UNIVERSIDAD DE PANAMÁ

VICERRECTORÍA DE INVESTIGACIÓN Y POSTGRADO

PROGRAMA DE MAESTRÍA EN MATEMÁTICA

FÓRMULAS ASINTÓTICAS PARA FUNCIONES ARITMÉTICAS EN $\mathbb{F}_q[X]$

por :

Jaime J. Gutiérrez G.

Tesis presentada como uno de los requisitos
para optar al grado de Maestro en Ciencias
con especialización en Matemática.

TM

UNIVERSIDAD DE PANAMA

FACULTAD DE CIENCIAS NATURALES Y EXACTAS
Programa de Maestría Centroamericana en Matemática

PANAMA, _____

Aprobado por:

Director de Tesis _____
Victor Samuel Albis G., Ph. D.

Miembro del Jurado _____
Julio A. Vallarino, M. Sc.

Miembro del Jurado _____
Pedro A. Marrone, M. Sc.

Fecha 17 de julio de 1989

DEDICATORIA

Dedico este trabajo a mi esposa, Islián, y a mi Madre. Se que este paso que doy las hace sentir felices.

AGRADECIMIENTO

Deseo reconocer al Dr. Víctor Albis por el gran apoyo que ha tenido a bien brindarnos.Por su asesoría muchas de las metas trazadas fueron realizadas.

CONTENIDO

INTRODUCCIÓN

Por diversas razones escogimos la Aritmética de Polinomios como tema de nuestro trabajo de graduación. El motivo principal radica en que es bien conocido que la aritmética del anillo de los polinomios $\mathbb{F}_q[X]$ de coeficientes en un cuerpo finito $\mathbb{F}_q$ de q elementos es notablemente similar a la del anillo $\mathbb{Z}$ de los enteros racionales. Ambos son euclídeos y por lo tanto principales y factoriales. Aún más, todo resultado válido en $\mathbb{Z}$ es en general válido en $\mathbb{F}_q[X]$, si el análogo tiene sentido en $\mathbb{F}_q[X]$. Pero la demostración en $\mathbb{F}_q[X]$ es también en general, menos complicada que en $\mathbb{Z}$ dada la "sencillez estructural" de $\mathbb{F}_q[X]$. Esto nos lleva a plantear problemas análogos a los conocidos en la Teoría de Números, los cuales pretendemos resolver basados escencialmente en las propiedades aritméticas de $\mathbb{F}_q[X]$.

La obra ha sido dividida en dos capítulos.

En el primer capítulo abordamos aspectos básicos respecto a los semigrupos aritméticos aditivos tales como : relaciones de congruencia, funciones aritméticas, L-series, etc.

En el segundo capítulo aplicamos los resultados obtenidos en el anterior al caso específico del semigrupo multiplicativo de los polinomios mónicos de $\mathbb{F}_q[X]$, logrando simplificar demostraciones conocidas y establecer fórmulas asintóticas para valores promedio de funciones aritméticas sobre clases de equivalencia.

He creído conveniente incluir un apéndice que contiene resultados relacionados con los temas tratados en §5 del capítulo 1 y §4 del capítulo 2. Estos resultados servirán al lector como referencia inmediata.

CAPITULO I

FUNCIONES ARITMÉTICAS Y L-SERIES EN UN SEMIGRUPO ARITMÉTICO

§1.- Caracteres según una relación de equivalencia.

Consideremos un semigrupo conmutativo G con unidad 1. Sea $\mathcal{R}$ una relación de equivalencia sobre G, para la cual escribimos $a\equiv b(\text{mód}\mathcal{R})$ si los elementos de a y b de G son equivalentes según $\mathcal{R}$. Si dados a,b, $c \in G$, $a\equiv b(\text{mód}\mathcal{R})$ implica que $ac\equiv ab(\text{mód}\mathcal{R})$,decimos que $\mathcal{R}$ es una relación de congruencia. Para una relación de congruencia $\mathcal{R}$ sobre G, decimos que $a \in G$ es invertible módulo $\mathcal{R}$ si existe $b \in G$ tal que $ab\equiv 1(\text{mód}\mathcal{R})$.

Las siguientes propiedades de elementos invertibles módulo $\mathcal{R}$ son de fácil comprobación.

(1.1) Si a es invertible módulo $\mathcal{R}$ y $a\equiv b(\text{mód}\mathcal{R})$ entonces b es invertible módulo $\mathcal{R}$.

(1.2) ab es invertible módulo $\mathcal{R}$ si y sólo si a y b son invertibles módulo $\mathcal{R}$.

Si $\mathcal{R}$ es una relación de congruencia sobre G para cada a elemento de G definimos :

$$\bar{a}=\{\ b \in G : a\equiv b(\text{mód}\mathcal{R})\ \},$$

y denotamos con $G/\mathcal{R}$ al conjunto de estas clases $\bar{a}$ módulo $\mathcal{R}$. De manera muy natural podemos definir sobre $G/\mathcal{R}$ una composición (inducida por la de G) así :

$$(\forall\ \bar{a})\forall(\ \bar{b})(\bar{a}\bar{b}=\overline{ab}),$$

concluyendo inmediatamente que $G/\mathcal{R}$ adquiere así una estructura de semigrupo conmutativo, cuyo elemento unidad es la clase $\bar{1}$ de 1.

El conjunto Γ de las clases de equivalencias de los

elementos de G que son invertibles módulo $\mathcal{R}$ es, por (1.1) y (1.2) un subsemigrupo de $G/\mathcal{R}$. Además, es claro que los elementos de Γ son invertibles para la composición antes definida y, por consiguiente, Γ es un grupo conmutativo. El orden de Γ lo designamos con h.

Si $G/\mathcal{R}$ es finito, decimos que $\mathcal{R}$ es una relación de congruencia finita, en cuyo caso Γ es un grupo finito.

Dados un semigrupo conmutativo G y una relación de congruencia $\mathcal{R}$ sobre G, llamaremos cáracter módulo $\mathcal{R}$ a toda función $\chi: G \longrightarrow \mathbb{C}$ que satisfaga :

(1.3) $\chi(ab)=\chi(a)\chi(b)$ para todo a, b $\in$ G.

(1.4) $\chi(1)= 1$.

(1.5) $\chi(a)=0$ si a no es invertible módulo $\mathcal{R}$.

(1.6) $\chi(a)=\chi(b)$ si $a\equiv b(\text{mód}\mathcal{R})$

Claramente, si χ_1 y χ_2 son caracteres módulo $\mathcal{R}$, la función $\chi(a)=\chi_1(a)\chi_2(a)$, para todo a $\in$ G, satisface (1.3)-(1.6) y es, por tanto, un cáracter módulo $\mathcal{R}$.

El cáracter (llamado cáracter principal) definido por $\chi_0(a)=1$ si a es invertible módulo $\mathcal{R}$ y $\chi_0(a)=0$ en caso contrario, actúa como el elemento unidad de esta multiplicación. Además, si χ es un cáracter módulo $\mathcal{R}$ la función :

$$\chi^{-1}(a) = \begin{cases} 1/\chi(a) \text{ si } \chi(a)\neq 0 , \\ 0 \text{ en caso contrario,} \end{cases}$$

es otro carácter módulo $\mathcal{R}$ que satisface $\chi\chi^{-1}= \chi^{-1}\chi = \chi_0$. De lo

anterior resulta que el conjunto $\mathfrak{X}$ de todos los caracteres módulo $\mathfrak{R}$ conforman un grupo aditivo.

Ahora si $\hat{\Gamma}=\mathrm{Hom}(\Gamma,S^1)$, donde $S^1=\{z \in \mathbb{C} : |z|=1\}$, designa al grupo de caracteres de Γ, la aplicación $\varphi:\hat{\Gamma}\longrightarrow\mathfrak{X}$ definida por $f\longrightarrow\varphi(f)=\chi_f$, donde :

$$\chi_f(a) = \begin{cases} f(\bar{a}) \text{ si } \bar{a} \in \Gamma, \\ 0 \text{ en caso contrario,} \end{cases}$$

es un isomorfismo de grupos, en efecto :

$\chi_{fg}(a)=(fg)(\bar{a}) =f(\bar{a})g(\bar{a})=\chi_f(a)\chi_g(a)$, para todo $a\in G$ muestra que $\varphi(f)\varphi(g)=\varphi(fg)$. Por otra parte, si $\chi_f(a)=\chi_g(a)$ para todo $a \in G$, entonces $f(\bar{a})=g(\bar{a})$ para todo $\bar{a} \in \Gamma$, es decir $f=g$. Finalmente, dado $\chi \in \mathfrak{X}$, la función $f(\bar{a})=\chi(a)$ si $\bar{a}$ está en Γ define un carácter de Γ, en virtud de (1.3)-(1.6).

Si $\mathfrak{R}$ es una relación de congruencia finita sobre G, $\hat{\Gamma}$ y por tanto $\mathfrak{X}$ son grupos finitos, para los cuales valen las relaciones :

$$(1.7) \qquad \sum_{\bar{a}\in\Gamma} \chi(a) = \begin{cases} h \text{ si } \chi=\chi_0, \\ 0 \text{ en caso contrario,} \end{cases}$$

$$(1.8) \qquad \sum_{\chi\in\mathfrak{X}} \chi^{-1}(a)\chi(b) = \begin{cases} h \text{ si } a\equiv b(\mathrm{mód}\,\mathfrak{R}), \\ 0 \text{ en caso contrario,} \end{cases}$$

Observemos que $\chi^{-1}=\bar{\chi}$, donde $\bar{\chi}(a)=\overline{\chi(a)}$ y la barra designa al conjugado del complejo $\chi(a)$.

Para detalles de (1.7) y (1.8) ver [2].

§2.- El álgebra de las funciones aritméticas.

Los detalles de lo que sigue puede consultarse en [3] ó en [6]-[10]. Sea G un monoide libre que posee un conjunto

finito o enumerable de generadores $\mathbb{P}$, cuyos elementos llamaremos los primos de G. Si existe una aplicación grado $\partial: G \longrightarrow \mathbb{Z}^+$, es decir, una aplicación ∂ que cumple :

(2.1) $\partial(1)= 0$; $\partial(p) \geq 1$, para todo $p \in \mathbb{P}$;

(2.2) $\partial(ab)= \partial(a) + \partial(b)$ para $a, b \in G$;

(2.3) $G(n) = \sum_{\substack{a \in G \\ \partial(a)=n}} 1 < \infty \qquad (n=0, 1, \ldots)$

diremos que (G, ∂) es un semigrupo aritmético aditivo.

Si existe una aplicación norma $|\ |: G \longrightarrow \mathbb{Z}^+$, es decir, una aplicación $|\ |$ que cumple :

(2.4) $|1|=1$; $|p| > 1$ para todo $p \in \mathbb{P}$;

(2.5) $|ab|=|a||b|$, para cada $a, b \in G$.

(2.6) $\hat{G}(n)= \sum_{\substack{a \in G \\ |a|=n}} 1 < \infty \qquad (n=0, 1, \ldots)$

diremos que $(G, |\ |)$ es un semigrupo aritmético.

Si (G, ∂) es un semigrupo aritmético aditivo y q es un entero positivo $q > 1$, podemos definir $|\ |: G \longrightarrow \mathbb{Z}^+$ por $|a|=q^{\partial(a)}$ y obtener así un semigrupo aritmético.

En esta sección presentaremos algunas propiedade de las funciones aritméticas de G, es decir, de las funciones $f: G \longrightarrow \mathbb{C}$. El conjunto de estas funciones se designa con Dir(G), y para las operaciones :

(2.7) $(f+g)(a)=f(a)+g(a)$, $f, g \in Dir(G)$, $a, b \in G$.

(2.8) $(\lambda f)(a)= \lambda f(a)$, $\lambda \in \mathbb{C}$, $f \in Dir(G)$, $a, b \in G$.

(2.9) $(f*g)(a)= \sum_{d|a} f(d)g(a/d)$, $f, g \in Dir(G)$, $a, b \in G$.

conforma un $\mathbb{C}$-álgebra conmutativa y unitaria, cuyo elemento unidad es la función :

$$I(a) = \begin{cases} 1 \text{ si } a=1, \\ 0 \text{ en caso contrario,} \end{cases}$$

Para que un elemento $f \in Dir(G)$ sea invertible es necesario y suficiente que $f(1)\neq 0$. Además, el conjunto $Dir^{\times}(G)$ de los elementos invertibles de $Dir(G)$ es un grupo.

Una función aritmetica f se dice multiplicativa si f no es la función nula y $f(ab)=f(a)f(b)$, siempre que $(a,b)=1$. En caso que $f(ab)=f(a)f(b)$ para todo $a, b \in G$ diremos que f es completamente multiplicativa. Las funciones multiplicativas conforman un subgrupo de $Dir^{\times}(G)$.

Es claro ahora que si $\mathcal{R}$ es una relación de congruencia todo carácter χ módulo $\mathcal{R}$ es una función completamente multiplicativa.

§3.- Relaciones aritméticamente distribuidas.

Una relación de congruencia finita $\mathcal{R}$ sobre un semigrupo aritmético aditivo (G,∂) se dice aritméticamente distribuida si :

(AD1) Sólo un número finito de primos de G no son invertibles módulo $\mathcal{R}$.

(AD2) Existe un entero m, que depende sólo de $\mathcal{R}$, tal que si $r > m$, entonces el número de elementos de G de grado r en cualquier clase de equivalencia de Γ es el mismo. Es decir :

$$\sum_{\substack{x\in a \\ \partial(x)=r}} 1 = \sum_{\substack{x\in b \\ \partial(x)=r}} 1$$

El menor entero positivo para el cual se cumple (AD2) se designa con $m(\mathcal{R})$.

Si $\mathcal{R}_1$ y $\mathcal{R}_2$ son dos relaciones de congruencia sobre G, la relación $\mathcal{R}$ definida como $a\equiv b(\text{mód}\mathcal{R})$ si, y sólo si, $a\equiv b(\text{mód}\mathcal{R}_1)$ y $a\equiv b(\text{mód}\mathcal{R}_2)$ es una relación de equivalencia sobre G, llamada la intersección de $\mathcal{R}_1$ y $\mathcal{R}_2$. Por otra parte, dos relaciones de congruencia $\mathcal{R}_1$ y $\mathcal{R}_2$ sobre un semigrupo aritmético aditivo (G,∂) se dicen independientes si para todo a, b $\in$ G existe c $\in$ G tal que $a\equiv c(\text{mód}\mathcal{R}_1)$ y $b\equiv c(\text{mód}\mathcal{R}_2)$. Con otras palabras $\mathcal{R}_1$ y $\mathcal{R}_2$ son independientes si, y sólo si, $H_1\cap H_2\neq\emptyset$ para toda $H_1 \in G/\mathcal{R}_1$ y toda $H_2 \in G/\mathcal{R}_2$.

Tenemos, entonces, los siguientes resultados :

Teorema 3.1 Sean (G,∂) un semigrupo aritmético aditivo, $\mathcal{R}_1$ y $\mathcal{R}_2$ dos relaciones de congruencia sobre G. Si $\mathcal{R}$ es la intersección de $\mathcal{R}_1$ y $\mathcal{R}_2$, entonces :

(1) $\mathcal{R}$ es una relación de congruencia sobre G.

(2) $\Gamma_{\mathcal{R}}$ consiste de todas las intersecciones no vacías $H_1\cap H_2$ donde $H_1 \in \Gamma/\mathcal{R}_1$ y $H_2 \in \Gamma/\mathcal{R}_2$.

(3) Si $\mathcal{R}_1$ y $\mathcal{R}_2$ son finitas y a $\in$ G es invertible tanto módulo $\mathcal{R}_1$ como $\mathcal{R}_2$, entonces a es invertible módulo $\mathcal{R}$.

Demostración : Las afirmaciones (1) y (2) son inmediatas Veamos (3). Que en estas condiciones $\mathcal{R}_1\cap\mathcal{R}_2$ es finita es claro, porque el número de clases, es decir el número de intersecciones $H_1\cap H_2$, donde H_i es una clase de $\mathcal{R}_i$

es finito. Finalmente, sea U_i la clase de equivalencia de 1 módulo $\mathcal{R}_i$ ($i=1,2$), entonces $U_1 \cap U_2$ no es vacía (pues 1 le pertenece) y si $a \in U_i$ ($i=1,2$) entonces $a \in U_1 \cap U_2$, es decir a es invertible módulo $\mathcal{R}$.

Teorema 3.2 Si $\mathcal{R}_1$ y $\mathcal{R}_2$ son relaciones de congruencia finitas e independientes sobre G, y si $\mathcal{R}$ es su intersección, entonces :

(1) $\Gamma_{\mathcal{R}} \cong \Gamma_{\mathcal{R}_1} \times \Gamma_{\mathcal{R}_2}$.

(2) $a \in G$ es invertible módulo $\mathcal{R}$ si, y sólo si, a es invertible módulo $\mathcal{R}_1$ y módulo $\mathcal{R}_2$.

(3) Los caracteres módulo $\mathcal{R}$ son de la forma $\chi_1\chi_2$ donde χ_i es un carácter módulo $\mathcal{R}_i$, $i=1, 2$.

Demostración (1). Definamos $\varphi: G/\mathcal{R} \longrightarrow G/\mathcal{R}_1 \times G/\mathcal{R}_2$. por $\varphi(\bar{a})=(\bar{a},\bar{a})$.(aquí la "barra" indica clase de equivalencia módulo la correspondiente relación). Si $\varphi(a) = \varphi(b)$, entonces $(\bar{a},\bar{a}) = (\bar{b},\bar{b})$ y esto implica que $a \equiv b (\text{mód} \mathcal{R}_i)$ $i=1, 2$. Por lo tanto $\bar{a} = \bar{b}$ en $G/\mathcal{R}$, luego φ es inyectiva.

Sea ahora $(\bar{a},\bar{b}) \in G/\mathcal{R}_1 \times G/\mathcal{R}_2$, como $\mathcal{R}_1$ y $\mathcal{R}_2$ son independientes existe $c \in G$ tal que $(\bar{a},\bar{b})=(\bar{c},\bar{c})=\varphi(c)$, lo que muestra que φ es sobre. Por otra parte $\varphi(\bar{a}\bar{b})= (\bar{a}\bar{b},\bar{a}\bar{b})= (\bar{a},\bar{a})(\bar{b},\bar{b})= \varphi(\bar{a})\varphi(\bar{b})$.

(2). En el teorema 3.1 ya hemos visto que si $a \equiv 1 (\text{mód} \mathcal{R}_i)$ $i=1, 2$. entonces $a \equiv 1 (\text{mód}\ \mathcal{R})$. Recíprocamente, si $a \equiv 1 (\text{mód} \mathcal{R})$ entonces $\varphi(\bar{a})= \varphi(\bar{1})= \varphi(\bar{a},\bar{a})=(\bar{1},\bar{1})$, por lo que $a \equiv 1 (\text{mód} \mathcal{R}_i)$ $i=1,2$. Podemos en virtud de (1) del presente teorema afirmar que $G/\mathcal{R} = G/\mathcal{R}_1 \times G/\mathcal{R}_2$. Si χ_i es un carácter módulo

$\mathcal{R}_i (i=1,2)$, podemos definir $\chi(\bar{a}_1,\bar{a}_2)=\chi_1(\bar{a}_1)\chi_2(\bar{a}_2)$. Por lo tanto χ es un carácter módulo $\mathcal{R}$. Recíprocamente, si χ es un carácter módulo $\mathcal{R}$ definimos χ_i como la restricción de χ a $G/\mathcal{R}_i$, para obtener :

$$\chi(\bar{a}_1,\bar{a}_2)= \chi[(\bar{a}_1,\bar{1})(\bar{a}_2,\bar{1})]= \chi(\bar{a}_1,\bar{1})\chi(\bar{a}_2,\bar{1})=\chi_1(\bar{a}_1)\chi_2(\bar{a}_2)$$

Observemos que este teorema es un generalización del teorema chino de los restos.

§ 4.- L- series de Dirichlet.

Si $f \in Dir(G)$ es completamente multiplicativa y $f(a) \in S^1 \cup \{0\}$, para todo $a \in G$, definimos a

$$(4.1) \qquad L(z,f) = \sum_{d=0}^{\infty} S(d;f)q^{-dz}$$

como su L-serie de Dirichlet, donde :

$$(4.2) \qquad S(d;f) = \sum_{\partial(a)=d} f(a) \ .$$

Observemos que :

$$|S(d;f)| \leq \sum_{\partial(a)=d} |f(a)| \leq G(d)$$

por lo que lo concerniente a la convergencia de la serie (4.1) está supeditada en buena parte al comportamiento de la sucesión $\{G(d)\}_{d\geq 0}$.

Si $\mathcal{R}$ es una relación aritméticamente distribuida sobre G y $\chi \neq \chi_0$ es un carácter módulo $\mathcal{R}$, entonces $S(d;\chi)=0$ si $d > m(\mathcal{R})$. En efecto, sea $G/\mathcal{R} =\{H_1,\ldots H_k\}$ y tomemos $a_i \in H_i$ Si $d > m(\mathcal{R})$, tenemos :

$$(4.3) \qquad S(d,\chi)= \sum_{i=1}^{k} \sum_{\partial(a)=d} \chi(a) = \sum_{i=1}^{k} \chi(a_i) \sum_{\substack{a\in H_i \\ \partial(a)=d}} 1$$

por lo tanto :

$$S(d,\chi) = K\sum_{\iota=1}^{k} \chi(a_\iota)=0$$

(donde K es el valor común de cada una de las sumas $\sum_{\substack{a\in H \\ \partial(a)=d}} 1$)

puesto que, $\sum_{\iota=1}^{k} \chi(a_\iota)=0$, en virtud de (1.7). En este caso, $\chi\neq\chi_o$, la serie $L(z,\chi)$ es un polinomio en q^{-z} :

$$(4.4) \qquad L(z,\chi)= \sum_{d=o}^{m(\mathcal{R})} S(d;\chi)q^{-zd}$$

y define por lo tanto, una función de z analítica en el plano complejo.

Si $\chi = \chi_o$, se verifica formalmente la igualdad :

$$(4.5) \qquad L(z,\chi_o) = \prod_{r} (1-|r|^{-z})^{-1}$$

donde r recorre los irreducibles de G que son invertibles módulo $\mathcal{R}$.

Sea $\chi\neq\chi_o$, y definamos :

$$(4.6) \qquad \beta(Z,\chi) = \sum_{d=o}^{m(\mathcal{R})} S(d;\chi)Z^{m(\mathcal{R})-d}$$

que claramente es una función polinómica de grado $m(\mathcal{R})$.

Podemos, pues, escribir :

$$(4.7) \qquad \beta(Z,\chi) = \prod_{a} (Z-a)$$

donde a recorre las $m(\mathcal{R})$ raíces de $\beta(Z,\chi)$. Observemos que $S(0,\chi)=1$ es el coeficiente de $Z^{m(\mathcal{R})}$ en $\beta(Z,\chi)$. Por

consiguiente, si $\chi \neq \chi_o$:

$$(4.8) \qquad L(z,\chi) = q^{-m(\mathcal{R}oz)}\beta(q^z,\chi)$$

lo que nos permite estudiar con comodidad los ceros de $L(z,\chi)$, si $\chi \neq \chi_o$.

§5.- Algunas funciones aritméticas especiales.

En esta sección presentaremos algunas funciones aritméticas y estudiaremos algunas de sus propiedades. Para detalles remitimos a [3].

(i) La función de Möbius definida por :

$$\mu(a)=\begin{cases} 1 \text{ si } a=1 \\ (-1)^k \text{ si } a=p_1\ldots p_k,\ p_i\in\mathbb{P}, p_i\neq p_j \\ 0 \text{ si existe } p\in\mathbb{P} \text{ tal que } p^2/a. \end{cases}$$

(ii) La función u dada por $u(a)=1$ para todo $a \in G$.

Es interesante señalar que $\mu * u = I$; es decir μ es la inversa multiplicativa de u en Dir(G), y viceversa. Además si f es completamente multiplicativa se cumple :

$$(\mu * f)(a) = f(a)\prod_{\substack{p\in\mathbb{P}\\ p|a}}(1-f(p)^{-1})$$

(iii) La función d(a) que indica el número de divisores de a en G :

$$d(a) = \sum_{d|a} 1$$

(iv) Las generalizaciones de la función anterior :

$$d_k(a)= \sum_{\substack{(b_1,\ \ldots\ b_k)\\ b_1\ldots b_k=a}} 1$$

(k=1, 2, ...). Observemos que $d_1 = u$, $d_2 = d$ y que $d_k = u*...*u$ k veces, si $k \geq 1$.

(v) La función σ_t (t real) definida por :

$$\sigma_t(a) = \sum_{d|a} |d|^t$$

Claramente, $\sigma_0 = d$ y en general $\sigma_t = |\ |^t * u$, donde $|\ |^t(a) = |a|^t$, para todo $a \in G$.

(vi) Si $a = \prod_{i=0}^{k} p_i^{e_i}$, $p_j \in \mathbb{P}$, $e_j \geq 1$, definimos :

$$\omega(a) = \begin{cases} 0 \text{ si } a=1, \\ k \text{ en caso contrario,} \end{cases}$$

ω indica el número de divisores primos de a.

$$\Omega(a) = \begin{cases} 0 \text{ si } a=1, \\ e_1 + e_2 \ldots + e_k \text{ en caso contrario,} \end{cases}$$

$$\beta(a) = \begin{cases} 1 \text{ si } a=1 \\ e_1 \ldots e_k \text{ en caso contrario} \end{cases}$$

(vii) Las funciones de tipo euleriano.

$$\phi(a) = \sum_{\substack{(a,b)=1 \\ \partial(b)<\partial(a)}} 1$$

$$\phi_r(a) = \sum_{\substack{(a,b)=1 \\ \partial(b)=r}} 1$$

$$\hat{\phi}_r(a) = \sum_{\substack{(a,b)=1 \\ |b|=r}} 1$$

También utilizaremos la relación :

$$\phi(a) = \sum_{d|a} \mu(\tfrac{a}{d})|d| \qquad \text{(Veáse [3])}$$

Si f es una función completamente multiplicativa y $h \in Dir(G)$, definimos :

$$(5.1) \quad h(z,f) = \sum_{a\in G} h(a)f(a)|a|^{-z} = \sum_{d=0}^{\infty} \Big(\sum_{\substack{a\in G \\ \partial(a)=d}} h(a)f(a)\Big)q^{-dz}$$

Observemos que toda L-serie es de la forma (5.1)

$$L(z,f) = \sum f(a)|a|^{-z} = u(z,f)$$

En particular , la serie :

$$\xi_G(z) = L(z,u) = \sum_{a\in G} |a|^{-z}$$

la llamaremos función de Riemann de G. Si no hay lugar a confusión, escribimos $\xi(z)$ en vez de $\xi_G(z)$.

Nuestro interés inmediato es determinar h(z,f), para las funciones que hemos mencionado antes, en términos de $\xi(z)$. Pero antes, otra definición : si $f \in Dir(G)$, $f^k(a) := [f(a)]^k$, para todo $a \in G$ y $k=0, 1, \ldots$

<u>Teorema 5.1</u> Sea $f \in Dir(G)$ una función completamente multiplicativa. Entonces :

$$(5.2) \quad d_k(z,f) = [L(z,f)]^k$$

$$(5.3) \quad \sum_{a\in G} f(a)[d(a)]^2|a|^{-z} = [L(z,f)]^4/L(2z,f^2)$$

$$(5.4) \quad \sigma_t(z,f) = L(z,f)L(z-t,f)$$

(5.5) $\hat{d}(z,f) = [L(z,f)]^2/L(2z,f^2)$, donde $\hat{d}(a) = 2^{\omega(a)}$

(5.6) $\mu(z,f) = 1/L(z,f)$

(5.7) $\beta(z,f) = L(z,f)L(2z,f^2)L(3z,f^3)/L(6z,f^6)$

(5.8) $J_t(z,f) = L(z-t,f)/L(z,f)$

CAPITULO II

APLICACIONES AL SEMIGRUPO ARITMÉTICO ADITIVO DE LOS POLINOMIOS UNITARIOS DE $\mathbb{F}_q[X]$

§1.- Algunas propiedades del semigrupo $\mathbb{M}(q,X)$

Sea $\mathbb{F}_q[X]$ el anillo de los polinomios en la indeterminada X y coeficientes en el cuerpo finito $\mathbb{F}_q$ de q elementos. Dado que $\mathbb{F}_q[X]$ es un anillo factorial el conjunto $\mathbb{M}(q,X)$ de los polinomios unitarios (o mónicos) de $\mathbb{F}_q[X]$ es un monoide libre cuyos primos son los polinomios unitarios irreducibles. Designemos con $\mathbb{P}(q,X)$ al conjunto de estos polinomios irreducibles. Por otra parte, $\partial : \mathbb{M}(q,X) \longrightarrow \mathbb{Z}^+$ donde $\partial(A(X))$ designa el grado del polinomio $A(X) \in \mathbb{M}(q,X)$, es claramente una aplicación grado que hace de $(\mathbb{M}(q,X),\partial)$ un semigrupo aritmético aditivo. Si hacemos $|A(X)| = q^{\partial(A(X))}$ obtenemos una aplicación norma.

De ahora en adelante escribiremos $\mathbb{M}$ en vez de $\mathbb{M}(q,X)$ y $\mathbb{P}$ en vez de $\mathbb{P}(q,X)$.

Es importante señalar, como hecho bien conocido, que :

$$(1.1)\quad \mathbb{M}(n) = \sum_{\substack{A\in\mathbb{M} \\ \partial(A)=n}} 1 = q^n \ , \quad (n= 0,\ 1,\ldots)$$

Sea $H = H(X) \in \mathbb{M}$ y consideremos la relación de equivalencia $\mathcal{R}_H$ sobre $\mathbb{M}$ definida por $A \equiv B (\text{mód} \mathcal{R}_H)$ si y sólo si $A-B \in (H)$, donde (H) designa al ideal generado por H en $\mathbb{F}_q[X]$.

Lema 1.1 .Sea $H \in \mathbb{M}$. Si $K \in \mathbb{F}_q[X]$, entonces existe $A \in \mathbb{M}$ tal que $A \equiv K (\text{mód} \mathcal{R}_H)$ y $\partial(A) < \partial(H)$.

Lema 1.2 Sea $H \in \mathbb{M}$. Si $K \in \mathbb{F}_q[X]$ y $r \geq \partial(H)$ existe $A \in \mathbb{M}$ tal que $\partial(A) = r$ y $A \equiv K (\text{mód} \mathcal{R}_H)$.

Demostración .Por el lema 1.1, sabemos que existe $R \in \mathbb{M}$

tal que $\partial(R)<\partial(H)$ y $R\equiv K(\text{mód}\mathcal{R}_H)$. Tomemos $A= R + HC$, donde $C=X^{r-\partial(H)}$. Es claro que $A\equiv K(\text{mód}\mathcal{R}_H)$, $A \in \mathbb{M}$ y $\partial(A) = r$.

Teorema 1.1 Si $H \in \mathbb{M}$, entonces $\text{card}(\mathbb{M}/\mathcal{R}_H) = |H|$.

Demostración. Si en el lema 1.2, hacemos $r = \partial(H)$, tenemos que todo polinomio de $\mathbb{M}$ es congruente a un polinomio unitario de grado $\partial(H)$, y como dos polinomios unitarios de grado $\partial(H)$ no pueden ser congruentes módulo $\mathcal{R}_H$, resulta que $\text{card}(\mathbb{M}/\mathcal{R}_H) = \mathbb{M}(\partial(H)) = q^{\partial(H)} = |H|$.

Corolario. Dado $H \in \mathbb{M}$, la relación $\mathcal{R}_H$ es una relación de congruencia finita sobre $\mathbb{M}$.

Teorema 1.2. Dados H, $K \in \mathbb{M}$ y $r\geq\partial(H)$, existen exactamente $q^r/|H|$ polinomios en $\mathbb{M}$ de grado r que son congruentes con K módulo $\mathcal{R}_H$.

Demostración . Por el lema 1.2, existe $A \in \mathbb{M}$ tal que $\partial(A) = r$ y $A\equiv K(\text{mód}\mathcal{R}_H)$. Hagamos $B = A + RH$, con $\partial(R)<r-\partial(H)$, de modo que $B \in \mathbb{M}$, $\partial(B) = r$ y $B\equiv A(\text{mód}\mathcal{R}_H)$. Por tanto, $B\equiv K(\text{mód}\mathcal{R}_H)$. Además, como todo polinomio unitario B de grado r congruente con K módulo $\mathcal{R}_H$, es de la forma $A + RH$, con $\partial(R)<r-\partial(H)$, resulta que existen $q^{r-\partial(H)} = q^r/|H|$ de tales polinomios.

Teorema 1.3. Sean H, $A \in \mathbb{M}$. Entonces A es invertible módulo $\mathcal{R}_H$ si, y sólo si, $(A,H) = 1$.

Demostración. Decir que A es invertible módulo $\mathcal{R}_H$ equivale a decir que existe $B \in \mathbb{M}$ tal que $AB\equiv 1(\text{mód}\mathcal{R}_H)$. Pero entonces $AB + HC = 1$ para algún $C \in \mathbb{F}_q[X]$ y esto implica que $(A,H) = 1$. Recíprocamente, si $(A,H) = 1$, existen B y C en

$\mathbb{F}_q[X]$ tales que AB + HC = 1 y por tanto $AB \equiv 1 (\text{mód} \mathcal{R}_H)$, por el lema 1.1, podemos escoger $B \in \mathbb{M}$. Por lo tanto A es invertible módulo $\mathcal{R}_H$.

Corolario . Si Γ es el grupo de las clases de elementos invertibles módulo $\mathcal{R}_H$ ($H \in \mathbb{M}$), entonces su orden está dado por :

$$\phi(H) = \sum_{\substack{(A,H)=1 \\ \partial(A)<\partial(H)}} 1$$

Si $H \in \mathbb{P}$, $\phi(H) = |H|-1$.

Teorema 1.4 . Si $H \in \mathbb{M}$, entonces la relación $\mathcal{R}_H$ está aritméticamente distribuida sobre $\mathbb{M}$.

Demostración . Por el teorema 1.3, los polinomios de $\mathbb{M}$ que no son invertibles módulo $\mathcal{R}_H$ son precisamente aquellos que tienen un factor común, de grado mayor o igual que 1, con H. Así, un polinomio de $\mathbb{P}$ que no es invertible módulo $\mathcal{R}_H$ es necesariamente un divisor irreducible de H. Como sólo existen un número finito de tales irreducibles, hemos comprobado que $\mathcal{R}_H$ verifica (AD1). Que $\mathcal{R}_H$ verifica (AD2) es una consecuencia inmediata del teorema 1.2.

§2.- L-funciones relativas a la relación $\mathcal{R}_H$

Si $\mathbb{E}$ es un subconjunto de $\mathbb{M}$ y $n \geq 0$ es un entero, definimos :

$$\mathbb{E}(n) = \{ A \in \mathbb{E};\ \partial(A) = n \} \quad ; \quad N_{\mathbb{E}}(n) = \text{card}\,\mathbb{E}(n)$$

y

$$\mathbb{E}[n] = \{ A \in \mathbb{E};\ \partial(A) \leq n \} \quad ; \quad N_{\mathbb{E}}[n] = \text{card}\,\mathbb{E}[n]$$

Es claro entonces que :

$$\mathbb{E}[n] = \bigcup_{\iota=0}^{n} \mathbb{E}(\iota) \text{ y } N_{\mathbb{E}}[n] = \sum_{\iota=0}^{n} N_{\mathbb{E}}(\iota)$$

También, si $A \in \mathbb{M}$ designamos con $\bar{A}$ su clase módulo $\mathcal{R}_H$.

Teorema 2.1 . Si $A \in \mathbb{M}$, entonces :

$$N_{\bar{A}}[r] = \sum_{\substack{B \in \bar{A} \\ \partial(B) \leq r}} 1 = q^{r+1}/(q-1)|H| + O(1)$$

cuando $r \longrightarrow \infty$

Demostración . Si tomamos $r \geq \partial(H)$, obtenemos :

$$N_{\bar{A}}[r] = \sum_{\iota=0}^{r} N_{\bar{A}}(\iota) = \sum_{\iota=0}^{\partial(H)-1} N_{\bar{A}}(\iota) + \sum_{\iota=\partial(H)}^{r} N_{\bar{A}}(\iota)$$

Pero,

$$\sum_{\iota=\partial(H)}^{r} N_{\bar{A}}(\iota) = \sum_{\iota=\partial(H)}^{r} q^{\iota}/|H| = (1/|H|)\sum_{\iota=\partial(H)}^{r} q^{\iota}$$

$$= (1/|H|)(q^{r+1}-q^{\partial(H)})/(q-1)$$

$$= q^{r+1}/|H|(q-1) - 1/(q-1)$$

en virtud del teorema 1.2. Por consiguiente queda establecido el teorema 2.1.

Teorema 2.2.

$$N_{\mathbb{M}}[r] = q^{r+1}/(q-1) - 1/(q-1) = q^{r+1}/(q-1) + O(1)$$

Demostración .

$$N_{\mathbb{M}}[r] = \sum_{\iota=0}^{r} N_{\mathbb{M}}(\iota) = \sum_{\iota=0}^{r} q^{\iota} = (q^{r+1}-1)/(q-1)$$

$$= q^{r+1}/(q-1) - 1/(q-1)$$

en virtud de (1.1).

Sea $\mathfrak{X}$ el grupo de caracteres módulo $\mathcal{R}_H$ ($H \in \mathbb{M}$) y $\chi \in \mathfrak{X}$, $\chi \neq \chi_o$. Entonces por (4.3) del capítulo 1 se tiene :

$$(2.1) \qquad S(d,\chi) = \sum_{A \in \mathbb{M}(d)} \chi(A) = 0 \ ; \ \text{si } d \geq \partial(H)$$

De aquí resulta lo siguiente :

Teorema 2.3. Si $\chi \in \mathfrak{X}$ es un carácter módulo $\mathcal{R}_H$, $\chi \neq \chi_o$, entonces :

$$\sum_{A \in \mathbb{M}[r]} \chi(A) = O(1)$$

Demostración . Si $r \geq \partial(H)$, tenemos :

$$\sum_{A \in \mathbb{M}[r]} \chi(A) = \sum_{\iota=0}^{r} |S(\iota,\chi)| = \sum_{\iota=0}^{\partial(H)-1} S(\iota,\chi)$$

Pero entonces, si $n = \partial(H)-1$ se tiene :

$$\left| \sum_{A \in \mathbb{M}[r]} \chi(A) \right| \leq \sum_{\iota=0}^{n} S(\iota,\chi) \leq \sum_{\iota=0}^{n} q^{\iota} = (q^{\partial(H)} - 1)/(q-1)$$

puesto que :

$$|S(\iota,\chi)| = \left| \sum_{A \in \mathbb{M}(\iota)} \chi(A) \right| \leq \sum_{A \in \mathbb{M}(\iota)} 1 = q^{\iota}$$

y de aquí resulta la fórmula pedida.

Teorema 2.4. Sea $F \in \mathrm{Dir}(\mathbb{M})$ y supongamos que para cada carácter χ módulo $\mathcal{R}_H$ se verifica :

$$\sum_{A \in \mathbb{M}(r)} \chi(A)F(A) = f(\chi,r) + O(\rho(r)), \quad r \longrightarrow \infty$$

Entonces, para cada clase $\mathbb{E}$ invertible módulo $\mathcal{R}_H$ se tiene :

$$(2.2)\quad \sum_{A\in\mathbb{E}(r)} F(A) = (1/\phi(H))\sum_{\chi\in\mathcal{X}} \chi(\mathbb{E})f(\chi,r) + O(\nu(r))$$

Demostración. Sea $\mathbb{E}$ una clase invertible módulo $\mathcal{R}_H$, entonces :

$$\sum_{A\in\mathbb{M}(r)} \bar{\chi}(\mathbb{E})\chi(A)F(A) = \chi(\mathbb{E})f(r,\chi) + O(\nu(r)) \quad (r\longrightarrow\infty)$$

así :

$$\sum_{A\in\mathbb{M}(r)} \Big[\sum_{\chi\in\hat{\Gamma}} \chi(\mathbb{E})\chi(A)F(A) \Big] = \sum_{\chi\in\Gamma} \Big[\sum_{A\in\mathbb{M}(r)} \chi(\mathbb{E})\chi(A)F(A)\Big]$$

$$= \sum_{\chi\in\Gamma} \bar{\chi}(\mathbb{E})f(\chi,r) + O(\nu(r))$$

usando (1.8) del capítulo 1, finalmente obtenemos lo afirmado en (2.2).

Corolario. Si $f(r,\chi) = O(\nu(r))$, $r\longrightarrow\infty$ para todo $\chi \neq \chi_0$. Entonces para cada clase invertible módulo $\mathcal{R}_H$ tenemos :

$$\sum_{A\in\mathbb{E}(r)} F(A) = f(r,\chi_0)/\phi(H) + O(\nu(r)) \ , \ r\longrightarrow\infty$$

Demostración . Se sigue inmediatamente de (2.2) y de la hipótesis.

Si $F \in Dir(\mathbb{M})$ puede escribirse como un producto finito de ξ funciones, y como cada una de ellas es un polinomio en q^{-z}, obtenemos inmediatamente la existencia de un entero positivo $m(F,\mathcal{R}_H) = m$ tal que :

$$\sum_{A\in\mathbb{M}(r)} F(A)\chi(A) = 0 \ , \text{ si } r > m \ \text{ y } \chi \neq \chi_0.$$

Con el fin de aplicar la proposición (2.4) y su

corolario es suficiente estudiar el comportamiento de :

$$\sum_{A\in M(r)} F(A)\chi_0(A) \quad \text{cuando } r\longrightarrow\infty$$

Lema 2.1. Para todo número positivo ε, tenemos :

(a) $d_k(A) = O(|A|^{k\varepsilon})$

(b) $\sigma_t(A) = O(|A|^{t+\varepsilon})$

(c) $\phi(A) = O(|A|^{1+\varepsilon})$

(d) $\lambda(A) = O(|A|^{\varepsilon})$, donde $\lambda(A) = (-1)^{\Omega(A)}$

Demostración . (a). En [1] se prueba que $d_2(A)=O(|A|^{\varepsilon})$, es decir $d_2(A)\leq C|A|^{\varepsilon}$ para alguna constante $C>0$. Si $k\geq 1$, observemos que $d_{k+1}(A) = \sum_{D|A} d_k(A)$. Así, si $d_k(A)\leq [d_2(A)]^k$,

obtenemos que $d_{k+1}(A)\leq [d_2(A)]^k \sum_{D|A} 1 = [d_2(A)]^{k+1}$, y como

evidentemente $d_1(A) = u(A) = 1\leq d_2(A)$, tenemos que la desigualdad $d_k(A)\leq [d_2(A)]^k$ es válida para $k = 1,2, \ldots$. Por lo tanto $d_k(A)\leq [d(A)]^k\leq C^k|A|^{k\varepsilon}$ y así $d_k(A) = O(|A|^{k\varepsilon})$, para todo $\varepsilon > 0$.

(b) se sigue inmediatamente de :

$$\sigma_t(A) = \sum_{D|A} |D|^t \leq \sum_{D|A} |A|^t \leq |A|^t d_2(A)\leq C|A|^{t+\varepsilon}$$

(c) se deduce fácilmente de $\sigma_1(A)\leq C_1|A|^{1+\varepsilon}$ y de el hecho conocido :

$$|\phi(A)| = \left| \sum_{D|A} \mu(A/D)|D| \right| \leq \sum_{D|A} |D| = \sigma_1(A)$$

(d) es inmediato pues $\lambda(A) = (-1)^{\Omega(A)}$.

§3.- Fórmulas asintóticas para funciones aritméticas sobre clases de equivalencias módulo $\mathcal{R}_H$.

Teorema 3.1. Para todo $\varepsilon > 0$ y toda clase $\mathbb{E}$ invertible módulo $\mathcal{R}_H$ se tiene :

$$\sum_{A\in\mathbb{E}(r)} d_k(A) = (1/\phi(H))\left[\begin{matrix} r+k-1 \\ k-1 \end{matrix}\right] q^r + O(q^{r(k\varepsilon+1)})$$

Dmostración . Sabemos que :

$$\sum_{A\in\mathbb{M}(r)} d_k(A)\chi_0(A) = \sum_{A\in\mathbb{M}(r)} d_k(A) - \sum_{\substack{A\in\mathbb{M}(r) \\ (A,H)\neq 1}} d_k(A)$$

o equivalentemente :

$$\sum_{A\in\mathbb{M}(r)} d_k(A) - \sum_{A\in\mathbb{M}(r)} d_k(A)\chi_0(A) = \sum_{\substack{A\in\mathbb{M}(r) \\ (A,H)\neq 1}} d_k(A)$$

si $r\geq\partial(H)$ existen exactamente $q^r\left[1-\phi(H)/|H|\right]$ polinomios A de grado r en $\mathbb{M}$ tales que $(A,H)\neq 1$ y utilizando el lema 2.1 en su parte (a), obtenemos :

$$\sum_{\substack{A\in\mathbb{M}(r) \\ (A,H)\neq 1}} d_k(A) = O(q^{r(k\varepsilon+1)}) \qquad (r\longrightarrow\infty)$$

y así :

$$\sum_{A\in\mathbb{M}(r)} d_k(A)\chi_0(A) = \left[\begin{matrix} r+k-1 \\ k-1 \end{matrix}\right] q^r + O(q^{r(k\varepsilon+1)})$$

usando un resultado debido aCarlitz [4].Finalmente,porel corolario del teorema 2.1 y dado que :

$$\sum_{A\in\mathbb{M}(r)} \chi(A)d_k(A) = O(q^{r(k\varepsilon+1)}), \text{ si } \chi \neq \chi_0$$

obtenemos :

$$\sum_{A\in\mathbb{E}(r)} d_k(A) = (1/\phi(H))\begin{bmatrix} r+k-1 \\ k-1 \end{bmatrix} q^r + O(q^{r(k\varepsilon+1)})$$

Teorema 3.2 . Para todo $\varepsilon > 0$ y cada clase $\mathbb{E}$ invertible módulo $\mathcal{R}_H$, tenemos :

$$\sum_{A\in\mathbb{E}(r)} \phi(A) = q^{2r}/\zeta(2)\phi(H) + O(q^{r(2+\varepsilon)}) \qquad (r\longrightarrow\infty)$$

Demostración . Con un argumento similar al empleado en el teorema anterior, tenemos :

$$\sum_{\substack{A\in\mathbb{M}(r) \\ (A,H)\neq 1}} \phi(A) \leq q^r\left[1-\phi(H)/|H|\right]C_2 q^{r(1+\varepsilon)}$$

por lo tanto :

$$\sum_{\substack{A\in\mathbb{M}(r) \\ (A,H)\neq 1}} \phi(A) = O(q^{r(2+\varepsilon)})$$

Por otro lado , Carlitz [4] ha demostrado que :

$$\sum_{\partial(A)=r} \phi(A) = \begin{cases} 1 \text{ si } r=0 \\ q^{2r-1}(q-1) \end{cases}$$

y de aquí obtenemos lo que se afirma en el teorema.

Teorema 3.3 . Para todo $\varepsilon > 0$ y cada clase $\mathbb{E}$ invertible módulo $\mathcal{R}_H$ se tiene :

$$\sum_{A\in\mathbb{E}(r)} \sigma_t(A) = 1/\phi(H)\left[\, q^r(q^{t(r+1)})/(q^{t-1}) \,\right] + O(q^{r(t+\varepsilon+1)}),$$

$(r\longrightarrow\infty)$.

Demostración . Por argumento similar a los anteriores vemos que :

$$\sum_{\substack{A\in\mathbb{M}(r)\\(A,H)\neq 1}} \sigma_t(A) \leq q^r\left[1-\phi(H)/|H|\right]C_4 q^{r(t+\varepsilon)} = C_5 q^{r(t+\varepsilon+1)}$$

por lo tanto :

$$\sum_{\substack{A\in\mathbb{M}(r)\\(A,H)\neq 1}} \sigma_t(A) = O(q^{r(t+\varepsilon+1)})$$

Por otro lado, Carlitz ha demostrado que :

$$\sum_{A\in\mathbb{M}(r)} \sigma_t(A) = q^r(q^{t(r+1)}-1)/(q^t-1),$$

de donde se infiere, inmediatamente, el resultado.

Teorema 3.4 . Para todo $\varepsilon > 0$ y cada clase $\mathbb{E}$ invertible módulo $\mathcal{R}_H$ se tiene :

$$\sum_{A\in\mathbb{E}(r)} \lambda(A) = (-1)^r q^{[(r+1)/2]}/\phi(H) + O(q^{r(\varepsilon+1)}) \quad (r\longrightarrow\infty)$$

Demostración . Sabemos que :

$$\sum_{\substack{A\in\mathbb{M}(r)\\(A,H)\neq 1}} \lambda(A) \leq q^r\left[1-\phi(H)/|H|\right]q^{r\varepsilon} = C_6 q^{r(\varepsilon+1)}$$

Por lo tanto :

$$\sum_{\substack{A\in\mathbb{M}(r)\\(A,H)\neq 1}} \lambda(A) = O(q^{r(\varepsilon+1)})$$

Además, según Carlitz [4]:

$$\sum_{A \in \mathbb{M}(r)} \lambda(A) = (-1)^r q^{[(r+1)/2]}$$

donde [ ] indica la función parte entera.

Luego utilizando, una vez más, el corolario de la proposición 2.4 obtenemos :

$$\sum_{A \in \mathbb{E}(r)} \lambda(A) = (-1)^r q^{[(r+1)/2]} + O(q^{r(\ell+1)}) \quad (r \longrightarrow \infty)$$

CONCLUSIONES

La "sencillez estructural" del anillo $\mathbb{F}_q[X]$, a la cual hice referencia en la introducción hizo posible establecer las fórmulas asintóticas que aquí presentamos. Talvez, muchas de estas fórmulas pueden ser mejoradas. Pero lo importante a señalar es el hecho que fueron establecidas descansando en los aspectos aritméticos y evitando en lo posible el uso de herramientas analíticas.

Podemos entonces concebir una teoría, en $\mathbb{F}_q[X]$, análoga ala Teoría de Números que, por lo visto en este trabajo, podría servir como una excelente orientación a quien se inicie en el estudio de la Teoría Analítica de Números, pues resultaría menos exigente tanto en experencias como en requisitos.

Un aspecto especial que deseamos destacar es que el establecimiento de las fórmulas asintóticas puede ser tratado en situaciones más generales, pues basta que la relacion de congruencia sea una relación aritméticamente distribuida. Los otros factores que intervienen son independientes de la relación de congruencia, por lo tanto al considerar otras relaciones se enriquece de manera sustancial la teoría que proponemos.

APÊNDICE

Teorema 1. En un semigrupo aritmético G se verifica :

(a) $d_k = u * u * \ldots * u$ (k-veces) $k \geq 1$

(b) $d^2 * h_2 = d_4$

(c) $\sigma_t = u * |\ |^t$

(d) $\hat{d} * h_2 = d_2$

(e) $J_t * u = |\ |^t$

(f) $\beta * h_0 = u * h_2 * h_3$

donde $h_k(a) = \begin{cases} 1 \text{ si } b^k = a, \text{ para algún } b \in G \\ 0 \text{ en otro caso.} \end{cases}$

y $\hat{d}(a) = 2^{\omega(a)}$

Demostración . Todas las funciones que aparecen en el teorema son multiplicativas, por lo tanto para probar (a)-(f) basta verificar la igualdades para los elementos de G que son potencias de los elementos primos.

Es claro que, si $p \in \mathbb{P}$ y $\alpha \geq 1$ se tiene :

$$d_k(p^\alpha) = \binom{\alpha+k-1}{k-1}.$$

Demostremos (a). Es inmediato que $d_2 = u * u$. Si suponemos que $d_k = u * \ldots * u$, k-veces, resulta que :

$$\begin{aligned} d_{k+1}(p^\alpha) &= \binom{\alpha+k}{k} \\ &= \sum_{\iota=0}^{\alpha} \binom{k+\iota-1}{k-1} \\ &= \sum_{\iota=0}^{\alpha} d_k(p^\iota) = (d * u)(p^\alpha) \\ &= (\underbrace{u * u \ldots * u}_{k+1 \text{ veces}})(p^\alpha) \end{aligned}$$

Luego, hemos probado afirmado en (a).

Para demostrar (b) comencemos por calcular $d^2 * h_2(p^\alpha)$

$$(d^2 * h_2)(p^\alpha) = \sum_{\iota=0}^{\alpha} h_2(p^\iota) d^2(p^{\alpha-\iota})$$

$$= (1/2)\left[\sum_{\iota=0}^{\alpha} \iota + \sum_{\iota=0}^{\alpha} \iota^2 \right]$$

$$= (\alpha+1)(\alpha+2)(\alpha+3)/6$$

$$= d_4(p^\alpha)$$

Esto prueba que $d^2 * h_2 = d_4$

(c) y (e) son inmediatas por las definiciones de σ_ι y J_ι respectivamente.

Veamos (d) :

$$(h_2 * \hat{d})(p^\alpha) = \sum_{\iota=0}^{\alpha} h_2(p^\iota)\hat{d}(p^{\alpha-\iota})$$

$$= \sum_{\iota=0}^{\alpha-1} [(-1)^\iota + 1] + [(-1)^\alpha + 1]/2$$

$$= \alpha+1 = d_2(p^\alpha).$$

Hemos probado con esta igualdad que $h_2 * \hat{d} = d_2$

De manera análoga se logra probar (f).

El teorema anterior y el siguiente tienen como corolario inmediato el teorema 5.1 del capítulo 1.

Teorema 2 Sean G un semigrupo aritmético aditivo y f, g, h $\in$ Dir(G). Si f es completamente multiplicativa entonces :

(a) $f(g * h) = fg * fh$

(b) $g(z,f)h(z,f) = (g * h)(z,f)$

Demostración . Sea $a \in G$ y evalúemos $(fg * fh)(a)$

$$(fg * fh)(a) = \sum_{d|a} (fg)(d)(fh)(a/d)$$

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

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

$$= f(g * h)$$

Esto prueba (a).

La prueba de (b) se basa en (a) y en el hecho fundamental que la aplicación $f \longrightarrow f(z) = \sum_{a\in G} f(a)|a|^{-z}$ de $Dir(G)$ en $\{ \sum_{a\in G} f(a)|a|^{-z} \ / \ f\in Dir(G)\}$ es un isomorfismo de álgebras, ver [3]. En efecto

$$(g * h)(z,f) = \sum_{a\in G} ((g * h)f)(a)|a|^{-z}$$

$$= \sum_{a\in G} (gf * hf)(a)|a|^{-z}$$

$$= \sum_{a\in G}(gf)(a)|a|^{-z} \times \sum_{a\in G} (hf)(a)|a|^{-z}$$

$$= g(z,f)h(z,f)$$

El teorema a continuación, conjuntamente con el teorema 1, se emplea para demostrar las afirmaciones,hechas en §3 del capítulo 2, referentes a expresiones del tipo $\sum_{A\in\mathbb{M}(r)} f(A)$, donde $f \in Dir(\mathbb{M})$.

Teorema 3. Si $q \geq 2$ es un número real y $F(\sigma)=\sum_{k}^{\infty} c_k q^{-k} \longrightarrow 0$ absolutamente para $\sigma > \sigma_0$, donde σ, $c_k \in \mathbb{R}$, entonces $c_k = 0$ para $k=0, 1, 2,....$

Demostración . Supongamos que $c_k \neq 0$ para algún k y sea t

el menor índice con esta propiedad, de modo que :

$$0= \sum_{k=0}^{\infty} c_k q^{-k\sigma} = c_t q^{-t\sigma}\left[1+ \sum_{k=t+1}^{\infty} (c_k/c_t) q^{(k-t)\sigma}\right]$$

$$= c_t q^{-t\sigma}\left[1 + G(\sigma) \right]$$

Ahora bien, si $\sigma > \sigma_1 > \sigma$, tenemos para todo $k \geq t+1$ que :

$$q^{(k-t)} = \left[q^{k-t} \right]^{(\sigma-\sigma_1)} \left[q^{k-t} \right]^{(k-t)(\sigma_1)} \geq \left[q \right]^{\sigma-\sigma_1} \left[q^{k-t} \right]^{\sigma_1}$$

Luego :

$$|G(\sigma)| \leq \left| \sum_{k=t+1} (c_k/c_t) \left(q^{(t-k)}\right)^{\sigma} \right| \leq |c_t|^{-1} \left[q \right]^{\sigma_1-\sigma} \sum_{k=t+1}^{\infty} |c_k| \left(q^{(t-k)}\right)^{\sigma_1}$$

Pero elmiembro derecho de esta desigualdad tiende a cero cuando $\sigma \longrightarrow \infty$, pues :

$$\sum_{k=t+1}^{\infty} |c_k| \left(q^{(t-k)}\right)^{\sigma_1} = \sum_{k=t+1}^{\infty} |c_k| \left(q^{-k}\right)^{\sigma_1}$$

converge a una constante independiente de σ. Por consiguiente $| 1 + G(\sigma) | > 1/2$ para σ suficientemente grande, lo que en virtud de (2) obliga que $c_t = 0$, lo cual es contradictorio. Por tanto $c_k = 0$, para todo k.

Corolario. Si $q \geq 2$ es un número real y :

$$\sum_{k=0}^{\infty} c_k q^{-k\sigma} = \sum_{k=0}^{\infty} d_k q^{-k\sigma}$$

absolutamente para $\sigma > \sigma_0$, donde σ, c_k, $d_k \in \mathbb{R}$. entonces $c_k = d_k$, para todo k=0,1, ...

BIBLIOGRAFÍA

[1] ALBIS GONZÁLEZ, Víctor S. On a theorem of Mobius : Elementary variations on the polynomials tonality Rev. Colombiana Mat 21 (1987), 85-94.

[2] APOSTOL, Tom. Introduction to Analytic Number Theory. Springer Verlag (New York) 1976.

[3] BATISTA, Feliciano. Estudio de las funciones aritméticas sobre el monoide de los Polinomios.Universidad de Panamá (Panamá), 1989.

[4] CARLITZ, Leonard. The arithmetic of polynomials in a Galois field. Journal of Mathematics. 54. (1932), 34-69

[5] HAYES, David R. The distributions of irreducibles inGF[q,x]. Transactions American Mathematical Society. 117. (1963), 101-126.

[6] KNOPFMACHER, John. Arithmetical properties of finite rings and algebras, and analytic number theory I. J. reine angew. Math 252. (1972), 74-99.

[7] KNOPFMACHER, John. Arithmetical properties of finite rings and algebras, and analytic number theory II. J. reine angew. Math 254. (1972), 16-43.

[8] KNOPFMACHER, John. Arithmetical properties of finite rings and algebras, and analytic number theory III. J.reine angew. Math 259. (1973), 157-170.

[9] KNPOFMACHER, John. Arithmetical properties of finite rings ans algebras, and analytic number theory IV. J.reine angew. Math 270. (1974), 97-114.

[10] KNOPFMACHER, John. Arithmetical properties of

finite rings and algebras, and analytic number theory V. J.reine angew. Math 271. (1974), 95-121.

[11] VINOGRÁDOV. I. M. Fundamentos de la teoría de los números. Mir (Moscú) 1971.