pi}(X) = \sum_{\substack{P\in\mathbb{P} \\ \partial(P)\leq X}} 1 = \sum_{r\leq X} \hat{P}(r)$$

Con la ayuda de estas funciones empezaremos la obtención de propiedades de las funciones definidas de (i) - (IX).

En primer lugar, usaremos el teorema de Möbius (proposición 1.2.6) para obtener expresiones en término de otras funciones aritméticas, para las funciones indicatrices de tipo euleriano y las funciones de Jordan.

<u>Proposición 1.2.7</u>: <u>Sea</u> $(\mathbb{M}, |\,|)$ <u>un semigrupo aritmético entonces</u>

(a) $\phi(A) = \sum_{D|A} \mu(D)N(|A/D|)$

La expresión (a) es equivalente a la siguiente.

(b) $N(|A|) = \sum_{D|A} \phi(D)$

Prueba Si $D_J = (A,A_J)$ donde $A_J \in \{A_J : |A_J| \leq |A|\}$ y $F(D_J) = 1$,
entonces la proposición 1.2.6 nos dice que

$$S' = \phi(A) = \sum_{D|A} \mu(D)S(D)$$

donde

$$S(D) = \sum_{\substack{|A_J| \leq |A| \\ D|A_J}} 1 = \sum_{\substack{DC_J = A_J \\ |C_J| \leq |A/D|}} 1$$

$$= N(|A/D|)$$

Esto demuestra (a). La igualdad (b) resulta de la proposición 1.2.5. (fórmula de inversión de Möbius).

Corolario 1: Si $\mathbb{M} = \mathbb{N}$ entonces

$$\phi(a) = \sum_{d|a} \mu(d)(a/d) \Longleftrightarrow a = \sum_{d|a} \phi(d)$$

para todo $a \in \mathbb{N}$.

Corolario 2: Si $\mathbb{M} = \mathbb{M}(q;X)$ y $|a(X)| = q^{\partial(a)}$, entonces

(a) $\phi(a(X)) = |a(X)| \sum_{d(X)|a(X)} \mu(d(X)|\; d(X)|$

Esta expresión es equivalente a la siguiente.

(b) $|a(X)| = \sum_{d(X)|a(X)} \phi(d(X))$

Prueba: $N(|a(X)/d(X)|) = \sum_{c;\, \partial(c) \leq \partial(a) - \partial(d)} 1$

$$= q^{\partial(a) - \partial(d)} = |a(X)|d(X)|$$

Corolario 3: Si $\mathbb{M} = \mathbb{N}$ ó $\mathbb{M} = \mathbb{M}(q,X)$, subsiste la expresión

$$\phi(A) = |A| \prod_{P|A} (1-|P|^{-1})$$

Prueba: Resulta de los dos corolarios anteriores y la proposición 1.2.3.

Observemos que como $\phi(A) = \hat{\phi}(A)$ en el caso de un semigrupo aritmético aditivo, los corolarios 2 y 3 son válidos para $\hat{\phi}$.

Proposición 1.2.8: Si $\mathbb{M}$ es $\mathbb{N}$ o $\mathbb{M}(q,X)$ entonces

$$\phi^{-1}(A) = \sum_{D|A} \mu(D)|D|$$

Prueba: De los corolarios 2 y 3 resulta que en ambos casos $\phi = \mu * ||$. Luego $\phi^{-1} = \mu^{-1} * ||^{-1}$. Pero $||$ es completamente multiplicativa, luego por la proposición 1.2.4, $||^{-1} = \mu . ||$.
Por consiguiente $\phi^{-1} = u*(\mu . ||)$, es decir,

$$\phi^{-1}(A) = \sum_{D|A} \mu(D)|D|$$

Corolario: Si $\mathbb{M}$ es $\mathbb{N}$ o $\mathbb{M}(q;X)$, entonces

$$\phi^{-1}(A) = \prod_{P|A} (1-|P|)$$

Prueba: Resulta de aplicar la proposición 1.2.3.

En virtud del corolario 3 de la proposición 1.2.7, vemos que $J_1(A) = \phi(A) = \hat{\phi}(A)$, si $\mathbb{M}$ es bien $\mathbb{N}$ o bien $\mathbb{M}(q;X)$.

Proposición 1.2.9: Sea $(\mathbb{M},||)$ un semigrupo aritmético entonces

(a) $J_r(A) = \sum_{D|A} \mu(D)|A/D|^r$

lo que equivale a.

(b) $|A|^r = \sum_{D|A} J_r(D)$

Prueba: Como $|A|^r$ es multiplicativa la proposición 1.2.3 nos da

$$\sum_{D|A} \mu(D)|D|^{-r} = \prod_{P|A}(1-|P|^{-r})$$

de donde

$$|A|^r \prod_{P|A}(1-|P|^{-r}) = \sum_{D|A} \mu(D)|A/D|^r = J_r(A)$$

La parte (b) de la proposición resulta de la fórmula de inversión de Möbius.

La proposición anterior es válida en $(\mathbb{M},||)$; pero en general, no se tiene $\phi(A) = J_1(A)$, esto sí ocurre, por ejemplo, si $N(|A|) = |A|$.

Proposición 1.2.10: Sea $(\mathbb{M},||)$ un semigrupo aritmético entonces

$$\phi_r(A) = \sum_{\substack{D|A \\ 1\leq |D| \leq r}} \mu(D)G(r/|D|); \quad (r = 1,2,3,\ldots)$$

si $r \geq |A|$ entonces

$$\phi_r(A) = \sum_{D|A} \mu(D)G(r/|D|) \Longleftrightarrow G(r/|A|) = \sum_{D|A} \phi_r(D)$$

Prueba: Resulta del teorema de Möbius

Corolario 1: Si $\mathbb{M} = \mathbb{N}$ entonces

$$\phi_r(a) = \sum_{\substack{d|a \\ 1\leq d< r}} \mu(d)(r/d)$$

Corolario 2· Si $\mathbb{M} = \mathbb{M}(q,X)$ entonces

$$\phi_r(a(X)) = \sum_{\substack{d(X)|a(X)\\ 1\leq |d(X)|\leq r}} \mu(D)q^{[r/|d(X)|]}$$

$(r = 1,2,3,\ldots)$. Si $r \geq |a(X)|$, tenemos

$$\phi_r(a(X)) = \sum_{d(X)|a(X)} \mu(d(X)q^{[|a(X)/d(X)|]}$$

si, y solo si,

$$q^{[|a(X)|]} = \sum_{d(X)|a(X)} \phi_r(d(X))$$

Proposición 1.2.11: Sea $(\mathbb{M},\partial)$ un semigrupo aritmético aditivo. Entonces.

$$\hat{\phi}_r(A) = \sum_{\substack{D|A\\ 0\leq\partial(D)\leq r}} \mu(D)G(r-\partial(D)),\ (r=1,2,\ldots).$$

Si $r \geq \partial(A)$ entonces

$$\phi_r(A) = \sum_{D|A} \mu(D)G(r-\partial(D))$$

Si, y sólo si,

$$G(r-\partial(A)) = \sum_{D|A} \hat{\phi}_r(D)$$

Proposición 1 .2: En un semigrupo aritmético $(\mathbb{M},|\,|)$ tenemos

$$\sum_{D|A} \lambda(D) = \begin{cases} 1 \text{ si } A \text{ es un cuadrado} \\ \\ 0 \text{ si } A \text{ no es un cuadrado} \end{cases}$$

Prueba: Como $\sum_{D|A} \lambda(A)$ es multiplicativa (proposición 1.2.3 y su corolario) basta observar que,

$$\sum_{D|P^e} \lambda(D) = \begin{cases} 1 \text{ si } e \equiv 0 \pmod 2 \\ \\ 0 \text{ si } e \equiv 1 \pmod 2 \end{cases}$$

pero esto es claro sí consideramos la expresión

$$1+P+ \ldots + (P^e) = 1 + (-1)^{\Omega(P)} + (-1)^{\Omega(P^2)} + \ldots + (-1)^{\Omega(P^e)}$$

$$= 1 + (-1) + (-1)^2 + \ldots + (-1)^e$$

Proposición 1.2.13: En un semigrupo aritmético $(\mathbb{M},||)$ tenemos

$$\lambda^{-1}(A) = |\mu(A)|$$

donde $||$ designa aquí el valor absoluto de un número complejo.

Prueba: Como λ es completamente multiplicativa $\lambda^{-1}(A) = \mu(A)\,\lambda(A)$ (proposición 1.2.3). Luego $\lambda^{-1}(A) = 0$. Si existe $P \in \mathbb{P}$ tal que $P^2|A$ y $\lambda^{-1}(A) = 1 = [\mu(A)]^2 = |\mu(A)|$ en la alternativa.

Proposición 1.2.14. En un semigrupo aritmético $(\mathbb{M},||)$ tenemos

(a)
$$\sigma_t(P^e) = \begin{cases} e+1 & \text{si } t = 0 \\ \\ \dfrac{|P|^{t(e+1)}-1}{|P|^t - 1} & \text{si } t \neq 0 \end{cases}$$

(b) $\sigma_0(A) = \prod_{j=1}^{k} (1+e_j) = \tau(A)$ si $A = P_1^{e_1} \ldots P_k^{e_k}$

Proposición 1.2.15· En un semigrupo aritmético $(M,||)$ tenemos

$$\sigma_t^{-1}(A) = \sum_{D|A} |D|^t \mu(D)\mu(A/D)$$

Prueba: Como $||^t$ es completamente multiplicativa la relación $\sigma_t = ||^t * u$ implica que $\sigma_t^{-1} = (\mu . ||^t) * u^{-1}$. La proposición resulta entonces de que $\mu = u^{-1}$.

Corolario: En un semigrupo aritmético $(M,||)$ se tienen las relaciones

(a) $\tau^{-1}(A) = \sum_{D|A} \mu(D)\mu(A/D)$,

(b) $\sigma_1(A) = \sum_{D|A} |D| \mu(D)\mu(A/D)$

Proposición 1.2.16: En un semigrupo aritmético $(M,||)$ tenemos

$$\sigma_t(A)\ \sigma_t(B) = \sum_{D|(A,B)} |D|^t\ \sigma_t(AB/D^2)$$

Proposición 1.2.17: En un semigrupo aritmético $(M,||)$ Si $A = P_1^{e_1} \ldots P_k^{e_k}$ y $P_r(e)$ = card $\{(\alpha_1, \ldots, \alpha_r);\ \alpha_i \in \mathbb{Z},\ \alpha_i \geqslant 0,\ \alpha_1 + \ldots + \alpha_r = e\}$ entonces

$$d_r(A) = \prod_{i=1}^{k} (P_r(e_i))$$

Prueba: Basta observar que $d_r(P^e) = P_r(e)$, si $e \geqslant 1$.

Proposición 1.2.18: En un semigrupo aritmético $(M,||)$ tenemos

$$\log(A) = \sum_{D|A} \Lambda(D)$$

Prueba: De $|A| = |P_1|^{e_1} \dots |P_k|^{e_k}$, resulta $\log |A| = \sum_{i=1}^{k} e_i \log|P_i|$; por otra parte, también se tiene

$$\sum_{i=1}^{k} \sum_{m=1}^{e_i} \Lambda(P_i^m) = \sum_{i=1}^{k} \sum_{m=1}^{e_i} \log |P_i|)$$

$$= \sum_{i=1}^{k} e_i \log |P_i|$$

Definamos ahora una derivación en la $\mathbb{C}$-álgebra Dir $(\mathbb{M})$ mediante la fórmula.

$$f'(A) = f(A) \log |A|$$

Que se trata de una derivación nos lo indica la siguiente.

Proposición 1.2.19: Sean $(\mathbb{M}, |\,|)$ y Dir $(\mathbb{M})$

Entonces, si $f, g \in$ Dir$(\mathbb{M})$ se tiene

(a) $(f+g)' = f'+g'$

(b) $(f*g)' = f'*g + f*g'$

(c) $(f^{-1})' = -f'*(f*f)^{-1}$, si $f(1) \neq 0$

Por ejemplo tenemos las siguientes fórmulas.

(i) $u'(A) = \log |A|$

(ii) $I'(A) = 0$

(iii) $\Lambda * u = u'$

(Esta última en virtud de la proposición 1.2.18)

Como aplicación del uso de esta derivación demostraremos enseguida la versión de SELBERG en un semigrupo aritmético.

Corolario: En un semigrupo aritmético $(\mathbb{M}, |\,|)$ se tiene la fórmula de (SELBERG).

$$\Lambda(A)\log(A) + \sum_{D|A} \Lambda(D)\Lambda(A/D) = \sum_{D|A} \mu(D)\log^2(|A/D|)$$

Prueba: Tenemos

$$\Lambda * u = u' \Rightarrow \Lambda' * \mu + \Lambda * u' = u'',$$

o también $\Lambda' * u + \Lambda * (\Lambda * u) = u''$; multiplicando esta última ecuación por μ obtenemos $\Lambda' + \Lambda * \Lambda = u'' * \mu$ que es la fórmula pedida.

I.3- SERIES FORMALES DE DIRICHLET SOBRE $\mathbb{M}$.

Una expresión de la forma

$$\sum_{A \in \mathbb{M}} f(A)|A|^{-z}$$

donde cada $f(A) \in \mathbb{C}$, se llama una serie formal de Dirichlet sobre $\mathbb{M}$. Dos series formales de Dirichlet.

$$\sum_{A \in \mathbb{M}} f(A)|A|^{-z}; \quad \sum_{A \in \mathbb{M}} g(A)|A|^{-z}$$

se dicen iguales si $f(A) = g(A)$, para todo $A \in \mathbb{M}$. Por el momento dejamos de lado la posibilidad de que como función de la variable compleja z una serie formal de Dirichlet converja. Es claro, por otra parte, que los coeficientes $f(A)$ de una de estas series definen una función aritmética $f \in \mathrm{Dir}(\mathbb{M})$, y, recíprocamente, una función aritmética f define una serie formal de Dirichlet: $\tilde{f}(z) = \sum_{A \in \mathbb{M}} f(A)|A|^{-z}$. De acuerdo con estas definiciones la aplicación $f \longrightarrow \tilde{f}$ de $\mathrm{Dir}(\mathbb{M})$ en el conjunto de todas las series formales de Dirichlet es una biyección para la cual se tiene $\widetilde{f+g} = \tilde{f}+\tilde{g}$; $\widetilde{\lambda f} = \lambda\tilde{f}$; $(\lambda \in \mathbb{C})$. Además si $f,g \in \mathrm{Dir}(\mathbb{M})$ entonces

$$\Big(\sum_{A\in\mathbb{M}} f(A)|A|^{-z}\Big)\Big(\sum_{B\in\mathbb{M}} g(B)|B|^{-z}\Big) = \sum_{A\in\mathbb{M}}\sum_{B\in\mathbb{M}} f(A)g(B)|AB|^{-z}$$

es decir $\widetilde{f*g} = \tilde{f}.\tilde{g}$, donde el miembro izquierdo no es otra cosa que el producto formal usual de dos series de funciones. En todo lo anterior están los ingredientes de la siguiente.

Proposición 1.3.1: La aplicación $f \longrightarrow \tilde{f}$ es un isomorfismo de $\mathbb{C}$-álgebra entre $\mathrm{Dir}(\mathbb{M})$ y el conjunto de todas las series formales de Dirichlet sobre $\mathbb{M}$.

Si dado $(\mathbb{M},|\,|)$ designamos con $|\mathbb{M}|$ al conjunto $\{|A|;\ A\in\mathbb{M}\}$, podemos escribir.

$$\tilde{f}(z) = \sum_{r\in|\mathbb{M}|}\Big(\sum_{|A|=r} f(A)\Big)r^{-z}$$

mientras que si estamos en un semigrupo aritmético aditivo $(\mathbb{M},\partial)$ y $\partial(\mathbb{M}) = \{\partial(A);\ A\in\mathbb{M}\}$ escribimos

$$\tilde{f}(z) = \sum_{k\in\partial(\mathbb{M})}\Big(\sum_{\partial(A)=k} f(A)\Big)q^{-kz}$$

Teniendo en cuenta nuestra definición de derivada de una función aritmética f, hacemos corresponder a f' la serie formal de Dirichlet definida por

$$\tilde{f}'(z) = -\sum_{A\in\mathbb{M}} f(A)(\log|A|)|A|^{-z}$$

con lo cual tenemos evidentemente una derivación (formal) en la $\mathbb{C}$-álgebra de las series formales de Dirichlet.

También es posible definir en Dir($\mathbb{M}$) y, por tanto, en la de las series formales de Dirichlet) una norma $|| \ ||$, mediante la fórmula

$$||f|| = \begin{cases} \sup \left\{ |A|^{-1}; f(A) \neq 0 \right\} & \text{si } f \neq 0 \\ 0 & \text{si } f = 0 \end{cases}$$

Es evidente que $\sup \left\{ |A|^{-1};\ f(A) \neq 0 \right\} = \max \left\{ |A|^{-1};\ f(A) \neq 0 \right\}$, pues existe $\min \left\{ |A|;\ f(A) \neq 0 \right\}$ como sub conjunto de $\mathbb{N}$.

Como este mínimo es $\geqslant 1$ entonces siempre $||f|| \leqslant 1$. Subsiste entonces la siguiente.

<u>Proposición 1.3.2</u>: <u>La norma</u> $|| \ ||$ <u>es una valuación no arquimediana sobre Dir</u>($\mathbb{M}$). <u>Es decir</u>,

(a) $||f|| \geq 0$; $||f|| = 0$ si, y solo si, $f = 0$

(b) $||f*g|| = ||f||.||g||$

(c) $||f|g|| \leqslant \max \left\{ ||f||,\ ||g|| \right\}$

<u>Prueba</u>: Es mas cómodo trabajar con

$$\langle f \rangle = \begin{cases} \min \left\{ |A|:\ f(A) \neq 0 \right\} & \text{si } f \neq 0 \\ \infty & \text{si } f = 0 \end{cases}$$

(donde formalmente hemos tomado $0 = \infty^{-1}$). La propiedad (a) resulta del hecho que $\langle f \rangle \geqslant 1$ si $f \neq 0$. Por otra parte, si $f(A)+g(A) \neq 0$ entonces $f(A)$ y $g(A)$ son ambas distintas de cero, y, por consiguiente, $|A|$ es mayor que $\langle f \rangle$ y que $\langle g \rangle$, y, con mayor razón, que $\min\left\{\langle f \rangle, \langle g \rangle\right\}$. Esto demuestra (c). Para demostrar (b) trabajaremos en el álgebra de las series formales de Dirichlet, observando que $|A|^{-z} = h(z)$ corresponde a una función aritmética definida por $h(-)=1$

y $h(B) = 0$ para $B \nmid A$. Por otra parte, basta considerar sólo el caso en que $f \neq 0$ y $g \neq 0$. Sean, pues, $A_1, \ldots A_r$ los elementos de $\mathbb{M}$ que cumplen $|A_i| = \langle f \rangle$ y $B_1, \ldots B_s$ los que cumplen $|B_j| = \langle g \rangle$ (que aparecen sólo en número finito en virtud de (iii) de la definición 1.1.1. Si $P_1, \ldots P_n$ son los primos que dividen a alguno de los A_i o los B_j entonces las series $|A_1|^{-z}, \ldots, |A_r|^{-z}, |B_1|^{-z}, \ldots, |B_s|^{-z}$ están en la subálgebra $\mathcal{A}$ generada sobre $\mathbb{C}$ por las series $|P_k|^{-z}$ $(k = 1,2,\ldots,n)$. Si definimos $|P_k|^{-z} \longrightarrow X_k$ obtenemos un $\mathbb{C}$-isomorfismo entre $\mathcal{A}$ y $\mathbb{C}[X_1, \ldots, X_n]$, donde las $X_1, \ldots, X_n$ son algebraicamente independientes sobre $\mathbb{C}$. Luego [8] $\mathcal{A}$ es un dominio de integridad y, por consiguiente las series

$$\sum_{i=1}^{r} f(A_i)|A_i|^{-z} \text{ y } \sum_{j=1}^{s} g(B_j)|B_j|^{-z}$$

que son diferentes de la serie nula, tienen un producto no nulo. Esto implica que $f(z)g(z) = (f*g)(z) \neq 0$ y que

$$\langle f*g \rangle = \langle f \rangle \langle g \rangle$$

Corolario: Dir($\mathbb{M}$) es un dominio de integridad.

Proposición 1.3.3: Dir($\mathbb{M}$) es un anillo factorial.

Prueba: Consideraremos dos casos. (a) $\mathbb{P}$ es enumerable infinito. En este caso $\mathbb{M}$ es algebraicamente isomorfo a $\mathbb{N}$ lo que implica que $\mathrm{Dir}(\mathbb{M}) \approx \mathrm{Dir}(\mathbb{N})$. Pero un teorema de Cashwell y Everett [9] nos dice que Dir($\mathbb{N}$) es ya un anillo factorial. (b) si $\mathbb{P} = \{P_1, \ldots, P_n\}$ es finito, entonces por la correspondencia $|P_i|^{-z} \longrightarrow X_i$, donde las X_i son algebraicamente independientes sobre $\mathbb{C}$, obtenemos un $\mathbb{C}$-isomor fismo de álgebras entre Dir(M) y $\mathbb{C}[[X_1,\dots,X_n]]$ (el álgebra de las series potenciales formales sobre $\mathbb{C}$ en las indeterminadas $(X_1,\dots,X_n)$. La proposición sigue entonces de que esta última álgebra es factorial [9].

Proposición 1.3.4: Dir(M) es un espacio topológico completo con respecto a $|| \ ||$.

Prueba: Sea $f_1, f_2, \dots, f_n \dots$ una sucesión Cauchy en Dir(M); es decir, una sucesión para la cual, dado $\varepsilon > 0$ existe un entero $M(\varepsilon) > 0$ tal que $||f_m - f_n|| < \varepsilon$ si $m,n \geq M(\varepsilon)$. Esto equivale también a lo siguiente:

$$f_m(A) = f_n(A) \text{ para todo } A \text{ que cumpla } |A| \leq 1/\varepsilon \text{ , si } m,n \geq M(\varepsilon).$$

Como ε es arbitrario y, por tanto $1/\varepsilon$ puede tomarse tan grande como se quiera; lo anterior implica que dado $A \in \mathbb{M}$, la sucesión $f_1(A), \dots, f_n(A) \dots$ es constante a partir de un cierto subíndice $M(A)$, Sea $f(A)$ este valor constante, de modo que $f_n(A) = f(A)$ si $n \geq M(A)$. Como $\{M(A);\ |A| < 1/\varepsilon\}$ es finito, podemos considerar su máximo $M_0(\varepsilon)$. Luego, si $|A| < 1/\varepsilon$, entonces $f_n(A) = f(A)$ si $n \geq M_0(\varepsilon)$. Es decir, para $n \geq M_0(\varepsilon)$, $f_n(A) \neq f(A)$ sólo si $|A|^{-1} < \varepsilon$, o lo que es lo mismo. $||f_n - f|| < \varepsilon$ si $n \geq M_0(\varepsilon)$.

Es fácil verificar que una serie $\sum_{n=1}^{\infty} f_n$ es convergente con respecto de $|| \ ||$ si, y sólo si, $||f_n|| \longrightarrow 0$ cuando $n \longrightarrow \infty$

Conectado con la convergencia con respecto de $|| \ ||$ está el siguiente concepto puramente algebraico: Sea $f_1, f_2, \dots,$ una sucesión de elementos de Dir(M) tal que, para cada $A \in \mathbb{M}$, $f_n(A) \neq 0$ para a lo sumo un número finito de índices n. Una tal sucesión se dice una serie seudoconvergente, definiendo su suma por la relación.

$$\sum_{n=1}^{\infty} f_n = \sum_{n=1}^{\infty} \tilde{f}_n(z) = \sum_{A\in \mathbb{M}} \left(\sum_{n=1}^{\infty} f_n(A)\right)|A|^{-z}$$

que es un elemento de $Dir(\mathbb{M})$, pues $\sum_{n=1}^{\infty} f_n(A)$ es de hecho una suma finita.

Proposición 1.3.5: $\sum_{n=1}^{\infty} f_n$ es seudoconvergente si, y solo si, $\sum_{n=1}^{\infty} f_n$ es convergente con respecto de $\| \ \|$.

Prueba: (a) ($\Longleftarrow$) Supongamos que la serie sea convergente con respecto de $\| \ \|$, o lo que es lo mismo que $\|f_n\| \longrightarrow 0$. Entonces, como en la demostración de la proposición anterior dado $A\in\mathbb{M}$, existe un entero positivo $\mathbb{M}(A)$ tal que $f_n(A) = 0$ para $n \geq M(A)$; esto demuestra que la serie es seudoconvergente.(b) ($\Longrightarrow$) Recíprocamente, si la serie es seudoconvergente, y teniendo en cuenta que $\{ M(A): |A| \leq 1/\varepsilon \}$ es finito, al tomar $M(\varepsilon) = \text{máx} \{\mathbb{M}(A)\cdot \ |A| \leq 1/\varepsilon\}$, vemos que para todo A que cumpla $|A| \leq 1/\varepsilon$, $f_n(A) = 0$ si $n > M(\varepsilon)$; es decir, $\|f_n\| \longrightarrow 0$.

Corolario: Si $g \in Dir(\mathbb{M})$ y $\sum_{n=1}^{\infty} f_n$ es seudoconvergente entonces $\sum_{n=1}^{\infty} (g*f_n)$ es seudoconvergente y

$$\sum_{n=1}^{\infty} g*f_n = g*\sum_{n=1}^{\infty} f_n$$

Prueba: La serie $\sum_{n=1}^{\infty} g*f_n$ es seudoconvergente pues $\|g*f_n\| = \|g\| \ \|f_n\| \longrightarrow 0$ si $\|f_n\| \longrightarrow \hat{0}$. Por otra parte si

$$h = \sum_{n=1}^{\infty} g*f_n = \sum_{n=1}^{\infty} \tilde{g}(z)\tilde{f}_n(z)$$

$$= \sum_{A\in\mathbb{M}} \left(\sum_{n=1}^{\infty} (g*f_n)(A)\right)|A|^{-z}$$

$$= \sum_{A\in\mathbb{M}} \left[g * \left(\sum_{n=1}^{\infty} f_n\right)(A)\right]|A|^{-z}$$

$$= \sum_{A\in\mathbb{M}} (g*h)(A)|A|^{-z}$$

$$= \tilde{g}(z)\tilde{h}(z) = g * \sum_{n=1}^{\infty} f_n$$

puesto que $\sum_{n=1}^{\infty} (g*f_n)(A)$ es una suma finita.

Proposición 1.3.6: $f_{,}\in$ Dir($\mathbb{M}$) es invertible, sí y sólo si, $||f||=1$.

Prueba: Por la proposición 1.1.3 sabemos que f es invertible si, y sólo si, $f(1) \neq 0$. Pero esto es claramente equivalente a decir que $||f|| = 1$.

Corolario: Para $||\ \ ||$, Dir($\mathbb{M}$) es un anillo de valuación discreta completo.

Prueba: Un anillo de valuación discreta es un anillo entero, con valuación no arquimediana que satisface la condición establecida en la proposición 1.3.6. La completez ya la demostramos en la proposición 1.3.4.

Lema: En Dir($\mathbb{M}$), si $||h||<1$ se cumple las siguientes propiedades

(a) La serie geométrica

$1+h+h*h+\ldots+(h*h*\ldots*h)$ [r veces] $+\ldots$ converge y su suma es $1/1-h$.

(b) $(h*h \;\ldots *h)$ [rveces] $(A) \neq 0$ <u>para a lo sumo un número finito de índices r</u>.

<u>Prueba</u>: En primer lugar observemos que $||1-h|| = 1$, de modo que $1-h$ es invertible (proposición 1.3.6). Luego

$$|| \frac{1}{1-h} -(1+h+\ldots (h*\ldots *h)[r \text{ veces}] || =$$

$$= ||\frac{(-1)^r h^{r+1}}{1-h}|| = ||h||^{r+1}$$

que tiende a cero cuando $r \longrightarrow \infty$ (en la topología usual de los números reales). Esto demuestra (a). La parte (b) es una consecuencia de la proposición 1.3.5.

<u>Proposición 1.3.7</u>: <u>Si</u> $f \in Dir(M)$ <u>es invertible entonces</u>

$f = f(1)\,[1 + h]$, <u>donde</u> $||h|| < 1$. <u>Además,</u>

$f^{-1} = 1/f(1)[1+h]$

<u>o también</u>.

$$\frac{1}{f(z)} = \frac{1}{f(1)} \sum_{r=0}^{\infty} (-1)^r \,[h(z)]^{\,r}$$

<u>Prueba</u>: Como $H = f - f(1)$ cumple $H(1) = 0$, entonces $||H|| < 1$ esto hace que $h = (\frac{1}{f(1)})H$. también satisfaga $||h|| < 1$. Luego f puede escribirse como $f(1)\,[1 + h]$, con $||h|| < 1$. El resto de la proposición resulta del lema.

Consideremos ahora una sucesión de funciones aritméticas de la forma $f_n = 1+F_n$ con $||F_n||<1$, y supongamos además que $\sum_{n=1}^{\infty} F_n$ es una serie seudoconvergente. En este caso decimos que $\prod_{n=1}^{\infty} f_n$ es un producto seudoconvergente y definimos su producto mediante la expresión.

$$\prod_{n=1}^{\infty} f_n = \prod_{n=1}^{\infty} \tilde{f}_n(z)$$

$$= 1 + \sum_{\substack{A\in M \\ A\neq 1}} \Big(\sum_{\substack{B_1\ldots B_r = A \\ r\geq 1 \\ n_r>\ldots>n_1\geq 1}} \prod_{i=1}^{r} F_{n_i}(B_i)\Big)|A|^{-z}$$

Observemos que esta expresión define un elemento de $\mathrm{Dir}(M)$ pues,

$$h(A) = \sum_{\substack{B_1\ldots B_r \\ r\geq 1}} \prod_{n_i=1}^{r} F_{n_i}(B)$$

$$= \sum_{\substack{B_1\ldots B_r = A \\ r\geq 1}} \Big(\sum_{n_i\geq 1} \prod_{n_i}^{r} F_{n_i}(B_i)\Big)$$

es una suma finita y define, por tanto una función aritmética h.

Proposición 1.3.8: Sea $\prod f_n$ un producto seudoconvergente. Entonces.

$$\lim_{n\to\infty} \prod_{n=1}^{N} f_n = h \quad \text{según la norma } ||\ ||.$$

Prueba: Es claro que

$$\left[\prod_{n=1}^{N} (1+F_n)\right](A) = 1 + \left[\sum_{n=1}^{N} \sigma_n(F_1,\ldots,F_n)\right](A)$$

$$= 1 + \sum_{\substack{B_1\ldots B_r = A \\ 1\leq n_1<\ldots<n_r\leq N}} \prod_{i=1}^{r} F_{n_i}(B_i)$$

donde las σ_n son las funciones simétricas de $F_1,\ldots,F_N$. Luego

$$g_N(A) = h(A) - \prod_{n=1}^{N} (1+F_n)(A)$$

$$= \sum_{\substack{B_1\ldots B_r=A \\ 1\leq n_1<\ldots<n_r<N,\ \text{con algún } n_i>N}} \prod_{i=1}^{r} F_{n_i}(B_i)$$

Por otra parte sabemos que existe un entero $M(A)$ tal que $F_{n_i}(B_i) = 0$ para todo $B_i|A$, si $n_i \geq M(A)$. Si tomamos $N \geq N(A)$, es claro ahora que $g_N(A) = 0$ si $N \geq M(A)$. Por consiguiente, si $\varepsilon > 0$ podemos considerar el conjunto finito $\{M(A): |A| \leq 1/\varepsilon\}$ y, por tanto, su máximo $M = \text{máx}\ (M(A))$. Luego si $|A| \leq 1/\varepsilon$, entonces $g_N(A) = 0$ si $N>M$; es decir, $N>M$, $g_N(B) \neq 0$ sólo si $|A| \leq 1/\varepsilon < |B|$, lo cual implica que

$$||g_N|| = \text{máx}\left\{|B|^{-1};\ g_N(B) \neq 0\right\} \leq \varepsilon$$

Observemos que no estamos afirmando que si un producto de unidades de $\mathrm{Dir}(\mathbb{M})$ converge para la norma $||\ ||$, este producto sea convergente.

<u>Proposición 1.3.9</u>: <u>Si</u> $\prod_{n=1}^{\infty} f_n$ y $\prod_{n=1}^{\infty} g_n$ <u>son productos seudoconvergentes, también lo son</u>

$$\prod_{n=1}^{\infty} (f_n * g_n) \text{ y } \prod_{n=1}^{\infty} f_n^{-1}$$

<u>donde</u> f_n^{-1} <u>es el inverso de Dirichlet de</u> f_n. <u>Además</u>

$$\prod_{n=1}^{\infty} f_n(z) g_n(z) = \left[\prod_{n=1}^{\infty} f_n(z)\right]\left[\prod_{n=1}^{\infty} g_n(z)\right] \qquad \text{y}$$

$$\left[\prod_{n=1}^{\infty} f_n\right]^{-1} = \prod_{n=1}^{\infty} f_n^{-1}$$

Prueba: En efecto

$f_n = 1 + F_n$ con $||F_n||<1$ y $\sum_{n=1}^{\infty} F_n$ es seudoconvergente

$g_n = 1 + G_n$ con $||G_n||<1$ y $\sum_{n=1}^{\infty} G_n$ es seudoconvergente

$$f_n * g_n = (1+F_n)*(1+G_n) = (1+F_n)*1+(1+F_n)*G_n$$

$$= 1+F_n+G_n+F_n*G_n$$

ahora bien, como $\sum_{n=1}^{\infty} F_n$, $\sum_{n=1}^{\infty} G_n$ son seudoconvergentes $\sum_{n=1}^{\infty} F_nG_n$ es seudoconvergente así, pues, $\sum_{n-1}^{\infty} F_n+G_n+F_nG_n$ es seudoconvergente, por otro lado,

$$||F_n+G_n+F_nG_n||\leqslant \text{máx}\left\{||F_n||,\ ||G_n||,||F_nG_n||\right\}$$

$$\leqslant 1$$

luego, así, $\prod_{n=1}^{\infty} f_n*g_n$ es seudoconvergente .

Probemos ahora que $\prod_{n=1}^{\infty} f_n^{-1}$ es seudoconvergente.

Supongamos que $f_n^{-1} = 1 + G_n$ con $||G_n||<1$ y $\sum_{n=1}^{\infty} G_n$ seudoconvergente.

Veamos quien es G_n, sabemos que

$1 = f_n * f_n^{-1} = (1 + F_n)*(1 + G_n) = 1 + F_n + G_n + F_nG_n$ de donde

$$G_n = - \frac{F_n}{F_n+1}$$

Por tanto, $f_n^{-1} = 1 - \dfrac{F_n}{F_n+1}$

Por otro lado

$$||G_n|| = ||\frac{F_n}{F_n+1}||\leqslant \frac{||F_n||}{||F_n+1||}<1$$

Luego así f_n^{-1} es seudoconvergente.

De las fórmulas analizados para $\prod_{n=1}^{\infty} f_n g_n$ y $\prod_{n=1}^{\infty} f_n^{-1}$

se verifica facilmente que

$$\prod_{n=1}^{\infty} f_n g_n = \left(\prod_{n=1}^{\infty} f_n\right)\left(\prod_{n=1}^{\infty} g_n\right)$$

y

$$\prod_{n=1}^{\infty} f_n^{-1} = \left[\prod_{n=1}^{\infty} f_n\right]^{-1}$$

CAPÍTULO II

LA FUNCIÓN ζ DE RIEMANN DE UN SEMIGRUPO ARITMÉTICO

CAPITULO II

LA FUNCION ζ DE RIEMANN DE UN SEMIGRUPO ARITMETICO

En el presente capítulo estudiaremos la llamada función ζ de Riemann de un semigrupo aritmético, la que es de utilidad en la obtención de fórmulas y valores promedios para las funciones aritméticas.

Empezaremos el estudio de esta función en cualquier semigrupo aritmético, particularizándola luego al semigrupo $\mathbb{M}(q,X)$ de los polinomios unitarios de $\mathbb{F}_q [\![X]\!]$.

Escribiremos también una serie de fórmulas que nos relacionarán las funciones aritméticas vistas en el capítulo I con producto de funciones ζ de Riemann. Finalmente, daremos condiciones necesarias y suficientes para expresar una función aritmética como producto finito o infinito de funciones ζ.

II.2- LA FUNCION ζ DE RIEMANN DE UN SEMIGRUPO ARITMETICO.

Si $\mathbb{M}$ es un semigrupo aritmético, definiremos a

$$(1) \qquad \zeta_{\mathbb{M}}(z) = \sum_{A\in\mathbb{M}} |A|^{-z} = \sum_{n=1}^{\infty} G(n)n^{-z}$$

donde

$$G(n) = \sum_{\substack{A\in\mathbb{M}\\ |A|=n}} 1 < \infty$$

como la función ζ de Riemann de $\mathbb{M}$.

Proposición 2.1.1: La función ζ satisface un producto de Euler.

$$\zeta_{\mathbb{M}}(z) = \prod_{P\in\mathbb{P}} (1-|P|^{-z})^{-1}$$

Prueba: En efecto si $A = P_1^{e_1} \dots P_k^{e_k}$; $P_i \in \mathbb{P}$, entonces

$$\prod_{P\in\mathbb{P}} (1-|P|^{-z})^{-1} = \prod_{P\in\mathbb{P}} \cdot \left(\frac{1}{1-|P|^{-z}}\right)$$

$$= \prod_{P\in\mathbb{P}} \left(\sum_{j=0}^{\infty} \frac{1}{|P|^{jz}}\right)$$

$$= \sum_{A\in\mathbb{M}} |A|^{-z} = \zeta_{\mathbb{M}}(z)$$

donde hemos usado la expresión formal $\sum X^n = 1/(1-x)$.

Corolario 1:

$$\zeta_{\mathbb{M}}(mz) = \prod_{P\in\mathbb{P}} (1-|P|^{-mz})^{-1}$$

Corolario 2. Si $\mathbb{M} = \mathbb{M}(q;X)$, entonces

$$\zeta_{\mathbb{M}(q,X)}(z) = \frac{1}{1-q^{1-z}},$$

que converge como función de z si $Re(z)>1$

Prueba: De (1) obtenemos

$$\zeta_{\mathbb{M}(q;X)}(z) = \sum_{r=1}^{\infty}\left(\sum_{|A|=r} 1\right)r^{-z}$$

$$= \sum_{r=1}^{\infty} \left(\sum_{q^{\partial(A)}= r} 1\right)r^{-z}$$

$$= \sum_{r=0}^{\infty} \Big(\sum_{\partial(A)=r} 1 \Big) q^{-rz}$$

$$= \sum_{r=0}^{\infty} q^{r(1-z)}$$

$$= \frac{1}{1-q^{1-z}}$$

ahora bien esta serie converge absolutamente si

$$|q^{1-z}| = q^{1-\mathrm{Re}(z)} < 1$$

es decir si $\mathrm{Re}(z) > 1$.

Definición 2.1.2: (a) una función $f \in \mathrm{Dir}(\mathbb{M})$ se dice primo independiente si para todo $P_1, P_2 \in \mathbb{P}$ y $r \geq 1$ se tiene

$$f(P_1^r) = f(P_2^r)$$

(b) Una función $f \in \mathrm{Dir}(\mathbb{M})$ se llama primo independiente multiplicativa (abreviado PIM) si ella es primo independiente y multiplicativa.

Ejemplos:

(1) La función $\tau = d_2$ es primo independiente multiplicativa.

(2) Sea $f_r \in \mathrm{Dir}(\mathbb{M})$ definida por

$$f_r(A) = \begin{cases} 1 & \text{si existe } B \in \mathbb{M} \text{ tal que } B^r = A \\ 0 & \text{en la alternativa} \end{cases}$$

donde

$$f_r(P^k) = \begin{cases} 1 & \text{si } k = mr \text{ para algún } m \in \mathbb{N} \\ 0 & \text{en la alternativa} \end{cases}$$

Claramente se ve que f_r es primo independiente. Además si $(A,B) = 1$, $f_r(AB) = f_r(P_1^{e_1}\ldots P_s^{e_s}.Q_1^{f_1}\ldots Q_t^{f_t}) = 0$ si algún e_i, f_j no es divisible por r y $f_r(AB) = f_r(A)f_r(B)$ si todos los e_i, f_j son divisibles por r luego f_r es PIM.

<u>Proposición 2.1.2</u>: PIM(M) <u>es un subgrupo multiplicativo de</u> $Dir^X(M)$; <u>donde</u> $Dir^X(M)$ <u>es el conjunto de funciones invertibles de</u> Dir(M).

<u>Prueba</u>: Como $I \in$ PIM(M), vemos que este conjunto no es vacío. Sean ahora, $f,g \in$ PIM(M) y tomemos

$P_1, P_2 \in \mathbb{P}$ y $r \geq 1$, de modo que:

$$(f*g)(P_1^r) = \sum_{k=0}^{r} f(P_1^k)g(P_1^{r-k})$$

$$= \sum_{k=0}^{r} f(P_2^k)g(P_2^{r-k})$$

$$=(f*g)(P_2^r)$$

es decir $f*g \in$ PIM(M). Finalmente, si $f \in$ PIM(M), tenemos para $r = 1$.

$$0 = (f*f^{-1})(P_1) = f(1)f^{-1}(P_1)+f(P_1)f^{-1}(1)$$

$$= f^{-1}(P_1) + f(P_1)$$

además

$$0 = (f*f^{-1})(P_2) = f(1)f^{-1}(P_2) + f(P_2)f^{-1}(1)$$

$$= f^{-1}(P_2) + f(P_2)$$

de donde $f^{-1}(P_1) = f^{-1}(P_2)$, pues, $f(P_1) = f(P_2)$ por hipótesis. Supongamos ahora que $f^{-1}(P_1^j) = f^{-1}(P_2^j)$ con $j \leq r$ y demostraremos para P_1^{r+1} y P_2^{r+1}. Tenemos

$$0 = (f{*}f^{-1})(P_1^{r+1}) = \sum_{k=0}^{r+1} f(P_1^{r+1-k})f^{-1}(P_1^k),$$

$$0 = (f{*}f^{-1}(P_2^{r+1}) = \sum_{k=0}^{r+1} f(P_2^{r+1-k})(f^{-1}(P_2^k),$$

es decir,

$$f(1)f^{-1}(P_1^{r+1}) = f(1)f^{-1}(P_2^{r+1}),$$

pues, $f(P_1^{r+1-k})f(P_1^k) = f(P_2^{r+1-k})f^{-1}(P_2^k)$ si $k = 0,\dots r$, por la hipótesis de inducción. Luego $f^{-1} \in PIM(\mathbb{M})$.

II.2- RELACION ENTRE LA FUNCION ζ Y LAS FUNCIONES ARITMETICAS.

Empezaremos por verificar que algunas funciones aritméticas pueden expresarse como producto de funciones ζ facilmente se puede observar que

$$\breve{u} = \breve{u}(z) = \zeta(z)$$

pues, $\breve{u}(z) = \sum_{A\in\mathbb{M}} u(A)|A|^{-z} = \sum_{A\in\mathbb{M}} |A|^{-z} = \zeta(z)$ (1)

<u>Proposición 2.2.1:</u> <u>Sea $\mathbb{M}$ un semigrupo aritmético entonces</u>

(a) $\breve{d}_r(z) = \left[\zeta(z)\right]^r$ En particular, $\breve{\tau}(z) = \left[\zeta(z)\right]^2$

(b) $\breve{\mu}(z) = 1/\zeta(z)$

(c) $\breve{f}_r(z) = \zeta(rz)$

(d) $\tilde{d}_*(z) = [\zeta(z)]^2/\zeta(2z)$ donde $d_*(A) = 2^{w(A)}$

(e) $\tilde{\lambda}(z) = \zeta(2z)/\zeta(z)$

(f) $\tilde{\sigma}_s(z) = \zeta(z).\zeta(z-s)$

(g) $\tilde{\phi}(z) = \zeta(z-1)/\zeta(z)$

(h) $\sum_{A\in M} [d_2(A)]^2 |A|^{-z} = [\zeta(z)]^4/\zeta(2z)$

(i) $\tilde{\Lambda}(z) = -\zeta'(z)/\zeta(z)$

Prueba: (a) verifiquemos que $u*u = \tau = d_2$. Como tanto $u*u$ como τ son multiplicativas, basta verificar que

$$(u*u)(P^e) = \tau(P^e). \text{ Pero}$$

$$\tau(P^e) = e + 1 \quad y$$

$$(u*u)(P^e) = \sum_{k=0}^{e} u(P^k)u(P^{e-k}) = \sum_{K=0}^{e} 1 = e+1$$

por tanto $\tilde{d}_2(z) = \tilde{u}(z)\tilde{u}(z) = [\zeta(z)]^2$, en virtud de la proposición 1.3.1 y (1) mas generalmente;

$$[\zeta(z)]^r = \Big(\sum_{A\in M} |A|^{-z}\Big)^r = \sum_{A\in M}\Big(\sum_{B_1\ldots B_r=A} |B_1|^{-z}\ldots|B_r|^{-z}\Big)$$

$$= \sum_{A\in M}\Big(\sum_{B_1\ldots B_r=A} |A|^{-z}\Big) = \sum_{A\in M}\Big(\sum_{B_1\ldots B_r=A} 1\Big)|A|^{-z}$$

$$= \sum_{A\in M} d_r(A)|A|^{-z} = \tilde{d}_r(A)$$

(b) Como $\mu = u^{-1}$, y $\tilde{u}(z) = \zeta(z)$ resulta que $\tilde{\mu}(z) = \dfrac{1}{\zeta(z)}$

(c) $\tilde{f}_r = \tilde{f}_r(z) = \sum_{A\in M} f_r(A)|A|^{-z} = \sum_{A\in M} |A^r|^{-z}$

$$= \sum_{A\in M} |A|^{-rz} = \zeta(rz)$$

(d) Es claro que $d_* \in PIM(M)$. Si $d_* * f_2$ coincide con τ en las potencias de primos, tendremos que $d_* * f_2 = \tau$. Veamos, pues, que si coinciden

$$(d_* * f_2)(p^e) = \sum_{k=0}^{e} f_2(p^k) d_*(p^{e-k})$$

$$= f_2(p^e) + 2\sum_{K=0}^{e-1} f_2(p^k)$$

$$= \frac{(-1)^e+1}{2} + \sum_{K=0}^{e-1} (-1)^k + \sum_{K=0}^{e-1} 1$$

$$= \frac{(-1)^e+1}{2} + \frac{1-(-1)^e}{2} + e = e+1$$

Por consiguiente

$$d_*(z) = \left[\zeta(z)\right]^2 / \zeta(2z)$$

(e) La identidad resulta si demostramos que $\lambda * u = f_2$, pero, para ello basta verificar la anterior igualdad en las potencias de primos. Como

$$(\lambda * u)(p^e) = \sum_{k=0}^{e} u(p^{e-k})\,\lambda(p^k)$$

$$= \sum_{k=0}^{e} \lambda(p^k)$$

$$= \sum_{k=0}^{e} (-1)^k = \begin{cases} 1 \text{ si } e \text{ es par} \\ 0 \text{ en la alternativa} \end{cases}$$

$$= f_2(p^e)$$

podemos así concluir que $\breve{\lambda}(z) = \zeta(2z)/\zeta(z)$.

(f) En el capítulo anterior verificamos que $||^s * u = \sigma_s$ por consiguiente

$$\breve{\sigma}_s(z) = \breve{||^s}(z)\breve{u}(z) = \zeta(z)\breve{||^s}(z)$$

pero

$$\breve{||^s}(z) = \sum_{A\in M} |A|^s |A|^{-z} = \sum_{A\in M} |A|^{s-z} = \zeta(z-s)$$

de donde lo pedido.

(g) En la proposición 1.2.7 verificamos que

$$\phi = \mu * (N.||)$$

ahora bien,

$$\begin{aligned}\sum_{A\in M} N(|A|)|A|^{-z} &= \sum_{A\in M} \Big(\sum_{r\leq |A|}\ \sum_{|B|=r} 1\Big)|A|^{-z}\\ &= \sum_{n=1}^{\infty}\Big(\sum_{|A|=n}\Big(\sum_{r\leq |A|}\ \sum_{|B|=r} 1\Big)\Big)n^{-z}\\ &= \sum_{n=1}^{\infty}\ \sum_{|A|=n}\Big(\sum_{r\leq n}\ \sum_{|B|=r} 1\Big)n^{-z}\\ &= \sum_{n=1}^{\infty} N(n)\Big(\sum_{|A|=n} 1\Big)n^{-z}\\ &= \sum_{n=1}^{\infty} n(n)G(n)n^{-z}\end{aligned}$$

de donde obtenemos el resultado pedido.

(h) Como $d_2 = u*u$ y $u\in PIM(M)$ es claro que d_2 y por fuerza d_2^2 pertenece a PIM(M). Verifiquemos que $d_2^2 * f_2 = d_4$. Basta verificar esta propiedad en las potencias de primos, pues estas funciones son multiplicativas. En efecto

$$d_4(P^e) = \frac{(e+1)(e+2)(e+3)}{6} = \binom{e+3}{3}$$

$$f_2(P^e) = \frac{(-1)^e + 1}{2}$$

Pero

$$(d_2^2 * f_2)(P^e) = \sum_{k=0}^{e} f_2(P^k) d_2^2(P^{e-k})$$

$$= \sum_{k=0}^{e} \left[\frac{(-1)^k+1}{2}\right] (e-k+1)^2$$

$$= 1/2 \left[\sum_{k=0}^{e} (-1)^k (e-k+1)^2 + \sum_{k=0}^{e} (e-k+1)^2 \right]$$

$$= 1/2 \left[\frac{(e+1)(e+2)}{2} + \frac{(e+1)(e+2)(2e+3)}{6} \right]$$

$$= 1/12 \left[3(e+1)(e+2) + (e+1)(e+2)(2e+3) \right]$$

$$= 1/12 \left[(e+1)(e+2)(2e+6) \right]$$

$$= \frac{(e+1)(e+2)(e+3)}{6}$$

$$= \binom{e+3}{3}$$

Luego $\widetilde{d_2^2}(z) = \widetilde{d_4}(z)/\widetilde{f_2}(z)$

$= \left[\zeta(z)\right]^4 / \zeta(2z)$, en virtud de (1) y (c).

(i) De la proposición 1.2.19 obtenemos $\Lambda * u = u'$, por tanto

$\breve{\Lambda}(z)\breve{u}(z) = \breve{u}'(z)$ es decir $\breve{\Lambda}(z) = -\zeta'(z)/\zeta(z)$.

Ahora si definimos la función aritmética $q_r \in Dir(M)$ por

$$q_r(A) = \begin{cases} 1 \text{ si } A \text{ no tiene divisores de la forma } B^r \neq 1 \\ 0 \text{ en la alternativa} \end{cases}$$

podemos ver que $q_r * f_r = u$; en efecto q_r es multiplicativa y por tanto lo es $q_r * f_r$, y basta en consecuencia, verificar la anterior identidad en potencias de primos.

Así tenemos pues,

$$(q_r * f_r)(P^e) = \sum_{k=1}^{e} q_r(P^k) f_r(P^{e-k})$$

$$= \sum_{k=1}^{e} f_r(P^{e-1}) = 1$$

ya que entre los exponentes $P^e, P^{e-1}, \ldots P^{e-(k-1)}$ solo hay uno divisible por r.

Podemos enunciar el siguiente corolario y obtenemos una nueva expresión.

<u>Corolario</u>:

(j) $\breve{q}_r(z) = \breve{u}(z)/\breve{f}_r(z) = \zeta(z)/\zeta(rz)$

Comparando los coeficientes de q^{-kz} en los resultados anteriores obtenemos expresiones para $\sum_{\partial(A)=k} f(A)$ donde f es una función aritmética.

Proposición 2.2.2: En $\mathbb{M}(q,X)$ obtenemos las siguientes expresiones para las funciones aritméticas

(a') $$\sum_{\partial(A)=k} d_r(A) = \binom{k+r-1}{r-1} q^k, \quad k = 0,1,2,\ldots$$

(b') $$\sum_{\partial(A)=k} \mu(A) = 1 \text{ si } k = 0; \ -q \text{ si } k = 1; \ 0 \text{ si } k \geq 2.$$

(c') $$\sum_{\partial(A)=k} f_r(A) = 0 \text{ si } k \not\equiv 0 (\mathrm{mod}\ r); \ q \text{ si } r/k.$$

(d'') $$\sum_{\partial(A)=k} d_*(A) = (k+1)q^k - (k-1)q^{k-1} \text{ si } k \geq 1; \ 1 \text{ si } k = 0$$

(e') $$\sum_{\partial(A)=k} \lambda(A) = (-1)^k q^{[\![(k+1)/2]\!]}, \quad k = 0,1,2 \ldots,$$ donde $[\![X]\!]$ designa la parte entera del número real X.

(f') $$\sum_{\partial(A)=k} \sigma_s(A) = q^k (q^{s(k+1)}-1)/(q^s-1), \quad k=0,1,2 \ldots, s \neq 0.$$

(g') $$\sum_{\partial(A)=k} \phi(A) = 1 \ k = 0; \ q^{2k}-q^{2k-1}$$ si $k \geq 1$.

(h') $$\sum_{\partial(A)=k} [d_2(A)]^2 = 1 \text{ si } k=0; \ \binom{4}{3}q \text{ si } k = 1;$$

$$\frac{q^k}{q}\left[q^k\binom{k+3}{3} - \binom{k+1}{3}\right] \text{ si } k \geq 2$$

(i') $$\sum_{\partial(A)=k} \Lambda(A) = 0 \text{ si } k = 0, (\log q)q^k \qquad \text{si } k \geq 1$$

(j') $$\sum_{\partial(A)=k} q_r(A) = q^r \text{ si } k < r, \ q^k - q^{(k+1)-r} \quad \text{si } k \geq r$$

Prueba:

Empecemos recordando que

$$\sum_{\partial(A)=k} \mathcal{U}(A) = \frac{1}{1-q^{1-z}} ,$$

de aquí podemos deducir directamente

$$\sum_{\partial(A)=k} \mu(A) = 1 - q^{1-z}$$

pues, $\mathcal{U} = \mu^{-1}$. Así obtenemos directamente (b')

Recordemos además que

$$\sum_{\partial(A)=k} d_2(A) = (k+1)q^k$$

pues $\tilde{d}_2 = \tilde{u}^2$

Demostremos ahora

(a') Como $\tilde{d}_r(z) = (\zeta(z))^r$ obtenemos

$$\sum_{\partial(A)=k} d_r(A) q^{-kz} = \left[\sum q^k q^{-kz}\right]^r$$

$$= \sum_{k=0}^{\infty} \binom{k+r-1}{r-1} q^k q^{-kz}$$

Así

$$\sum_{\partial(A)=k} d_r(A) = \binom{k+r-1}{r-1} q^k$$

Podemos ver claro que tanto (c') como (j') se derivan directamente de las definiciones de f_r y q_r.

(d') Sabemos que $d_*(z) = (\zeta(z))^2 / \zeta(2z) = \tilde{d}_2(z)\tilde{f}_2(z)$

Así obtenemos

$$\sum_{\partial(A)=k} \tilde{d}_*(A) = \sum_{k=0}^{\infty} \left(\sum d_*(A)\right) q^{-kz}$$

$$= \sum_{k=0}^{\infty} q^k (k+1) q^{-kz} \sum_{k=0}^{\infty} (1-qq^{-2z}) q^{-kz}$$

$$= \sum_{k=0}^{\infty} (k+1) q^k (1-qq^{-2z}) q^{-kz}$$

haciendo $a_k = (k+1)q^k$ y $b_k = \begin{cases} 1 & \text{si } k = 0 \\ -q & \text{si } k = 2 \\ 0 & \text{si } k = 1 \text{ y } k \geqslant 2 \end{cases}$

obtenemos

$$C_k = (k+1)q^k - (k-1)q^{k-1}$$

Así pues,

$$\sum_{\partial(A)=k} d_*(A) = (k+1)q^k - (k-1)q^{k-1}$$

(e') Sabiendo que $\tilde{\lambda}(z) = \zeta(2z)/\zeta(z) = \tilde{f}_2(z)\tilde{\mu}(z)$

tenemos

$$\sum_{K=0}^{\infty} \left(\sum_{\partial(A)=k} \lambda(A) \right) q^{-kz} = \sum_{k=0}^{\infty} (q^k q^{-2kz})(1-qq^{-z}) q^{-kz}$$

$$= \sum_{K=0}^{\infty} (-1)^k q^{\left[\frac{k+1}{2}\right]} q^{-kz}$$

de donde obtenemos que

$$\sum_{\partial(A)=k} \lambda(A) = (-1)^k q^{\left[\frac{k+1}{2}\right]}$$

(f') Como $\tilde{\sigma}_s(z) = \zeta(z)\zeta(z-s)$ obtenemos

$$\sum_{\partial(A)=k} \sigma_s(z) = \sum_{k=0}^{\infty} q^k q^{-kz} \sum_{k=0}^{\infty} q^k q^{-k(z-s)}$$

$$= \sum_{k=0}^{\infty} q^k q^{-kz} \sum_{k=0}^{\infty} q^{k(1+s)} q^{-kz}$$

$$= \sum_{k=0}^{\infty} q^k q^{k(1+s)} q^{-kz}$$

de donde, por el producto de Cauchy

$$a_k = q^k \quad y \quad b_k = q^{k(1+s)}$$

Obtenemos

$$C_k = q^k \sum_{l=0}^{\infty} q^{ls} = q^k \left[\frac{q^{s(k+1)}-1}{q^s-1}\right]$$

por tanto

$$\sum_{\partial(A)=k} \sigma_s(A) = q^k \left[\frac{q^{s(k+1)}-1}{q^s-1}\right]$$

(g') Sabemos que $\phi = \mu * ||$ y que

$$\tilde{\phi}(z) = \tilde{\mu}(z) \tilde{||}(z) = \zeta(z-1)/\zeta(z)$$

ahora tenemos

$$\sum_{\partial(A)=k} \phi(A) = \sum_{k=0}^{\infty} \Big(\sum_{\partial(A)=k} \phi(A) \Big) q^{-kz}$$

$$= \sum_{k=0}^{\infty} |(1-qq^{-z})q^{2k}| q^{-kz}.$$

haciendo $a_k = q^{2k}$ y $b_k = \begin{cases} 1 & \text{si } k = 0 \\ -q & \text{si } k = 1 \\ 0 & \text{si } k \geqslant 2 \end{cases}$

obtenemos $C_k = q^{2k} - q^{2k+1}$

Así

$$\sum_{\partial(A)=k} \phi(A) = q^{2k} - q^{2k-1} \quad \text{si } k \geqslant 1.$$

(h') Como $\tilde{d}_2^2(z) = \left[\zeta(z)\right]^4 / \zeta(2z)$ y por (a') sabemos

$$\left[\zeta(z)\right]^4 = \tilde{d}_4(z) = \sum_{k=0}^{\infty} (d_4(A)) q^{-kz}$$

$$= \sum_{k=0}^{\infty} \binom{k+3}{3} q^k q^{-kz}$$

es decir $\displaystyle\sum_{\partial(A)=k} d_4(A) = \binom{k+3}{3} q^k$

ahora bien,

$$\tilde{d}_2^2(z) = \tilde{d}_4(z)\tilde{f}_2(z)$$

$$= \sum_{k=0}^{\infty} \binom{k+3}{3} q^k (1-q^{-2z}) q^{-kz}$$

haciendo $a_k = \binom{k+3}{3}$ y $b_k = \begin{cases} 1 & \text{si } k = 0 \\ -q & \text{si } k = 2 \\ 0 & \text{si } k = 1 \text{ y } k \geq 2 \end{cases}$

tenemos

$$\sum_{k=0}^{\infty} \binom{k+3}{3} q^k (1-q^{-2z}) q^{-kz} = \sum_{k=0}^{\infty} \left[\binom{k+3}{3} q^k - \binom{k+1}{3} q^{k-1} \right] q^{-kz}$$

Así

$$\sum_{\partial(A)=k} (d_2(A))^2 = \left[\binom{k+3}{3} q^k - \binom{k+1}{3} q^{k-1} \right]$$

$$= \frac{q^k}{q} \left[\binom{k+3}{3} q - \binom{k+1}{3} \right]$$

Donde además hemos supuesto que $\binom{k}{r} = 0$ si $r > k$. Este resultado es verdadero para $k \geq 2$, ya que si $k = 0; \sum (d_2(A))^2 = 1$ y si $k = 1$, $\sum (d_2(A))^2 = \binom{4}{3} q$.

(1') Por un lado tenemos que

$$\tilde{\Lambda}(z) = -\frac{\zeta'(z)}{\zeta(z)} = -\zeta'(z) \tilde{\mu}(z)$$

pero
$$\zeta'(z) = -\log q \sum_{k=0}^{\infty} k q^k q^{-kz}$$

de donde obtenemos

$$\sum_{k=0}^{\infty} \left(\sum_{\partial(A)=k} \Lambda(A) \right) q^{-kz} = \log q \sum_{k=0}^{\infty} k q^k q^{-kz} (1 - q q^{-z})$$

haciendo $a_k = kq^k$ y $b_k = \begin{cases} 1 & \text{si } k = 0 \\ -q & \text{si } k = 1 \\ 0 & \text{si } k \geq 2 \end{cases}$

obtenemos

$$C_k = q^k \quad \text{para } k \neq 0$$

Es decir

$$\sum_{\partial(A)=k} \Lambda(A) = \begin{cases} 0 & \text{si } k = 0 \\ (\log q)\, q^k & \text{si } k \geq 1 \end{cases}$$

Así

$$\sum_{\partial(A)=k} \Lambda(A) = (\log q)\, q^k \qquad \text{si } k \geq 1;\ 0 \text{ si } k = 0$$

II.3- CONDICIONES NECESARIAS Y SUFICIENTES PARA QUE UNA FUNCION ARITMETICA PUEDE EXPRESARSE COMO UN PRODUCTO DE FUNCIONES $\mathcal{T}$

Consideremos $\mathbb{C}[[Y]]$ el anillo de las series formales de potencias en la indeterminada Y y coeficientes en $\mathbb{C}$. La aplicación

$$\wedge : \text{PIM}(\mathbb{M}) \longrightarrow \mathbb{C}[[Y]]$$

definida por $\qquad f \longrightarrow \hat{f} = \sum_{r=0}^{\infty} f(P^r)Y^r$; donde P es un primo fijo, <u>es un monomorfismo multiplicativo</u>. En efecto:

$$\hat{f}\,\hat{g} = \Big(\sum_{r=0}^{\infty} f(P^r)Y^r\Big)\Big(\sum_{r=0}^{\infty} g(P^r)Y^r\Big)$$

$$= \sum_{r=0}^{\infty} \Big(\sum_{i=0}^{\infty} f(P^r)g(P^{r-i})Y^r$$

$$= \widehat{f * g}$$

Supongamos ahora que $\hat{f} = \hat{g}$, de modo que

$$\sum_{r=0}^{\infty} \left[f(P^r)-g(P^r)\right] Y^r = 0,$$

pero esto implica que $f(P^r)-g(P^r) = 0$ para todo $r \geqslant 0$, y para todo P pues tanto f como g pertenecen a PIM $(\mathbb{M})$. Por tanto, $f = g$.

Consideremos $\mathbb{Z}[[Y]]$ el subanillo de $\mathbb{C}[[Y]]$ de las series formales de coeficientes en $\mathbb{Z}$. Una serie $g \in \mathbb{Z}[[Y]]$ se dice racional ciclotómica si g puede expresarse como un producto de polinomios ciclotómicos o inversos de éstos, donde un polinomio ciclotómico es uno de la forma $\phi_m(Y) = \prod_i (Y-\alpha_i)$ donde $\alpha_1,\ldots,\alpha_m$ son las distintas raices m-ésimas de la unidad y $\phi_1(Y) = 1-Y$. Si g es de sólo polinomios ciclotómicos, decimos que g es entera ciclotómica en $\mathbb{Z}[[Y]]$.

Definición 2.3.1: Una función $f \in \mathrm{Dir}(\mathbb{M})$ se dice que admite una ζ-fórmula finita si $\breve{f} = \breve{f}(z)$ puede escribirse como producto finito de funciones de la forma $\zeta_{\mathbb{M}}(mz)$ ó inversas de éstas.

Proposición 2.3.1: Una función aritmética $f \in \mathrm{Dir}(\mathbb{M})$ admite una ζ-fórmula finita si, y sólo si, $f \in \mathrm{PIM}(\mathbb{M})$, y $\hat{f}$ es racional ciclotómica.

Prueba. Supongamos que

$$\breve{f}(z) = \prod_{i=1} \left[\zeta(m_i z)\right]^{k_i},$$

donde $m_i > 0$, k_i entero. Como $\zeta(m_i z) = \breve{f}_{m_i}(z)$ vemos que

$$\hat{f}_{m_i} = \sum_{r=0}^{\infty} f_{m_i}(P_i^r)Y^r = \sum_{r=0}^{\infty} Y^{m_i r} = \frac{1}{1-Y^{m_i}}, \text{ resulta}$$

que

$$\hat{f} = \prod_{i=1}^{n} \hat{f}_{m_i}^{\,k_i} = \prod_{i=1}^{n} (1-Y^{m_i})^{-k_i}$$

$$= \prod_{i} \prod_{d|m_i} \left[\phi_d(Y)\right]^{-k_i}$$

donde hemos usado $1-Y^m = \prod_{d|m} \Phi_d(Y)$. (Ver por ejemplo [9]) es decir $\hat{f}$ es racional ciclotómica.

Recíprocamente, si $f \in PIM(M)$ y, $\hat{f}$ es racional ciclotómica con

$$\hat{f} = \prod_i [\Phi_{n_i}(Y)]^{r_i},$$

entonces la fórmula usual de inversión de los polinomios ciclotómicos (ver [8]), implica que

$$\hat{f}(z) \prod_i \prod_{d|n_i} (1-Y^d)^{\mu(n_i)/d^{r_i}}$$

donde μ es la función de Möbius en $\mathbb{Z}$. Por tanto

$$\check{f}(z) = \prod_i \prod_{d|n_i} [\zeta(dz)]^{\mu(n_i|d)r_i}$$

lo que significa que f admite una ζ- fórmula finita.

<u>Corolario</u>: <u>Si</u> $f \in PIM(M)$ <u>y</u> $\hat{f} \in \mathbb{Z}[Y]$, <u>entonces</u> f <u>admite una</u> ζ<u>-fórmula finita si, y sólo si,</u> $\hat{f}$ <u>es entera ciclotómica</u>.

<u>Prueba</u>: Supongamos que $g \in \mathbb{Z}[[Y]]$ es racional ciclotómica, como podemos suponer que $g = h_1/h_2$, donde h_1, h_2 son enteros ciclotómicos primos entre sí, vemos que $h_1 = g\, h_2$, y como $\mathbb{Z}[[Y]]$ es anillo factorial, vemos que necesariamente g es producto de polinomios ciclotómicos y, por tanto, entero ciclotómico. Haciendo $g = \hat{f}$ obtenemos el corolario.

CAPÍTULO III

ORDENES PROMEDIOS DE ALGUNAS FUNCIONES ARITMÉTICAS

CAPITULO III

ORDENES PROMEDIOS DE ALGUNAS FUNCIONES ARITMETICAS

El comportamiento de una función aritmética puede ser irregular para valores grandes de $|A(X)|$, donde $A(X) \in \mathbb{M}(q;X)$. Por ejemplo, si consideramos la función $\mathcal{Z}(A)$ podemos observar que ésta toma el valor 2 una cantidad infinita de veces, precisamente en cada elemento de $\mathbb{P}$. Pero también alcanza valores tan grandes como se quiera cuando $A(X)$ admite un número arbitrariamente grande de factores que estén en $\mathbb{P}$ (recordemos que $\mathbb{P}$ tiene un cardinal infinito enumerable). Algo parecido sucede con otras funciones aritméticas, en cuyo caso, el estudio de la <u>media aritmética</u> de una función f, es decir, la función

$$(1)\quad \hat{f}(t) = \frac{1}{Z(q;t)} \sum_{\substack{A\in\mathbb{M} \\ 0 \leqslant \partial A(X) \leqslant t}} f(A(X)) = \frac{1}{Z(q,t)} \sum_{k=0}^{t} \Big(\sum_{\partial A(X)=k} f(A(X))\Big),$$

donde $Z(q;t) = (1 - q^{t+1})/(1-q)$ designa al número de elementos de $\mathbb{M}$ de grado $\leqslant t$, puede resultar provechoso, porque estos promedios moderan, en general, las fluctuaciones de f y es entonces razonable pensar que $\hat{f}$ tenga un comportamiento más regular que el de f. Lo usual en estos casos es estudiar este comportamiento comparando $\hat{f}(t)$ con otra función $g(t)$, de comportamiento conocido, que le sea <u>asintóticamente igual</u> cuando $t\to\infty$, es decir tal que $\lim_{t\to\infty} \hat{f}(t)/g(t) = 1$, en cuyo caso decimos que el <u>orden promedio</u> de $f(t)$ es $g(t)$.

Nuestro propósito en este capítulo es determinar el orden promedio de las funciones aritméticas estudiadas en el Capítulo II.

(3.1) La siguiente notación

$$(2) \qquad Z(q^s;t) = \sum_{k=0}^{t} (q^s)^k = \frac{1 - q^{s(t+1)}}{1 - q^s}$$

nos facilitará la expresión y manejo de algunas fórmulas y relaciones. Claramente cuando $t \longrightarrow \infty$, la expresión (2) diverge a infinito y su comportamiento es el de la serie geométrica de razón q^s.

Si $\Gamma(x)$ designa a la función gamma o factorial, el siguiente desarrollo, consecuencia del teorema de Stirling, es muy conocido:

$$\binom{k+r-1}{r-1} = \frac{k^{r-1}}{\Gamma(r)} + \sum_{s=1}^{p} c_s k^{r-s-1} + O(k^{r-p-2}),$$

donde las c_s son constantes positivas [6,xv]. en particular, para $p = r - 2$ obtenemos

$$(3) \qquad \binom{k+r-1}{r-1} = \frac{k^{r-1}}{\Gamma(r)} + (c_1 k^{r-2} + \ldots + c_{r-2}k) + O(1)$$

<u>Proposición 3.1.1</u>. <u>El orden promedio de μ es cero cuando $t \longrightarrow \infty$</u>

Prueba. De (b'), proposición 2.2.2, resulta inmediatamente

$$(4) \qquad \sum_{0 \leqslant \partial A \leqslant t} \mu(A) = 1 - q,$$

de donde

$$\hat{\mu}(t) = \frac{1}{Z(q;t)} \sum_{0 \leqslant \partial(A) \leqslant t} \mu(A) = \frac{(1 - q)^2}{1-q^{t+1}} = \frac{\zeta(-t)}{\zeta(0)^2}$$

como $\zeta(-t) \longrightarrow 0$ cuando $t \longrightarrow \infty$, obtenemos nuestro resultado.

Observemos que (4) resuelve nítidamente el análogo de la conjetura de Mertens [4] en $\mathbb{F}_q[X]$, pues nos dice simple y llanamente que el orden de magnitud del miembro izquierdo de (4) es precisamente la constante 1-q.

Proposición 3.1.2. El orden promedio de λ es cero cuando $t \to \infty$.

Prueba: De (e') proposición 2.2.2, tenemos

$$(5) \quad \sum_{k=0}^{t} \Big(\sum_{\partial A=k} \lambda(A) = \sum_{k=0}^{t} (-1)^k \, q^{[\![\frac{k+1}{2}]\!]}$$

$$= \begin{cases} 1 & \text{si } t \text{ es par,} \\ 1 - q^{(t+1)/2} & \text{si } t \text{ es impar} \end{cases}$$

Luego

$$\hat{\lambda}(t) = \begin{cases} (1-q)/(1-q^{t+1}) & \text{si } t \text{ es par,} \\ (1-q)/\ 1-q^{(t+1)/2} & \text{si } t \text{ es impar,} \end{cases}$$

expresión que define una función de t que tiende a cero cuando $t \longrightarrow \infty$.

Observemos también aquí que la fórmula (e') de la proposición 2.2.2 nos permite analizar fácilmente el análogo en $F_q\,[X]$ de la llamada conjetura de Turán en $\mathbb{N}$ [11] :

(6) $$\sum_{n \leqslant x} \lambda(n)/n \geqslant 0 \quad (x \geqslant 1)$$

En efecto, en $\mathbb{F}_q[X]$, tenemos

$$\sum_{0 \leqslant \partial A \leqslant t} \lambda(A)/|A| = \sum_{k=0}^{t}\Big(\sum_{\partial A=k}\lambda(A)\Big)q^{-k}$$

$$= \begin{cases} q^{-t/2} & \text{si } t \text{ es par,} \\ 0 & \text{si } t \text{ es impar,} \end{cases}$$

lo que muestra que en $\mathbb{F}_q[X]$ el análogo de la conjetura de Turán es correcta, mientras que (6) parece no ser cierta en $\mathbb{N}^*$, según la información no muy precisa dada en [11]

Por otra parte, el análogo de la <u>conjetura de Pólya</u>.

$$\sum_{n \leqslant x} \lambda(n) \leqslant 0, \text{ para } x \geqslant 2,$$

que no es correcta en $\mathbb{N}^*$ [7] , tampoco lo es en $\mathbb{F}_q[X]$ como lo muestra la relación (5).

<u>Proposición 3.1.3</u>. <u>El orden promedio de $d_*(t)$ es $(1-1/q)t$ cuando</u> $t \longrightarrow \infty$.

Prueba: Por (d'), proposición 2.2.2, obtenemos

$$\sum_{\partial A=k} d_*(A) = \begin{cases} 1 & \text{si } k = 0 \\ (k+1)q^k - (k-1)q^{k-1} & \text{si } k \geqslant 1 \end{cases}$$

Por tanto

$$\sum_{k=0}^{t}\Big(\sum_{\partial A=K} d_*(A)\Big) = 1 + \sum_{k=1}^{t}\Big[(k+1)q^k - (k-1)q^{k-1}\Big]$$

$$= \sum_{k=1}^{t} k(q^k - q^{k-1}) + q^{k-1} + \sum_{k=0}^{t} q^k$$

$$= \sum_{k=1}^{t}\Big[k(q^k - q^{k-1}) + q^{k-1}\Big] + Z(q;t)$$

$$= tq^t + Z(q;t)$$

Por consiguiente

$$\widehat{d}_*(t) = 1 + \frac{tq^t}{Z(q;t)} = 1 + t(1 - 1/q)\Big(\frac{1}{1 - \frac{1}{q^{t+1}}}\Big)$$

y entonces

$$\frac{d_*(t)}{t(1-1/q)} = \frac{1}{t(1-1/q)} + \frac{1}{(1 - 1/q^{t+1})}$$

tiende a 1 cuando $t \longrightarrow \infty$, tal como queríamos demostrar.

<u>Proposición 3.1.4</u>. <u>El orden promedio de f_r es $q^{[\![t/r]\!] - t}$ cuando $t \longrightarrow \infty$</u>

Prueba: De (c'), proposición 2.2.2, vemos que

$$\sum_{k=0}^{t}\Big(\sum_{\partial A=k} f_r(A)\Big) = Z(q;\ [\![t/r]\!]),$$

y, por consiguiente,

$$\widehat{f}_r(t) = \frac{Z(q;\ [\![t/r]\!])}{Z(q;t)}$$

$$= \frac{q^{[\![t/r]\!]-t} - q^{\frac{1}{t+1}}}{1 - \frac{1}{q^{t+1}}} \longrightarrow 0$$

pues

$$0 \leqslant \frac{q^{[\![t/r]\!]}}{q^t} \leqslant \frac{q^{t/r}}{q^t} = \frac{1}{q^{t(1-1/r)}} \longrightarrow 0$$

cuando $t \longrightarrow \infty$ puesto que, $r \geqslant 2$.

Proposición 3.1.5. <u>El orden promedio de q_r es la constante $1-q^{r-1}$</u> (cuando $t \longrightarrow \infty$).

Prueba: De (j'), proposición 2.2.2, obtenemos la relación

$$\sum_{k=0}^{t} \Big(\sum_{\partial A=k} q_r(A) \Big) = \sum_{k=0}^{r-1} q^k + \sum_{k=r}^{t} \left[q^k - q^{(k+1)-r} \right]$$

$$= \sum_{k=0}^{t} q^k - \sum_{k=r}^{t} q^{(k+1)-r}$$

$$= \sum_{k=0}^{t} q^k - (q+q^2+ \ldots + q^{(t+1)-r})$$

$$= 1 + Z(q;t) - Z(q;t+r-1)$$

y en seguida

$$\hat{q}_r(t) = 1 + \frac{1}{Z(q,t)} - \frac{Z(q;t+r-1)}{Z(q;t)}$$

De donde obtenemos

$$\lim_{t\to\infty} \hat{q}_r(t) = 1 - q^{r-1}$$

de donde la proposición.

Proposición 3.1.6: El orden promedio de la función σ_s (s real $\neq 0$) está dado por la función.

$$g(t) = \frac{q^{s(t+2)}}{q^s - 1}$$

Prueba: Usando (f') proposición 2.2.2, obtenemos

$$\sum_{k=0}^{t} \Big(\sum_{\partial A = k} \sigma_s(A) \Big) = \frac{Z(q;t) - q^s Z(q^{s+1}\ ;\ t)}{1 - q^s}$$

de donde resulta que

$$\hat{\sigma}_s(t) = \frac{1}{1 - q^s} - \frac{q^s}{1 - q^s} \cdot \frac{1 - q^{(s+1)(t+1)}}{1 - q^{t+1}}$$

y por consiguiente,

$$\frac{\hat{\sigma}_s(t)(q^s - 1)}{q^{s(t+2)}} \longrightarrow 1 \quad \text{cuando } t \longrightarrow \infty$$

como puede verificarse fácilmente.

Proposición 3.1.7: El orden promedio de la función ϕ de Euler es $(q-1)q^t/(q+1)$ cuando $t \longrightarrow \infty$.

Prueba: De (g'), proposición 2.2.2, obtenemos

$$\frac{1}{z(q;t)} \sum_{k=0}^{t} \left(\sum_{\partial A=k} \phi(A) \right) = (1-q)\,\frac{Z(q^2;t-1)}{Z(q;t)} + \frac{q^{2t}}{Z(q;t)}$$

$$= \frac{(1-q)}{1-q^{t+1}}\left(\frac{1-q^{2t}}{1+q} + q^{2t}\right)$$

$$= \frac{1-q}{1+q} \cdot \frac{1+q^{2t+1}}{1-q^{t+1}}$$

Dividiendo por $(q-1)q^t/(q+1)$, obtenemos

$$\frac{1+q^{2t+1}}{q^t - q^{2t+1}} = \frac{\frac{1}{q^{2t+1}} + 1}{\frac{1}{q^{t+1}} - 1} \longrightarrow 1$$

Si $t \to \infty$. Luego $\hat{\phi}(t) \sim (q+1)q^t(q+1)$

<u>Proposición 3.1.8:</u> <u>El orden promedio de la función Λ de Mangoldt está dado por la constante log q.</u>

Prueba: De (i') proposición 2.2.2, obtenemos

$$\sum_{k=0}^{t} \left(\sum_{\partial A=k} \Lambda(A) \right) = q \log q \; Z(q;t-1)$$

de donde

$$\hat{\Lambda}(t) = q \log q \,\frac{Z(q;t-1)}{Z(q;t)} \longrightarrow \log q$$

cuando $t \to \infty$.

Usando la relación (3) vamos a calcular el orden promedio de la función $d_r(t)$. En primer lugar de (a') proposición 2.2.2, y de (3) resulta que

$$\sum_{0 \leqslant \partial A \leqslant t} d_r(A) = \sum_{k=0}^{t} \Big(\sum_{\partial A = k} d_r(A) \Big) = \sum_{k=0}^{t} \binom{k+r-1}{r-1} q^k$$

$$= \sum_{k=0}^{t} \frac{k^{r-1} q^k}{\Gamma(r)} + q \sum_{k=0}^{t-1} q^k \left[C_1 k^{r-2} + \ldots + C_{r-2} k \right]$$

$$+ 0\,(Z(q;t))$$

Por tanto

$$\frac{\Gamma(r)\hat{d}_r(t)}{t^{r-1}} = \frac{1}{t^{r-1}} \sum_{k=0}^{t} \frac{k^{r-1} q^k}{Z(q;t)} +$$

$$+ \frac{\Gamma(r) q}{t^{r-1}\, Z(q;t)} \sum_{k=0}^{t-1} q^k \left[C_1 k^{r-2} + \ldots\ C_{r-2} k \right] + 0\Big(\frac{\Gamma(r)}{t^{r-1}}\Big)$$

Es decir existen constantes k y t_o tales que

$$(6)\quad \left| \frac{\Gamma(r) d_r(t)}{t^{r-1}} - \frac{1}{t^{r-1}} \sum_{k=0}^{t} \frac{k^{r-1} q^k}{Z(q;t)} - \frac{\Gamma(r) q}{t^{r-1} Z(q;t)} \sum_{k=0}^{t-1} q^k \left[C_1 k^{r-2} + \ldots C_{r-2} k \right] \right|$$

$$\leqslant k \frac{\Gamma(r)}{t^{r-1}} ,$$

si $t > t_o$. Como

$$0 \leqslant \frac{q}{Z(q;t)} \sum_{k=0}^{t-1} q^k \left[C_1 k^{r-2} + \ldots + C_{r-2} k \right]$$

$$\frac{q(r-2)Ct^{r-2}\,z(q;t-1)}{z(q;t)} = \frac{(r-2)Ct^{r-2}(q-q^{t+1})}{1-q^{t+1}}$$

en donde $C = \max\left\{ C_i;\ i = 1,\dots, r-2 \right\}$, resulta que

$$0 \leqslant \frac{\Gamma(r)q}{t^{r-1}\,z(q;t)} \sum_{k=0}^{t-1} q^k\left[C_1 k^{r-2} + \dots + C_{r-2}k\right]$$

$$\leqslant \frac{\Gamma(r)C(r-2)}{t^2}\;\frac{(1/q^t) - 1)}{(1/q^{t+1} - 1)} \qquad (r \geqslant 2),$$

cuyo miembro derecho tiende a cero cuando $t \to \infty$, de donde resulta que

$$\lim_{t\to\infty} \frac{\Gamma(r)q}{t^{r-1}z(q;t)} \sum_{k=0}^{t-1} q^k\left[C_1 k^{r-2} + \dots C_{r-2}k\right] = 0$$

Como el miembro izquierdo de (6) tiende a cero cuando $t \to \infty$, resulta que

$$(7)\ \lim_{t\to\infty}\left(\frac{\Gamma(r)d_r(t)}{t^{r-1}} - \frac{1}{t^{r-1}}\sum_{k=0}^{t}\frac{k^{r-1}q^k}{z(q;t)}\right) = 0$$

Mostremos ahora que

$$(8)\quad \lim_{t\to\infty}\frac{1}{t^{r-1}}\sum_{k=0}^{t}\frac{k^{r-1}q^k}{z(q;t)} = v_q$$

existe, donde $1 - 1/q \leqslant v_q \leqslant 1$. En efecto, hagamos

$$v_q(t) = \frac{1}{t^{r-1}} \sum_{k=0}^{t} \frac{k^{r-1}q^k}{z(q;t)}$$

Entonces

$$0 \leqslant v_q(t) \leqslant \frac{1}{t^{r-1}z(q;t)} (q + \dots + t^{r-1}q^t)$$

$$< \frac{t^{r-1}q\,(1 + \dots + q^{t-1})}{t^{r-1}\,(1 + \dots q^t)} \leqslant 1$$

para todo $t > 1$. Por otra parte

$$v_q(t) = \frac{(q+2^{r-1}q^2 + \dots + t^{r-1}q^t}{t^{r-1}z(q;t)} > \frac{t^{r-1}\,q^{t(1-q)}}{t^{r-1}(1-q^{t+1})}$$

$$= \frac{q^t - q^{t+1}}{1 - q^t} \geqslant 1 - 1/q$$

para todo $t > 1$ luego

$$1 - 1/q \leqslant v_q(t) \leqslant 1, \text{ para todo } q, \text{ para todo } t > 1$$

Sea $u_q(t) = \dfrac{1}{t^{r-1}z(q;t)} = \dfrac{1-q}{t^{r-1}\,(1-q^{t+1})}$

entonces

$$u_q(t+1)-u_q(t) = \frac{1-q}{t^{r-1}} \left[\frac{t^{r-1}}{(1+t)^{r-1}} - \frac{1}{1-q^{t+2}} - \frac{1}{1-q^{t+1}}\right]$$

$$\sim \frac{1-q}{t^{r-1}}\left[\frac{1}{q^{t+1}} - \frac{1}{q^{t+2}}\right] \sim -\frac{(1-q)^2}{t^{r-1}q^{t+2}} < 0,$$

cuando $t \to \infty$. Es decir, existe t_q tal que si $t \geqslant t_q$, entonces $u_q(t+1) - u_q(t) < 0$. Como

$$v_q(t) = u_q(t) \sum_{k=0}^{t} k^{r-1} q^k$$

entonces, si $t \geqslant t_q$,

$$v_q(t+1) - v_q(t) = \left[u_q(t+1) - u_q(t)\right] \sum_{k=0}^{t+1} k^{r-1} q^k + u_q(t)(t+1)^{r-1} q^{t+1}$$

$$\geqslant \left[u_q(t+1) - u_q(t)\right] (t+1)^{r-1} \sum_{k=1}^{t+1} q^k + u_q(t)(t+1)^{r-1} q^{t+1}$$

$$\sim (t+1)^{r-1}\left[\frac{-(1-q)^2}{t^{r-1}q^{t+2}} \quad \frac{1-q^{t+1}}{1-q}\, q + \frac{1-q}{t^{r-1}(1-q^{t+1})}\, q^{t+1}\right]$$

$$= (1-q)\left(\frac{t+1}{t}\right)^{r-1}\left[\frac{1-q^{t+1}}{q^{t+1}} + \frac{q^{t+1}}{1-q^{t+1}}\right]$$

$$= (1-q)\left(\frac{t+1}{t}\right)^{r-1}\left[\frac{q^{t+1}-1}{q^{t+1}} - \frac{q^{t+1}}{q^{t+1}-1}\right] > 0$$

Esto demuestra que $v_q(t+1) > v_q(t)$ para todo t lo suficientemente grande. Como

$$1 - 1/q \leqslant v_q(t) \leqslant 1$$

Si $t > 1$, se deduce que $\lim\limits_{t \to \infty} v_q(t) = v_q$ existe y que

$$1 < 1/q \leqslant v_q \leqslant 1.$$

Podemos, pues, enunciar la siguiente proposición

Proposición 3.1.9. <u>El orden promedio de la función</u> d_r $(r \geqslant 2)$ <u>está dado por</u> $v_q \dfrac{t^{r-1}}{\Gamma(t)}$ cuando $t \to \infty$.

La prueba resulta de la discusión anterior.

Pasemos ahora a $\left[d_2(A)\right]^2 = D(A)$. Tenemos

$$\sum_{k=0}^{t} \Big(\sum_{\partial A = k} D(A) \Big) = 1 + \sum_{k=1}^{t-1} \binom{k+2}{2} q^k + \binom{t+3}{3} q^t$$

$$= \sum_{k=0}^{t-1} \binom{k+2}{2} q^k + \binom{t+3}{3} q^t;$$

de donde

$$\hat{D}(t) = \frac{1}{z(q;t)} \left[\sum_{k=0}^{t-1} \binom{k+2}{2} q^k + \binom{t+3}{3} q^t \right]$$

$$= d_3(t-1) \frac{z(q;t-1)}{z(q;t)} + \binom{t+3}{3} \frac{q^t}{z(q;\, t)}$$

Por consiguiente

$$\frac{\Gamma(3)D(t)}{(t-1)^2} = \frac{\Gamma(3)d_3(t-1)}{(t-1)^2} \frac{(1-q^t)}{(1-q^{t+1})} + \binom{t+3}{3} \frac{\Gamma(r)q^t(1-q)}{(t-1)^2(1-q^{t+1})}$$

El primer sumando de la derecha tiende a 1/q cuando $t \to \infty$. Veamos que pasa con el segundo sumando. Utilizando una fórmula muy conodida tenemos

$$\binom{t+3}{3} \frac{\Gamma(3)q^t(1-q)}{(t-1)^2(1-q^{t+1})} = \frac{\Gamma(t+3)}{t\Gamma(t)} \frac{1}{(t-1)^2} \frac{(q^t - q^{t+1})}{(1 - q^{t+1})}$$

$$= \frac{\Gamma(t+3)}{t^3\Gamma(t)} \frac{t^2}{(t-1)^2} \frac{(q^t - q^{t+1})}{(1 - q^{t+1})},$$

expresión que tiende a 1 - 1/q cuando $t \to \infty$, pues $\frac{\Gamma(t+3)}{t^3 \Gamma(t)} \sim 1$ cuando $t \longrightarrow \infty$. [12,58]. Es decir

$$\lim_{t\to\infty} \frac{\Gamma(3)\, D(t)}{(t-1)^2} = v_q$$

Enunciamos ahora la siguiente proposición.

<u>Proposición 3.1.10</u>. <u>El orden promedio de la función aritmética</u> D(A) <u>está dado por</u> $g(t) = (t-1)^2\, v_q / \Gamma(3)$

CONCLUSIONES

CONCLUSIONES

Hemos escogido el monoide ($\mathbb{M}(q;X)$) de los polinomios sobre un cuerpo finito $\mathbf{F}_q$, primero por la sencillez de algunos resultados y segundo porque en este monoide no se cumple el axioma A. "Existen constantes positivas A y δ que dependen de G, y una constante η con $0 \leq \eta \leq \delta$ tal que

$$N_G = AX^{\delta} + O(X^{\eta})\text{"}$$

en el cual KNOPMACHER basa sus resultados.

Entre los resultados sobresalientes que logramos están:

(1) Establecer un isomorfismo entre el álgebra de Dirichlet ($\mathrm{Dir}(\mathbb{M})$) y el álgebra de las series formales. Este isomorfismo nos permitirá un camino más sencillo que el usado por "Carlitz" para obtener relaciones y ordenes promedios de algunas funciones aritméticas.

(2) Expresar funciones aritméticas (f) como producto de funciones ζ de Riemann y obtener expresiones para $\sum_{\partial(A)=k} f(A)$, todo esto con la ayuda del isomorfismo establecido anteriormente.

(3) Encontrar ordenes promedios para las funciones aritméticas.

BIBLIOGRAFÍA

[1] **ALBIS GONZALEZ, VICTOR S.** ON A THEOREM OF MÖBIUS: ELEMENTARY VARIATIONS ON THE POLYNOMIALS TONALITY REV COLOMBIANA MAT 21 (1987) 85-94.

[2] **ALBIS GONZALEZ, VICTOR S.** LECCIONES SOBRE LAS FUNCIONES ARITMÉTICAS (SEMINARIO) 1987. UNIVERSIDAD DE PANAMÁ.

[3] **ALBIS GONZALEZ, VICTOR S.** LECCIONES SOBRE LA ARITMÉTICA DE LOS POLINOMIOS. POLICOPIADO BOGOTÁ UNIVERSIDAD NACIONAL DE COLOMBIA 1989.

[4] **APOSTOL, TOM.** *Introduction to Analytic Number Theory,* NEW YORK SPRINGER-VERLAG, 1976.

[5] **CARLITZ, LEONARD.** THE ARITMETICAL OF POLYNOMIAL IN GALOIS FIELDS. AMER J. MATH 54 (1932)-39-50.

[6] **HASSELGROVE, C.B.** A DISPROOF OF A CONJETURA OF PÓLYA. MATHEMATIKA 5 (1958)-141-148.

[7] **KNOPMACHER, J.; ARIDLEY, J.N.** ARITHMETICAL PROPERTIES OF FINITE RINGS AND ALGEBRAS, AND ANALYTIC NUMBER THEORY II J. REINE ANGEW. MATH 254 (1972), 74-99.

[8] **KNOPMACHER, J.; RIDLEY, J.N.** ANALYTIC PROPERTIES OF FIÑITE RINGS AND ALGEBRAS, AND ANALYTIC NUMBER THEORY V.J. REINE ANGEW. MATH 27 (1974) 95-121.

[9] KNOPMACHER, J.; RIDLEY, J.N. PRIME INDEPENDENT ARITHMETICAL FUNCTIONS. ANNALI MAT. PURA ED APPLICATA. SERIE IV, 101 (1974) 153-169.

[10] MORA OSEJO, LUCIANO. UNA NOTA SOBRE ALGUNAS CONJETURAS EN TEORÍA DE LOS NÚMEROS. REV. COLOMBIANA MAT. 8 (1978).

[11] TITCHMARSH, EDWARD CHARLES. *The Theory of functions*. 2ND ED LONDON: OXFORD UNIVERSITY PRESS, 1939.