Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional

Unidad Zacatenco
Departamento de Control Automático

Relaciones entre los valores multizeta y los números de Bernoulli-Carlitz

Tesis que presenta

M.C.M. José Alejandro Lara Rodríguez

para obtener el Grado de

Doctor en Ciencias

en la Especialidad de

Control Automático

Directores de tesis:

Dr. Gabriel Daniel Villa Salvador

Dr. Dinesh Shraddhanand Thakur

México, D.F. Enero, 2013

Agradecimientos

Agradezco a mis directores de tesis, los doctores Gabriel Daniel Villa Salvador y Dinesh S. Thakur por el tiempo y el valioso apoyo que me brindaron durante mis estudios de doctorado. Gracias al comité revisor ya que sus observaciones contribuyeron a mejorar este trabajo.

Un agradecimiento especial a Luis Alfonso Rodríguez Carvajal por sus acertados consejos y por ayudarme a corregir innumerables veces la gramática de mis escritos en Inglés, incluyendo la versión en ese idioma de este documento. Gracias a Javier Díaz Vargas por alentarme a obtener el grado de doctor. A Enrique Acosta Jaramillo y a Verónica Mariño Salazar les agradezco el invaluable apoyo que me brindaron durante mis primeros días en la ciudad de Tucson, Arizona, y también por recibirme año tras año en su hogar, pero más que nada les agradezco por haberme privilegiado con su amistad. Gracias a las familias Camarillo por la calidez con me recibieron en sus hogares.

Gracias a todo el personal del Departamento de Control Automático, particularmente a Martha Rzedowski, Lucero Fernández, Sonia Alfaro y Elizabeth León, y a mis compañeros de doctorado Walter De la Cruz y Víctor Bautista.

Muchas gracias al personal de la Facultad de Matemáticas de la Universidad Autónoma de Yucatán. Agradezco a Gabriel Murrieta Hernández y al Centro de Cómputo del Cuerpo Académico Modelado y Simulación Computacional de Sistemas Físicos (UADY-CA-101) por permitirme el uso de su servidor para realizar mis experimentos computacionales.

Gracias al Departamento de Matemáticas de la Universidad de Arizona y a su personal, por los recursos académicos y computacionales puestos a mi disposición así como por las facilidades brindadas durante mis visitas.

Gracias a la Universidad Autónoma de Yucatán (Uady), al Consejo Nacional de Ciencia y Tecnología (Conacyt) y al Programa de Mejoramiento del Profesorado (Promep) por su apoyo financiero.

Principalmente le doy gracias a mi familia por su amor y su apoyo, en particular a Glendy, Graciela, Jesús y Abraham a quienes les pido perdon por haberlos dejado tanto tiempo solos.

Gracias a Dios por permitirme vivir esta maravillosa experiencia.

Resumen

D. Thakur introduce y estudia los valores multizeta asociados a un campo de funciones algebraicas de una variable con campo de constantes $\mathbb{F}_q$, donde q es una potencia de un primo p, cuyo lugar al infinito es racional, y prueba la existencia de relaciones entre los valores multizeta ([Tha04, Sección 5.10], [Tha09b], [Tha10]). En particular, Thakur prueba que el producto $\zeta(a)\zeta(b)$ es una combinación lineal de valores multizeta, sin dar una descripción explícita. Para el caso $q = 2$, Thakur formula una conjetura recursiva de cómo expresar el producto de valores zeta como una suma de valores multizeta. Aquí probaremos parte de esa conjetura y también probaremos una generalización de esta conjetura debida al autor de esta tesis. Para q general, se probarán fórmulas explícitas y también una fórmula recursiva para expresar $\zeta(a)\zeta(b)$ como una suma de valores multizeta. Demostraremos varias de las conjeturas formuladas en [Lar10, Tha09b] para valores pequeños de a o para familias de valores especiales de a acerca de cómo escribir $\zeta(a)\zeta(b)$ como una combinación lineal de valores multizeta. También probaremos la conjetura acerca de la paridad formulada en [Tha09b].

Cuando el grado del lugar al infinito es mayor que 1, generalizaremos la definición del valor multizeta y daremos evidencia de que, a diferencia del caso racional, el producto de valores zeta no siempre se puede escribir como una combinación de valores multizeta. También probaremos que para ciertas familias de valores de a y b, $\zeta(a)\zeta(b)$ se puede escribir como una combinación de valores multizeta.

Por otro lado, en 1935, L. Carlitz introdujo los análogos a los números de Bernoulli [Car35, Car37]. Actualmente, estos números son llamados números de Bernoulli-Carlitz. Carlitz probó un teorema análogo al Teorema de von Staudt-Clausen, con un enunciado mucho más sutil que en el caso clásico, que describe completamente los denominadores de estos números. Thakur consideró como un análogo a $\mathcal{B}_m/m$, el cual es un importante asociado del número de Bernoulli $\mathcal{B}_m$, al número $B_m(m-1)!_C/m!_C$, donde $m!_C$ es el factorial de Carlitz, y describió completamente su denominador, excepto cuando $q = 2$ y m es de cierta forma. Aquí completaremos esta descripción. También mostraremos que un grupo de simetrías recientemente descubierto por D. Goss [Gos11] puede ser realizado como simetrías de nuestros resultados.

Abstract

D. Thakur introduces and studies the multizeta values for function fields with constant field $\mathbb{F}_q$ (for a general A, with a rational place at infinity) and proves the existence of relations between them ([Tha04, Sección 5.10], [Tha09b], [Tha10]). In particular, he proves that the product $\zeta(a)\zeta(b)$ is a linear combination of multizeta values. For $q = 2$, a full conjectural description of how the product of two zeta values can be described as the sum of multizeta was given by Thakur. Here, we shall prove part of the latter conjecture and also we shall prove a generalization of this conjecture made by the author of this thesis. Moreover, for general q, we shall prove closed formulas as well as a recursive recipe to express $\zeta(a)\zeta(b)$ as a sum of multizeta values. Several of the conjectures formulated in [Lar10, Tha09b] for small values or for special families of a about how to write $\zeta(a)\zeta(b)$ as an $\mathbb{F}_p$-linear combination of multizeta values, will be proved. Also, we shall prove the parity conjecture formulated in [Tha09b].

When the place at infinity is not rational, we generalize the multizeta value definition and provide evidence that, in contrast with the rational case, the product of zeta values is not always a sum of multizeta. Also, we shall prove that for special families of a and b, $\zeta(a)\zeta(b)$ can be expressed as a sum of multizeta values.

On the other hand, in 1935, L. Carlitz introduced analogues of Bernoulli numbers for $\mathbb{F}_q[t]$ [Car35, Car37]. These are now called Bernoulli-Carlitz numbers B_m. He proved a von Staudt-Clausen type theorem, with a much more subtle statement than the classical one, describing their denominators completely. As an analog of the important relative $\mathcal{B}_m/m$ of the usual Bernoulli number $\mathcal{B}_m$, Thakur considered an analog $B_m(m-1)!_C/m!_C$, where $m!_C$ is the Carlitz factorial. He described their denominator fully, except when $q = 2$ and m has a particular form. In this work we shall completely describe the latter. Also, we shall see that a group of symmetries recently discovered by D. Goss [Gos11] may be realized as symmetries of our results.

Notación

$\mathbb{Z}$	Anillo de enteros
$\mathbb{Z}_+$	enteros positivos
$\mathbb{Z}_{\geq 0}$	enteros no negativos
$\mathbb{Q}$	el campo de los números racionales
$\mathbb{C}$	el campo de los números complejos
R^*	el grupo multiplicativo de las unidades del anillo R
q	potencia de un número primo p, $q = p^s$ con $s \in \mathbb{Z}_+$, 6
$\mathbb{F}_q$	un campo finito con q elementos, 6
t	una variable independiente, 6
$\mathbb{F}_q[t]$	el anillo de los polinomios en la variable t con coefficientes en $\mathbb{F}_q$, 6
$\mathbb{F}_q(t)$	el campo de la funciones racionales en la variable t con coeficientes en $\mathbb{F}_q$, 6
K	un campo de funciones en una variable con campo de constantes $\mathbb{F}_q$, 6
∞	un lugar de K de grado uno, 24
v_∞	valuación con respecto al lugar ∞, 79
K_∞	$\mathbb{F}_q((1/t))$, la completación de K con respecto a ∞, 8
$\mathbb{C}_\infty$	la completación de alguna cerradura algebraica de K_∞, 8
A	el anillo de los elementos de K que no tienen polos excepto posiblemente en ∞, 24
deg	función que asigna a cada $x \in K_\infty^*$ su grado, 79
A_+	elementos mónicos en A, 6, 78
A_d	elementos de A de grado d
$A_{<d}$	elementos de A de grado menor que d
A_{d+}	$A_d \cap A_+$, 8
$A_{<d+}$	$A_{<d} \cap A_+$, 82
$[n]$	$t^{q^n} - t$, 19
D_n	$[n][n-1]^q \cdots [1]^{q^{n-1}} = \prod_{i=0}^{n-1}(t^{q^n} - t^{q^i})$, 19
L_n	$[n][n-1] \cdots [1] = \prod_{i=1}^{n}(t^{q^i} - t)$, 19
ℓ_n	$(-1)^n L_n$, 19
"par"	múltiplo de $q-1$, 7

$S_d(k)$	$\sum_{a \in A_{d+}} a^{-k}$, 8
$S_{<d}(k)$	$\sum_{a \in A_{<d+}} a^{-k}$, 20, 79
$\binom{x}{q^d}_C$	$\sum_{i=0}^{d} \frac{x^{q^i}}{D_i \ell_{d-i}^{q^i}}$, 20
$\mathrm{Int}\,(x)$	$= \begin{cases} 0 & \text{si } x \text{ no es entero} \\ 1 & \text{si } x \text{ es entero.} \end{cases}$, 15
$\ell(k)$	suma de los dígitos de la descomposición en base q de k, 43
$\lfloor x \rfloor$	máximo número entero no superior a x, 10
$\lceil x \rceil$	mínimo número entero no inferior a x, 11

Índice general

CAPÍTULO 1

Introducción

1.1. Funciones zeta y multizeta en característica cero

En esta sección se introducen la función zeta de una variable y su generalización a r variables, denominada función multizeta, y se muestran las relaciones algebraicas que existen entre los valores $\zeta(s_1, \dots, s_r)$ de estas funciones. Los valores de las funciones zeta cuando $r = 1, 2$, fueron estudiados originalmente por L. Euler [Eul75]. A manera de ejemplo de estas relaciones algebraicas, mencionamos la relación $\zeta(3) = \zeta(2, 1)$ descubierta por L. Euler. En [Zag94], D. Zagier define y estudia la función multizeta para cualquier número de variables.

1.1.1. Funciones zeta y multizeta clásicas

Sea s un número complejo. La serie de Dirichlet $\sum_{n=1}^{\infty} n^{-s}$ converge si $\mathrm{Re}(s) > 1$ y diverge en cualquier otro caso. Así, esta serie define una función analítica en la región $\mathrm{Re}(s) > 1$. La *función zeta de Riemann* es la continuación analítica de esta serie de Dirichlet a todo el plano complejo menos el punto $s = 1$. En particular, para $\mathrm{Re}(s) > 1$, la función zeta de Riemann está definida por

$$\zeta(s) = \zeta_{\mathbb{Z}}(s) = \sum_{n=1}^{\infty} n^{-s}.$$

Para cualquier $s \in \mathbb{C}$, la función zeta de Riemann satisface la ecuación funcional

$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-(1-s)/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s).$$

Esta ecuación fue descubierta por L. Euler, estudiando únicamente valores especiales (o particulares) de la función zeta, específicamente, estudiando los valores de ζ en los números enteros, tanto en los positivos como en los negativos. Quizá uno de sus descubrimientos más notables fue la fórmula $\zeta(2) = \pi^2/6$.

Hay toda una teoría de valores especiales asociada con $\zeta_{\mathbb{Z}}(s)$, que se relaciona de manera muy estrecha con los números de Bernoulli, los cuales denotaremos por $\mathcal{B}_n$. Por ejemplo, para $n \geq 0$ se tiene $\zeta_{\mathbb{Z}}(-n) = -\mathcal{B}_{n+1}/(n+1)$. La función generadora para los números de Bernoulli está dada por

$$\frac{x}{e^x - 1} = 1 - \frac{x}{2} + \sum_{n=2}^{\infty} \frac{\mathcal{B}_n}{n!} x^n.$$

Así $\mathcal{B}_1 = -1/2$. Se puede ver $\mathcal{B}_{2n+1} = 0$ para toda $n \geq 1$. Por lo tanto, si $n \geq 1$, $\zeta_{\mathbb{Z}}(-2n) = 0$. Estos ceros son los llamados ceros triviales. Con respecto a los ceros no triviales, se tiene la bien conocida *hipótesis de Riemann*, que dice que todos los ceros no triviales de $\zeta_{\mathbb{Z}}(s)$ yacen sobre la recta $\mathrm{Re}(s) = 1/2$. Éste es un problema que todavía permanece abierto. Para los enteros pares positivos m se tiene el Teorema de Euler

$$\zeta_{\mathbb{Z}}(m) = -\frac{\mathcal{B}_m (2\pi i)^m}{2(m!)}.$$

Hasta la fecha no se conoce una fórmula para $\zeta_{\mathbb{Z}}(2k+1)$ análoga a la anterior. Gracias a R. Apéry [Apé79] se sabe que $\zeta(3)$ es irracional. En general, no se sabe si $\zeta_{\mathbb{Z}}(2k+1)$ es un número racional o irracional. En 2001, K. Ball y T. Rivoal probaron que hay una infinidad de valores irracionales de la función zeta de Riemann en los números impares [BR01]. En 2002, T. Rivoal probó que al menos uno de los nueve números $\zeta(5), \zeta(7), \ldots, \zeta(21)$ es irracional [Riv02].

La fórmula de Euler para expresar la función zeta como un producto infinito muestra explícitamente la conexión entre los números primos y la función zeta de Riemann. Para $s \in \mathbb{C}$ y $\mathrm{Re}(s) > 1$, se tiene

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1},$$

donde el producto infinito se toma sobre todos los números primos. Esta fórmula, debida a L. Euler, aparece por primera vez en el libro de Euler publicado en 1748 y que lleva por título *Introductio in Analysin Infinitorum*. Esta fórmula muestra como la función zeta codifica información relativa a los números enteros y la distribución de los números primos.

En 1775, más de 30 años después de que Euler introdujera los valores zeta, mientras trataba de evaluar $\zeta(3)$, él mismo introduce las *zetas dobles* o *multizetas* [Eul75]:

$$\zeta(s_1, s_2) = \sum_{n_1 > n_2 > 0} \frac{1}{n_1^{s_1} n_2^{s_2}} \qquad (s_1, s_2 \in \mathbb{Z}, s_1 > 1, s_2 > 0).$$

La condición $s_1 > 1$ es necesaria para garantizar la convergencia de la serie. Euler estudió por muchos años esta nueva serie y descubrió algunas identidades, tales como $\zeta(3) = \zeta(2,1)$ y

$$\zeta(s,1) + \zeta(s-1,2) + \cdots + \zeta(2,s-1) = \zeta(s+1).$$

Para enteros positivos s_i ($i = 1, 2, \ldots, r$) con $s_1 > 1$, los *valores multizeta* están definidos por

$$\zeta(s_1, \ldots, s_r) = \sum_{n_1 > n_2 > \cdots > n_r > 0} \frac{1}{n_1^{s_1} \cdots n_r^{s_r}}.$$

A los enteros r y $\sum s_i$ se les llama *profundidad* y *peso*, respectivamente, del valor multizeta.

Para $s_1, \ldots, s_r \in \mathbb{C}$, *la función multizeta* o *función zeta múltiple*

$$\zeta(s_1, \ldots, s_r) = \sum_{n_1 > n_2 > \cdots > n_r > 0} \frac{1}{n_1^{s_1} \cdots n_k^{s_r}}$$

es absolutamente convergente en la región

$$\left\{ (s_1, \ldots, s_r) \mid \mathrm{Re}(s_1) > 1, \sum_{i=1}^{r} \mathrm{Re}(s_i) > r \right\}.$$

Abusando de la notación, estamos usando $\zeta(s_1, \ldots, s_r)$ para denotar tanto al valor multizeta como a la función multizeta.

Claramente esta función generaliza a los valores multizeta. El problema de la continuación analítica de esta función la estudian J. Zhao [Zha00], S. Akiyama, S. Egami e Y. Tanigawa [AET01].

Recordemos ahora que el producto de Cauchy de dos series convergentes converge si al menos una de las dos series converge absolutamente. Dado que la serie que define a la función zeta de Riemann es absolutamente convergente para $\mathrm{Re}(s) > 1$, el producto $\zeta(a)\zeta(b)$ es una serie convergente y de hecho absolutamente convergente. Por lo tanto, cualquier reordenamiento del producto de las series converge y de hecho converge al producto de las series. De acuerdo con la definición de producto de Cauchy para series y dado que para cualesquiera dos enteros n_1, n_2 se tiene $n_1 = n_2$, $n_1 < n_2$ o $n_2 < n_1$, se sigue que

$$\begin{aligned}
\zeta(a)\zeta(b) &= \lim_{M \to \infty} \sum_{N=2}^{M} \sum_{n_1 + n_2 = N} \frac{1}{n_1^a n_2^b} \\
&= \lim_{M \to \infty} \left(\sum_{\substack{n_1 = n_2 \\ n_1 + n_2 \leq M/2}} \frac{1}{n_1^{a+b}} + \sum_{\substack{n_1 < n_2 \\ n_1 + n_2 \leq M}} \frac{1}{n_1^a n_2^b} + \sum_{\substack{n_1 > n_2 \\ n_1 + n_2 \leq M}} \frac{1}{n_1^a n_2^b} \right) \\
&= \sum_{n=1}^{\infty} \frac{1}{n^{a+b}} + \sum_{n_2 > n_1 > 0} \frac{1}{n_1^a n_2^b} + \sum_{n_1 > n_2 > 0} \frac{1}{n_1^a n_2^b}.
\end{aligned}$$

Por lo tanto,

$$\zeta(a)\zeta(b) = \zeta(a+b) + \zeta(b,a) + \zeta(a,b). \tag{1.1.0.1}$$

De manera esquemática tenemos que el producto

$$\zeta(a)\zeta(b) = \left(\frac{1}{1^a} + \frac{1}{2^a} + \frac{1}{3^a} + \cdots\right)\left(\frac{1}{1^b} + \frac{1}{2^b} + \frac{1}{3^b} + \cdots\right),$$

da por resultado

$$\begin{array}{l}
\frac{1}{1^a1^b} + \frac{1}{1^a2^b} + \frac{1}{1^a3^b} + \frac{1}{1^a4^b} + \frac{1}{1^a5^b} + \cdots \\
\frac{1}{2^a1^b} + \frac{1}{2^a2^b} + \frac{1}{2^a3^b} + \frac{1}{2^a4^b} + \frac{1}{2^a5^b} + \cdots \\
\frac{1}{3^a1^b} + \frac{1}{3^a2^b} + \frac{1}{3^a3^b} + \frac{1}{3^a4^b} + \frac{1}{3^a5^b} + \cdots \\
\frac{1}{4^a1^b} + \frac{1}{4^a2^b} + \frac{1}{4^a3^b} + \frac{1}{4^a4^b} + \frac{1}{4^a5^b} + \cdots \\
\frac{1}{5^a1^b} + \frac{1}{5^a2^b} + \frac{1}{5^a3^b} + \frac{1}{5^a4^b} + \frac{1}{5^a5^b} + \cdots \\
\cdots
\end{array}$$

La suma de los elementos en la diagonal, es decir, los sumandos de la forma $1/n^an^b$ da por resultado $\zeta(a+b)$; los suma de todos los elementos que están por arriba de la diagonal, es decir, la suma de los elementos de la forma $1/n_1^an_2^b$ con $n_1 < n_2$, da por resultado $\zeta(b,a)$. Finalmente, la suma de todos los elementos que están por debajo de la diagonal da $\zeta(a,b)$.

Sean n_1, n_2 enteros tales que $n_1 > n_2$. Dado otro entero n, se dan cinco posibilidades: $n > n_1 > n_2$, $n = n_1 > n_2$, $n_1 > n > n_2$, $n_1 > n = n_2$ y $n_1 > n_2 > n$. Por lo tanto,

$$\begin{aligned}
\zeta(a)\zeta(b,c) &= \sum_{n=1}^{\infty} \frac{1}{n^a} \sum_{n_1>n_2>0} \frac{1}{n_1^bn_2^c} \\
&= \sum_{n>n_1>n_2} \frac{1}{n^an_1^bn_2^c} + \sum_{n=n_1>n_2>0} \frac{1}{n_1^{a+b}n_2^c} + \sum_{n_1>n>n_2>0} \frac{1}{n_1^bn^an_2^c} \\
&\quad + \sum_{n_1>n=n_2>0} \frac{1}{n_1^bn_2^{a+c}} + \sum_{n_1>n_2>n>0} \frac{1}{n_1^bn_2^cn^a}.
\end{aligned}$$

De esta manera llegamos a

$$\zeta(a)\zeta(b,c) = \zeta(a,b,c) + \zeta(a+b,c) + \zeta(b,a,c) + \zeta(b,a+c) + \zeta(b,c,a). \tag{1.1.0.2}$$

Nos referiremos a las sumas del tipo (1.1.0.1) o (1.1.0.2) como *sumas barajeadas clásicas*.

En general, el producto de dos valores multizeta es una $\mathbb{Z}$-combinación lineal de valores multizeta. Luego el $\mathbb{Q}$-espacio lineal generado por todos los valores multizeta es una $\mathbb{Z}$-álgebra.

El estudio de los valores multizeta ha resurgido con renovado interés por sus profundas conexiones con otras partes de las matemáticas. Por ejemplo, aparecen en el trabajo de Deligne y Goncharov sobre motivos mixtos de Tate en Spec $\mathbb{Z}$, y en el programa Grothendieck-Ihara para estudiar el grupo de Galois absoluto de $\mathbb{Q}$ a través del grupo fundamental de la recta proyectiva menos tres puntos. También aparecen como coeficientes del asociador de Drinfeld. Además, éstos tienen ciertas conexiones con topología [LM95] y física [BK97]. Las relaciones algebraicas entre los valores multizeta se han estudiado ampliamente por J. Borwein y D. Zagier entre otros ([BBBL98], [Zag93], [Zag94]). El estudio sistemático de los valores multizeta está en sus etapas iniciales.

1.1.2. La función zeta de Dedekind

La función zeta de Dedekind es una generalización de la función zeta de Riemann. Sea K un campo de números (i.e., una extensión finita del campo de los números racionales) y sea $\mathcal{O}_K$ su anillo enteros. La *función zeta de Dedekind* del campo de números K se define para $s \in \mathbb{C}$ con $\mathrm{Re}(s) > 1$, como sigue

$$\zeta_{\mathcal{O}_K}(s) := \sum_{I} \frac{1}{\mathrm{N}\,(I)^s}$$

donde la suma se toma sobre todos los ideales no nulos del anillo de enteros $\mathcal{O}_K$ de K, y $\mathrm{N}\,(I) = |\mathcal{O}_K/I|$ es la norma del ideal I. Observamos que si $K = \mathbb{Q}$, entonces $\zeta_{\mathcal{O}_K} = \zeta_{\mathbb{Z}}$ ya que $\mathrm{N}\,(n\mathbb{Z}) = |\mathbb{Z}/n\mathbb{Z}| = n$. Esta función tiene una continuación analítica a todo el plano complejo con exactamente un polo en $s = 1$ dado por una ecuación funcional sencilla que conecta $\zeta_{\mathcal{O}_K}(s)$ con $\zeta_{\mathcal{O}_K}(1-s)$. También existe un producto de Euler para esta función análogo al producto de Euler para $\zeta_{\mathbb{Z}}$.

En [Mas05], R. Masri, introduce algunos tipos especiales de funciones zeta de Dedekind múltiples que generalizan a la función zeta de Dedekind y a las sumas múltiples de Euler-Zagier, y establece la continuación meromorfa de estas funciones en algunos casos especiales.

1.2. Las funciones zeta y multizeta en campos de funciones

En la Teoría de Números es usual considerar las analogías entre los campos de números y los campos de funciones algebraicas. Hay varias analogías muy interesantes entre los campos de funciones sobre campos finitos y los campos de números [Gos79, Tha04, Vil06, Ros02]. Estas analogías se han usado para conjeturar y probar resultados de un contexto al otro.

Recordemos que si $\mathbb{F}$ es un campo finito, entonces la cardinalidad q de $\mathbb{F}$ es una potencia de algún número primo p. Usaremos la notación $\mathbb{F}_q$ para denotar a un campo finito con q elementos. En este trabajo la letra q está reservada para denotar la cardinalidad de algún campo finito. Por lo tanto q siempre hará referencia a la potencia de algún número primo p.

En este trabajo, un campo de funciones K significa un campo de funciones algebraicas de una variable sobre un campo finito, o más precisamente, una extensión finita de algún $\mathbb{F}_q(t)$, donde $\mathbb{F}_q(t)$ denota el campo de las funciones racionales en la variable t con coeficientes en $\mathbb{F}_q$.

A un campo de funciones podemos asociarle una función zeta. En este capítulo veremos dos maneras de hacer esto. La función zeta de Artin-Weil asocia a un campo de funciones valores zeta complejos. El análogo a la hipótesis de Riemann para este caso fue probado por H. Hasse [Has33, 1933] y A. Weil [Wei40, Wei41, 1940, 1941].

En 1935, L. Carlitz [Car35] define unos valores zeta que resultan ser un buen análogo a los valores zeta clásicos. El análogo a la hipótesis de Riemann fue probado por D. Wan [Wan96, 1996], J. Díaz-Vargas [DV96, 1996] y J. T. Sheats [She98, 1998]. En 2004, D. Thakur [Tha04, Sección 5.10] introduce dos tipos de funciones multizeta para campos de funciones, una que tiene valores complejos (y generaliza la función zeta de Artin-Weil), y otra que generaliza los valores de la función zeta de Carlitz. Estos últimos son el objeto de nuestro estudio.

1.2.1. La función zeta de Artin-Weil; una función multizeta

A continuación describiremos la función zeta de Artin-Weil. Sea K un campo de funciones con campo de constantes $\mathbb{F}_q$. Sea $\mathcal{D}$ un divisor de K y $|\mathcal{D}| = q^{\deg \mathcal{D}}$ la norma del divisor $\mathcal{D}$. La *función zeta de Artin-Weil* está definida por

$$\zeta_K(s) = \sum_{\mathcal{D}} \frac{1}{|\mathcal{D}|^s} \in \mathbb{C}, \quad (s \in \mathbb{C}, \operatorname{Re}(s) > 1).$$

donde la suma es sobre todos los divisores enteros (positivos o efectivos) $\mathcal{D}$. Esta función es absolutamente convergente en la región en la que está definida. Haciendo $K = \mathbb{F}_q(t)$ obtenemos $\zeta(s) = \sum \mathrm{N}\,(I)^{-s}$, donde la suma se toma sobre todos los ideales I distintos de cero. La función de Artin-Weil tiene un producto de Euler, una ecuación funcional, y una teoría de valores especiales; la hipótesis de Riemann en este caso se conoce como el Teorema de Weil. Esta función resulta ser una función racional de q^{-s}. Así, por ejemplo, no puede haber un análogo al Teorema de Euler que relacione $\zeta(2k)$ con $(2\pi i)^{2k}$.

Thakur generaliza la función de Artin-Weil cuando A es el anillo de los polinomios $\mathbb{F}_q[t]$ y $K = \mathbb{F}_q(t)$ como sigue. Sea A_+ el conjunto de los polinomios mónicos en A. Entonces

$$\zeta(s_1,\ldots,s_k)=\sum_{\substack{n_i\in A_+\\ |n_1|>\cdots>|n_k|}}\frac{1}{|n_1|^{s_1}\cdots|n_k|^{s_k}},$$

donde $|n|=q^{\deg n}$. Esta serie tiene una expresión simple en términos de q y de $s_1,\ldots,s_k$. Por cada $d\in\mathbb{Z}_{\geq 0}$, existen q^d polinomios mónicos de grado q^d. Por cada polinomio mónico n_1 de grado d_1, existen $\sum_{i=1}^{d_1} q^{d_1-i}=(q^{d_1}-1)/(q-1)$ polinomios mónicos n_2 que satisfacen $|n_1|>|n_2|$. Por lo tanto,

$$\zeta(s_1,s_2)=\sum_{d_1=1}^{\infty}\frac{q^{d_1}}{q^{d_1s_1}}\sum_{d_2=0}^{d_1-1}\frac{q^{d_2}}{q^{d_2s_2}}=\frac{q^{1-s_1}}{(1-q^{1-s_1})(1-q^{2-s_1-s_2})}. \tag{1.2.0.3}$$

Usando la Ecuación (1.2.0.3) y el hecho de que $\zeta(s)=\sum q^d/q^{ds}$, se obtiene

$$\zeta(s_1)\zeta(s_2)=\zeta(s_1,s_2)+\zeta(s_2,s_1)+\zeta(s_1+s_2-1). \tag{1.2.0.4}$$

La Ecuación (1.2.0.4) también se puede obtener a partir de las definiciones de los valores zeta y multizeta junto con argumentos combinatorios.

En [Mas06], R. Masri introduce una función multizeta ζ en varias variables complejas, para un campo de funciones arbitrario con campo de constantes $\mathbb{F}_q$. Su definición generaliza la función zeta de Artin-Weil. Sus principales resultados consisten en probar que esta función multizeta tiene una continuación meromorfa en todo $\mathbb{C}^r$ y que ésta es una función racional de $q^{-s_1},\ldots,q^{-s_k}$.

1.2.2. La función zeta de Carlitz

Un análogo más adecuado para los valores especiales trascendentes de la función zeta de Riemann es la *función zeta de Carlitz* definida por $\zeta_A(s)=\sum_{a\in A_+} a^{-s}$, donde $s\in\mathbb{Z}_+$ y A_+ denota como antes a los polinomios mónicos en $A=\mathbb{F}_q[t]$. Aquí, los polinomios mónicos juegan el papel que juegan los enteros positivos en la función zeta de Riemann. En vez de la norma que sólo depende del grado del polinomio, Carlitz usó todo el polinomio, y por ello pagó el precio de considerar un dominio más pequeño para s, dado que no sabemos cómo elevar un polinomio a una potencia compleja.

Una justificación de por qué éste es un mejor análogo para la zeta de Riemann está en el siguiente teorema [Car35, Car37], [Tha04, Teorema 5.2.1]. Si m es "par" (es decir, un múltiplo de $q-1$) y positivo, entonces

$$\zeta_A(m)=-B_m\widetilde{\pi}^m/(q-1)m!_C,$$

donde $B_m\in K=\mathbb{F}_q(t)$ es un análogo a los números de Bernoulli, $m!_C\in A$ es un análogo al factorial y

$$\widetilde{\pi}=(t-t^q)^{\frac{1}{q-1}}\prod_{n=1}^{\infty}\left(1-\frac{t^{q^n}-t}{t^{q^{n+1}}-t}\right)\in\mathbb{C}_\infty,$$

juega el papel de $2\pi i$ y se sabe que es trascendente sobre K [Wad41] ($\mathbb{C}_\infty$ denota la completación de alguna cerradura algebraica de K_∞). No se conoce una ecuación funcional. Pero, en contraste con el caso clásico, se sabe mucho acerca de la naturaleza de los valores especiales en los enteros positivos. Se tiene el siguiente resultado de G. Anderson, D. Thakur, y J. Yu [AT90, Yu91]: Para m positivo, $\zeta_A(m)$ es trascendente sobre K, y $\zeta_A(m)/\widetilde{\pi}^m$ también es trascendente si m no es "par".

El análogo a la hipótesis de Riemann para este caso está probado ([Wan96, DV96, Gos96, She98, Tha04, BADVVS10]). Cuando A es el anillo de enteros de un campo de funciones K de género mayor que uno, el orden de los ceros en los enteros negativos todavía no está completamente entendido pero se tienen algunos resultados al respecto (véase [Tha04, Gos96, DV06, BADVMB09]). Para los detalles acerca de la continuación analítica debida a D. Goss, la teoría de valores especiales, sus vínculos con la teoría ciclotómica, períodos de los t-motivos, etc, referimos al lector a [Gos96, Tha04].

1.3. Valores multizeta de Thakur

Para $s \in \mathbb{Z}_+$, los *valores zeta de Carlitz* [Gos96, Tha04] se definen como sigue

$$\zeta_A(s) := \sum_{a \in A_+} \frac{1}{a^s} \in K_\infty,$$

donde K_∞ es la completación de K con respecto a ∞. Para $s \in \mathbb{Z}$ y $d \in \mathbb{Z}_{\geq 0}$, escriba

$$S_d(s) := \sum_{a \in A_{d+}} \frac{1}{a^s} \in K,$$

donde A_{d^+} es el conjunto de elementos de A_+ de grado d. Dados enteros $s_i \in \mathbb{Z}_+$ y $d \geq 0$, sea

$$S_d(s_1, \ldots, s_r) = S_d(s_1) \sum_{d > d_2 > \cdots > d_r \geq 0} S_{d_2}(s_2) \cdots S_{d_r}(s_r) \in K.$$

Para $s_i \in \mathbb{Z}_+$, los *valores multizeta de Thakur* [Tha04, Tha09b] están definidos como sigue

$$\zeta(s_1, \ldots, s_r) := \sum_{d_1 > \cdots > d_r \geq 0} S_{d_1}(s_1) \cdots S_{d_r}(s_r) = \sum \frac{1}{a_1^{s_1} \cdots a_r^{s_r}} \in K_\infty,$$

donde la segunda suma es sobre todos los $a_i \in A_+$ de grado d_i tales que $d_1 > \cdots > d_r \geq 0$. Se dice que este valor multizeta o más precisamente que la r-ada es de *profundidad* r y *peso* $\sum s_i$.

Observe que no necesitamos la condición $s_1 > 1$ para la convergencia como en el caso clásico.

Los valores multizeta de Thakur tienen conexiones con el grupo absoluto de Galois via un análogo en campos de funciones a las series de potencias de Ihara. El análogo a las series de potencias de Ihara conecta varios objetos de interés tales como el grupo absoluto de Galois, sumas de Gauss-Jacobi, funciones Gama, elementos zeta especiales, jacobianos de los motivos de Fermat y los solitones de Anderson (trabajo en curso de G. Anderson y D. Thakur [AT]). Los valores multizeta también tienen conexiones con los períodos de los t-motivos mixtos de Carlitz-Tate-Anderson [AT09].

1.4. Relaciones entre los valores multizeta

Recordemos que los valores multizeta de Euler (solamente en este párrafo, la letra griega ζ será usada para denotar a los valores multizeta clásicos) están definidos por la serie $\zeta(s_1, \ldots, s_r) = \sum (n_1^{s_1} \cdots n_r^{s_r})^{-1}$, donde la serie se toma sobre todos los enteros positivos $n_1 > n_2 > \cdots > n_r$, y los s_i's son enteros positivos con $s_1 > 1$ (para garantizar la convergencia). Se tiene la suma barajeada clásica (1.1.0.1):

$$\begin{aligned}\zeta(a)\zeta(b) = \sum_{n_1=1}^{\infty} \frac{1}{n_1^a} \sum_{n_2=1}^{\infty} \frac{1}{n_2^b} &= \sum_{n_1=n_2} \frac{1}{n_1^{a+b}} + \sum_{n_1>n_2} \frac{1}{n_1^a n_2^b} + \sum_{n_2>n_1} \frac{1}{n_2^b n_1^a} \\ &= \zeta(a+b) + \zeta(a,b) + \zeta(b,a).\end{aligned}$$

Ahora bien, en el caso de campos de funciones, esta relación no se cumple porque hay muchos polinomios de un grado dado. En contraste con las sumas barajeadas clásicas, en los campos de funciones las identidades que se obtienen son mucho más complicadas.

Para $s_1, s_2 \in \mathbb{Z}_+$, sea

$$S_d(s_1, s_2) = \sum_{\substack{d=d_1>d_2 \\ a_i \in A_+}} \frac{1}{a_1^{s_1} a_2^{s_2}}$$

donde $d_i = \deg(a_i)$. Para $a, b \in \mathbb{Z}_+$, definamos

$$\Delta_d(a,b) = S_d(a)S_d(b) - S_d(a+b).$$

Escribiremos $\Delta(a,b)$ en vez de $\Delta_1(a,b)$. Note que la definición implica $\Delta_d(a,b) = \Delta_d(b,a)$.

Los siguientes dos teoremas se deben a Thakur [Tha10, Teoremas 1, 2].

Teorema 1.4.1. *Sea $A = \mathbb{F}_q[t]$. Dados $a, b \in \mathbb{Z}_+$, existen $f_i \in \mathbb{F}_p$ y $a_i \in \mathbb{Z}_+$, tal que la siguiente relación es válida para $d = 1$:*

$$\Delta_d(a,b) = \sum f_i S_d(a_i, a+b-a_i) \tag{1.4.1.1}$$

$\square$

Teorema 1.4.2. *Sea q una potencia de p. Si* (1.4.1.1) *es válido para algunos $f_i \in \mathbb{F}_p$ y algunos $a_i \in \mathbb{Z}_+$ cuando $d = 1$ y $A = \mathbb{F}_q[t]$, entonces* (1.4.1.1) *es válida, con las mismas a_i y f_i, para toda $d \geq 0$ y para toda A (correspondiente a la q dada). En este caso, se tiene la relación*

$$\zeta(a)\zeta(b) - \zeta(a+b) - \zeta(a,b) - \zeta(b,a) = \sum f_i \zeta(a_i, a+b-a_i). \qquad \square$$

Observación 1.4.3. De acuerdo con los Teoremas 1.4.1 y 1.4.2, es posible expresar $\Delta_d(a,b)$ como una combinación de S_d's:

$$\Delta_d(a,b) = \sum f_i S_d(a_i, a+b-a_i), \tag{1.4.3.1}$$

donde $f_i \in \mathbb{F}_p$ y los a_i son enteros positivos distintos.

Estamos interesados en desarrollar métodos efectivos o fórmulas explícitas para encontrar los pares (f_i, a_i) correspondientes a la terna (q, a, b).

Definición 1.4.4. Sean $a, b \in \mathbb{Z}_+$. Denotaremos por $S(q,a,b)$ o por $S(a,b)$ al conjunto de los pares (f_i, a_i) tales que (1.4.1.1) es válida cuando $d = 1$. Denotaremos con $s(a,b)$ la cardinalidad de $S(a,b)$. Usaremos la notación $S^\theta(a,b)$ para denotar el conjunto de los pares $(f_i, a_i) \in S(a,b)$ tales que $f_i = \theta$.

Definición 1.4.5. Sea $a \in \mathbb{Z}_+$.

(1) Pongamos

$$r_a := (q-1)p^m,$$

donde m es el entero positivo más pequeño tal que $a \leq p^m$.

(2) Sean i, j enteros. Pongamos

$$\begin{aligned} \phi(i,j) &:= r_a - a - j(q-1) + ir_a, \\ \phi(j) &:= \phi(0,j). \end{aligned}$$

(3) Definamos

$$j_{a,\text{máx}} := \left\lfloor \frac{r_a - a}{q-1} \right\rfloor,$$

donde $\lfloor x \rfloor$ es el entero más grande menor o igual que x.

(4) Sea q primo (así $q = p$). Para $0 \leq j \leq j_{a,\text{máx}}$, sea $c_{a,j} \in \mathbb{F}_p$ definida por:

$$c_{a,j} = \begin{cases} 1 & \text{si } j = 0, \\ \left\lceil \frac{j(q-1)}{j_{a,\text{máx}}} \right\rceil^{-1} \binom{r_a - a}{j(q-1)} & 0 < j \leq j_{a,\text{máx}}, \end{cases}$$

donde $\lceil x \rceil$ es el entero más pequeño mayor o igual a x.

(5) Para cada j, $0 \leq j \leq p-1$, sea μ_j el número de j's en la descomposición en base p de $a-1$. Sea

$$t_a = \prod_{j=0}^{p-2} (p-j)^{\mu_j}.$$

Observación 1.4.6. Cuando q es primo y $0 < j \leq j_{a,\text{máx}}$, $\left\lceil \frac{j(q-1)}{j_{a,\text{máx}}} \right\rceil$ es distinto de cero en $\mathbb{F}_p$ porque $0 < \frac{j(q-1)}{j_{a,\text{máx}}} \leq q-1 < p$. Por lo tanto, $c_{a,j}$ en la Definición 1.4.5 (4) tiene sentido. Si q no es primo, $c_{a,j}$ no siempre está definido. Por ejemplo, cuando $q = 4$, $a = 5$ y $j = 3$, se tiene

$$\left\lceil \frac{j(q-1)}{j_{a,\text{máx}}} \right\rceil = \left\lceil \frac{12}{6} \right\rceil = 2.$$

Alternativamente, de la Proposición 2.3.11 vemos que $c_{a,j}$ tiene sentido cuando q es primo.

A continuación presentamos la conjetura principal. Esta conjetura así como todas las conjeturas que aparecen en la Sección 1.5 fueron formuladas por el autor durante sus estudios de maestría, y son producto de la observación de casos particulares. Todos los apartados de esta conjetura, excepto el apartado 4 que se refiere a los valores iniciales, serán probados en la Sección 2.3 (Teorema 2.3.14, Corolario 2.3.19 y Observación 2.3.21).

Conjetura 1.4.7 ([Lar09, Lar10])**.** *Sea $a \in \mathbb{Z}_+$. Entonces*

(1) *Sea $b > r_a$. Los conjuntos $S(a,b)$se pueden encontrar de manera recursiva:*

$$S(a,b) = S(a, b - r_a) \cup T(a,b),$$

donde

a) *$T(a,b)$ es un conjunto de cardinalidad t_a,*

b) *$T(a,b)$ tiene la forma*

$$T(a,b) = \{(c_{j_\ell}, b - \phi(j_\ell)) \colon \ell = 0, \ldots, t_a - 1\}$$

para algún j_ℓ, $0 \leq j_\ell \leq j_{a,\text{máx}}$.

c) *El conjunto* T_a *de pares* $(c_{j_\ell}, \phi(j_\ell))$ *es independiente de* b.

Nos referiremos a los conjuntos $S(a,b)$ *con* $1 \leq b \leq r_a$ *como los conjuntos iniciales o los valores iniciales.*

(2) $(1, \phi(0)) = (1, r_a - a) \in T_a$. *Por lo tanto, si* $t_a = 1$, *entonces* $T_a = \{(1, \phi(0))\}$.

(3) *Si no hay acarreo en base* p *en la suma de* $j(q-1)$ *y* $\phi(j)$, *entonces* $(c, \phi(j)) \in T_a$ *para algún* $c \in \mathbb{F}_p$.

(4) *Para* $r_a - q + 2 \leq b \leq r_a$,

$$S(a,b) = \{(c_j, b - a_j) \colon (c_j, a_j) \in T_a \setminus \{(1, \phi(0))\}\}.$$

(5) *Si* q *es primo (y por lo tanto* $q = p$*), entonces* $(c_{a,j}, \phi(j)) \in T_a$ *si y sólo si no hay acarreo en base* p *en la suma de* $j(q-1)$ *y* $\phi(j)$.

(6) *Si* $T_a = \{(c_{j_\ell}, \phi(j_\ell)) \colon 0 \leq \ell \leq t_a - 1\}$, *entonces* $T_{p^{m'}a} = \{(c_{j_\ell}, p^{m'}\phi(j_\ell)) \colon 0 \leq \ell \leq t_a - 1\}$.

(7) *Denotemos por* $T^\theta(a,b)$ *al conjunto de pares* $(c_j, a_j) \in T(a,b)$ *tales que* $c_j = \theta$. *Entonces la cardinalidad de los conjuntos* $T^\theta(a,b)$ *es independiente de* b.

Con base en la Conjetura 1.4.7, para encontrar $S(a,b)$ para cualquier b es necesario conocer:

a) Los conjuntos iniciales $S(a,b)$, $1 \leq b \leq r_a$,

b) Los conjuntos $T(a,b)$.

Cuando q es primo, la Conjetura 1.4.7(5) describe a T_a completamente.

Observaciones 1.4.8.

(1) La Conjetura 1.4.7 (1) establece que la longitud de recursión es r_a. Esta conjetura mejora la estimación $(q-1)q^m$ para la longitud de recursión dada en [Tha09b].

(2) $\phi(j)$ es una función decreciente de j, así que

$$\phi(j_0) > \phi(j_1) > \cdots > \phi(j_{t_a-1}).$$

(3) El Teorema de Lucas [Luc78a, Luc78b, Dic02, Fin47] establece que si $k = \sum k_i p^i$ y $m_j = \sum m_{ji} p^i$ son descomposiciones en base p, entonces

$$\binom{k}{m_1, \ldots, m_r} \equiv \prod \binom{k_i}{m_{1i}, \ldots, m_{ri}} \text{ mód } p,$$

donde $\binom{k}{m_1,\ldots,m_r}$ es el coeficiente multinomial y está definido por

$$\binom{k}{m_1,\ldots,m_r} = \frac{k!}{m_1!\cdots m_r!}.$$

Dado que $\binom{a}{b} = 0$ si $b > a$, vemos como un corolario de este teorema que el coeficiente multinomial anterior es cero en $\mathbb{F}_p$, si hay acarreo p-ádico en la suma $k = \sum m_i$.

En particular, si q es primo tenemos que no hay acarreo en base q en la suma de $j(q-1)$ y $\phi(j)$ si

$$\binom{r_a - a}{j(q-1), \phi(j)} = \binom{r_a - a}{j(q-1)} \not\equiv 0 \text{ mód } p.$$

Por lo tanto, el Teorema de Lucas junto con la Conjetura 1.4.7 (5) implican que cuando q es primo se tiene

$$\begin{aligned} T_a &= \left\{(c_{a,j}, \phi(j)) \colon \tbinom{r_a-a}{j(q-1)} \not\equiv 0 \text{ mód } q\right\}, \\ t_a &= \#\{j \colon \tbinom{r_a-a}{j(q-1)} \not\equiv 0 \text{ mód } q, 0 \le j \le j_{a,\text{máx}}\}. \end{aligned}$$

(4) Dado que $c_{a,0} = 1$ y $\binom{r_a-a}{0} = 1$, el inciso 2 de la Conjetura 1.4.7 es consistente con el inciso 5 de la misma conjetura.

(5) Dados q, a y b, una conjetura completa para $S(a,b)$ incluye

   a) la longitud de recursión r_a,
   b) los conjuntos iniciales (o valores iniciales) $S(a,b)$, $1 \le b \le r_a$,
   c) el conjunto T_a.

   La Conjetura 1.4.7 no da una distribución de los signos (de los valores multizeta que aparecen en la combinación lineal) de T_a, excepto cuando q es primo, y tampoco conjetura cuáles deben ser los valores iniciales (los conjuntos iniciales), es decir, los conjuntos $S(a,b)$ para $1 \le b \le r_a$. En la Sección 1.5 daremos una descripción completa cuando q es par y $a = 2,3,4$, y cuando q es impar y $a = 2,3$.

(6) El Apartado 6 de la Conjectura 1.4.7 implica que los conjuntos T_a y $T_{p^{m'}}$ tienen la misma cardinalidad, y de acuerdo con el Apartado (1a) se debe cumplir que $t_a = t_{p^{m'}a}$. Esto efectivamente es así, como vemos a continuación. Si $a - 1 = \sum a_i p^i$ es la descomposición en base p de $a-1$, entonces

$$\begin{aligned} p^{m'}a - 1 &= p^{m'} - 1 + \sum a_i p^{m'+i} \\ &= (p-1) + (p-1)p + \cdots + (p-1)p^{m'-1} + \sum a_i p^{m'+i} \end{aligned}$$

   es la descomposición en base p de $p^{m'}a - 1$. De la Definición 1.4.5 (5) se sigue que t_a y $t_{p^{m'}a}$ son iguales.

A continuación se presentan algunas consecuencias de la Conjetura 1.4.7.

Para $b > r_a$, sea $b = r_a\sigma + b'$, $0 < b' \leq r_a$. Entonces

$$S(a,b) = S(a,b') \cup T(a, b-(\sigma-1)r_a) \cup \cdots \cup T(a, b-r_a) \cup T(a,b),$$

donde cada elemento de $T(a, b-ir_a)$ es de la forma $(c_{j_\ell}, b-\phi(j_\ell)-ir_a) = (c_{j_\ell}, \phi(i,j_\ell))$. Vemos que la forma general de $\Delta_d(a,b)$ es:

$$\Delta_d(a,b) = \sum_{(\gamma,\alpha)\in S(a,b')} \gamma S_d(\alpha,\beta) + \sum_{i=0}^{\sigma-1} \sum_{\substack{j \\ (c_j,\phi(j))\in T_a}} c_j S_d(b-\phi(i,j), a+\phi(i,j)). \tag{1.4.8.1}$$

Así, $\Delta_d(a,b)$ tiene una primera parte dada por los valores iniciales y segunda parte regular o recursiva.

Observaciones 1.4.9.

(1) D. Thakur ha conjeturado que todos los $a+b-a_i$ que aparecen en la Observación (1.4.3) deben ser "pares" [Tha09b, 5.3] (En este contexto, un número es "par" si es divisible por $q-1$). Dado que r_a es "par" se tiene que $a+\phi(i,j) = r_a - j(q-1) + ir_a$ siempre es "par"', lo cual es consistente con esta predicción de D. Thakur.

(2) Si para cada a conocemos T_a y también conocemos los valores iniciales $S(a,\beta)$, $1 \leq \beta \leq t_a$, entonces seremos capaces de calcular $S(a,b)$ para cualquier b. Cuando q es primo, la Conjetura 1.4.7 describe a T_a completamente.

1.5. Conjeturas completas

En esta sección presentamos conjeturas completas para expresar $\zeta(a)\zeta(b)$ como una suma de multizetas, para valores pequeños de a y también algunas conjeturas para valores grandes de a. Por una conjetura completa nos referimos a una conjetura que incluye tanto la parte de los valores iniciales como la parte recursiva. Estas conjeturas fueron formuladas durante los estudios de maestría del autor [Lar09, Lar10].

1.5.1. $\zeta(a)\zeta(b)$ cuando $a = 2,3,4$ y q es par

Aquí presentamos conjeturas completas para escribir $\zeta(a)\zeta(b)$ como una combinación lineal de multizetas, cuando $a = 2,3,4$ y q es una potencia de 2. Dado que $\mathbb{F}_2^* = \{1\}$, para simplificar la notación al describir a T_a, en vez de $(1,\phi(j))$ escribiremos $\phi(j)$. De la Conjetura principal 1.4.7 se sigue que si q es primo y $t_a = 2$, entonces, $T_a = \{(1,\phi(0)), (p-1, \phi(j_{a,\text{máx}})\}$. Esto no necesariamente es así si q no es primo. Por ejemplo, cuando $q = 4$ y $a = 7$, $T_7 = \{\phi(0), \phi(3)\}$, pero $3 \neq 5 = j_{7,\text{máx}}$. Introducimos una nueva conjetura: Para cualquier q par se tiene $T_3 = \{\phi(0), \phi(j_{3,\text{máx}})\}$. Sean ϕ, r_a y $j_{a,\text{máx}}$ como en la Definición 1.4.5. De acuerdo con esta nueva conjetura y la Conjetura 1.4.7 se tiene

a	r_a	t_a	T_a
2	$2(q-1)$	1	$\phi(0)$
3	$4(q-1)$	2	$\phi(0), \phi(j_{3,\text{máx}})$
4	$4(q-1)$	1	$\phi(0)$

La siguiente conjetura es una generalización del Teorema 7 en [Tha09b].

Conjetura 1.5.1. *Sea q una potencia de $p = 2$. Escribamos $b = r_2\sigma + \beta$, $0 < \beta \leq r_2$. Entonces*

$$\begin{aligned}\zeta(2)\zeta(b) &= \zeta(2+b) + \zeta(2,b) + \zeta(b,2)\\ &\quad + \sum_{i=0}^{\sigma-1} \zeta(b-\phi(i,0), 2+\phi(i,0)) + \operatorname{Int}\left(\frac{b}{q-1}\right)\frac{b}{q-1}\zeta(2,b),\end{aligned}$$

donde $\operatorname{Int}(x)$ *es* 1 *si* x *es entero y* 0 *en otro caso.*

La Conjetura 1.5.1 será probada en la Sección 2.6 (Teoremas 2.6.5 y 2.6.6). La siguiente conjetura será probada en la Sección 2.6 (Teorema 2.6.7).

Conjetura 1.5.2. *Sea $q = 2$. Entonces*

$$\begin{aligned}\zeta(3)\zeta(b) &= \zeta(b+3) + \zeta(3,b) + \zeta(b,3)\\ &\quad + \sum_{b-\phi(i,0)>3} \zeta(b-\phi(i,0), 3+\phi(i,0))\\ &\quad + \sum_{b-\phi(i,j_{3,\text{máx}})>3} \zeta(b-\phi(i,j_{3,\text{máx}}), 3+\phi(i,j_{3,\text{máx}}))\\ &\quad + \sum_{i=1}^{2} \operatorname{Int}\left(\tfrac{b-i}{r_3}\right)(\zeta(2,b+1)+\zeta(3,b)).\end{aligned}$$

Conjetura 1.5.3. *Sean $p = 2$ y $q = p^n, n > 1$. Entonces*

$$\begin{aligned}\zeta(3)\zeta(b) &= \zeta(3+b) + \zeta(3,b) + \zeta(b,3)\\ &\quad + \sum_{b-\phi(i,0)>3} \zeta(b-\phi(i,0), 3+\phi(i,0))\\ &\quad + \sum_{b-\phi(i,j_{3,\text{máx}})>3} \zeta(b-\phi(i,j_{3,\text{máx}}), 3+\phi(i,j_{3,\text{máx}}))\\ &\quad + \operatorname{Int}\left(\tfrac{b+1}{q-1}\right)\tbinom{(b+1)/(q-1)+1}{2}\zeta(2,b+1)\\ &\quad + \operatorname{Int}\left(\tfrac{b}{q-1}\right)\left(\tbinom{b/(q-1)+2}{2}-1\right)\zeta(3,b).\end{aligned}$$

Conjetura 1.5.4. *Sea q una potencia de $p = 2$. Entonces*

$$\begin{aligned}\zeta(4)\zeta(b) = {} & \zeta(4+b) + \zeta(4,b) + \zeta(b,4) \\ & + \sum_{b-\phi(i,0)>4} \zeta(b-\phi(i,0), 4+\phi(i,0)) \\ & + \mathrm{Int}\left(\tfrac{b-\max\{q-3,1\}}{r_4}\right)\zeta(2,b+2) + \mathrm{Int}\left(\tfrac{b-2q+3}{r_4}\right)\zeta(3,b+1) \\ & + \sum_{i=1}^{3}\mathrm{Int}\left(\frac{b-i(q-1)}{r_4}\right)\zeta(4,b).\end{aligned}$$

1.5.2. $\zeta(a)\zeta(b)$ cuando $a = 2, 3$ y q es impar

Ahora daremos una conjetura completa para escribir $\zeta(a)\zeta(b)$ como suma de multizetas, cuando $a = 2, 3$ y q es una potencia de un primo impar. El problema se vuelve más complicado porque ahora podríamos tener varios conjuntos $S^{\theta}(a,b)$ que describir.

Conjetura 1.5.5. *Sea p un primo impar y sea q una potencia de p. Entonces*

$$\begin{aligned}\zeta(2)\zeta(b) = {} & \zeta(2+b) + \zeta(2,b) + \zeta(b,2) \\ & + \sum_{j=0}^{p-1}(j+2)\sum_{b-\phi(i,p-1-j)>2}\zeta(b-\phi(i,p-1-j), 2+\phi(i,p-1-j)) \\ & + \mathrm{Int}\left(\tfrac{b}{q-1}\right)\tfrac{b}{q-1}\zeta(2,b).\end{aligned}$$

La Conjetura 1.5.5 será probada en la Sección 2.6 (Teorema 2.6.6).

Conjetura 1.5.6. *Sea p un primo impar y sea q una potencia de p. Entonces*

$$\begin{aligned}\zeta(3)\zeta(b) = {} & \zeta(3+b) + \zeta(3,b) + \zeta(b,3) \\ & + \sum_{b-\phi(i,0)>3}\zeta(b-\phi(i,0), 3+\phi(i,0)) \\ & + (1-\delta_{p3})\sum_{b-\phi(i,3)>3}\zeta(b-\phi(i,3), 3+\phi(i,3)) \\ & + \sum_{j=2}^{\frac{p-3}{2}}\tbinom{j+1}{2}\Bigg(\sum_{b-\phi(i,j+2)>3}\zeta(b-\phi(i,j+2), 3+\phi(i,j+2)) + \\ & \sum_{b-\phi(i,p+3-j-2)>3}\zeta(b-\phi(i,p+3-j-2), 3+\phi(i,p+3-j-2))\Bigg)\end{aligned}$$

$$
\begin{aligned}
&+ (1-\delta_{p3})\tbinom{\frac{p+1}{2}}{2} \sum_{b-\phi(i,\frac{p+3}{2})>3} \zeta(b-\phi(i,\tfrac{p+3}{2}), 3+\phi(i,\tfrac{p+3}{2}))\\
&+ \operatorname{Int}\left(\tfrac{b+1}{q-1}\right)\tbinom{(b+1)/(q-1)+1}{2}\zeta(2,b+1)\\
&+ \operatorname{Int}\left(\tfrac{b}{q-1}\right)(\tbinom{b/(q-1)+2}{2}-1)\zeta(3,b),
\end{aligned}
$$

donde δ_{ij} denota la delta de Kronecker[1]*.*

1.5.3. Conjeturas completas para ambos índices grandes

En esta sección presentamos algunas conjeturas, las cuales son generalizaciones de las fórmulas dadas en [Tha09b, 4.1.3].

Conjetura 1.5.7. *Para q general tenemos:*

$$\Delta_d(q^n, q^n-1) = -S_d(q^n, q^n-1). \tag{1.5.7.1}$$

$$
\begin{aligned}
\Delta_d(q^n+1, q^n) = {}& \operatorname{Int}\left(\tfrac{2}{q}\right) S_d(2, 2q^n-1)\\
&- \sum_{j=1}^{\frac{q^n-1}{q-1}} S_d(3+(j-1)(q-1), 2q^n-2-(j-1)(q-1)).
\end{aligned} \tag{1.5.7.2}
$$

$$\Delta_d(q^n-1, q^n+1) = -\sum_{j=1}^{\frac{q^n+q-2}{q-1}} S_d(2+(j-1)(q-1), 2q^n-2-(j-1)(q-1)).$$

$$
\begin{aligned}
\Delta_d(q^{n-1}, q^n+1) = {}& \operatorname{Int}\left(\tfrac{2}{q}\right) S_d(2, q^{n-1}+q^n-1)\\
&- \sum_{j=1}^{\frac{q^{n-1}-1}{q-1}} S_d(3+(j-1)(q-1), q^{n-1}+q^n-2+(j-1)(q-1)).
\end{aligned}
$$

---

[1] La delta de Kronecker se denota con el símbolo δ_{ij} y se define como sigue: $\delta_{ij}=1$ si $i=j$ y $\delta_{ij}=0$ en otro caso.

Para $0 \leq i \leq n$,

$$\begin{aligned}
\Delta_d(q^n+1, q^n+1-q^i) &= \operatorname{Int}\left(\tfrac{2}{q}\right) S_d(2, 2q^n-q^i) \\
&\quad - \sum_{j=1}^{\frac{q^n-q^i}{q-1}} S_d(3+(j-1)(q-1), 2q^n-q^i-1-(j-1)(q-1)) \\
&\quad + \sum_{j=\frac{q^n-q^i}{q-1}+1}^{\frac{q^n-q^i}{q-1}} S_d(3+(j-1)(q-1), 2q^n-q^i-1-(j-1)(q-1)). \qquad (1.5.7.3)
\end{aligned}$$

Observación 1.5.8. Cuando $i = 0$, la Conjetura 1.5.7.3 coincide con la Conjetura 1.5.7.2. Más aún, cuando $p = 2$, los conjuntos $S(q^n+1, q^n+1-q^i)$ son independientes de i.

Conjetura 1.5.9. *Para* $2 \leq m \leq q$, *tenemos que*

$$S_d(mq^i-1) = \frac{\ell_{d+i}}{\ell_i \ell_d^{mq^i}} = \frac{1}{\ell_d^{mq^i-1}} \frac{\ell_{d+i}}{\ell_i \ell_d}.$$

Podemos deducir esta fórmula para $m = 2$ e $i = 1$ de la fórmula para $S_d(aq+b)$ en [Tha09b, 3.3.1], y la hemos probado para $m = i = 2$ usando la función generadora [Tha09b, 3.2] y también la hemos verificado numéricamente para varios valores pequeños de m, i, q. Esta conjetura implica la Ecuación (1.5.7.1) justo como en el Teorema 4 en [Tha09b]. En la Sección 2.7, La Conjetura 1.5.7.1 será probada en tres formas diferentes (Teorema 2.7.2).

CAPÍTULO 2

Relaciones entre los valores multizeta en característica p

En este capítulo probaremos varias de las conjeturas enunciadas en el Capítulo 1. Más precisamente, probaremos la parte recursiva de la Conjetura principal 1.4.7, excepto los puntos referentes a los valores iniciales. También probaremos algunas de las conjeturas formuladas por D. Thakur. Para q general, probaremos fórmulas simétricas y no simétricas para expresar el producto de valores zeta como una suma de valores multizeta. Finalmente, también probaremos las conjeturas formuladas por el autor y por Thakur para valores pequeños o para familias especiales de a's acerca de cómo escribir $\zeta(a)\zeta(b)$ como una $\mathbb{F}_p$-combinación lineal de valores multizeta.

2.1. Fórmulas básicas

Empezamos con la definición de los números $[n]$, D_n y L_n que son fundamentales para la aritmética de $A = \mathbb{F}_q[t]$.

Sean $A = \mathbb{F}_q[t]$ y $K = \mathbb{F}_q(t)$, donde q es una potencia de un primo p.

1. Sea
$$[n] = t^{q^n} - t \in A.$$

2. Sea $D_0 = 1$, y para $n > 0$ sea,
$$D_n = [n][n-1]^q \cdots [1]^{q^{n-1}} \in A.$$

3. Definimos $L_0 = 1$ y para $n > 0$,
$$L_n = [n][n-1] \cdots [1] \in A.$$

   Sea $\ell_n = (-1)^n L_n \in A$.

De la definición vemos que $\ell_n = -[n]\ell_{n-1}$ para $n \geq 1$, y $D_n = [n]D_{n-1}^q$. Sean

$$\begin{aligned}\binom{x}{q^d}_C &= \sum_{i=0}^{d} \frac{x^{q^i}}{D_i \ell_{d-i}^{q^i}} \in K[x],\\ S_{<d}(k) &= \sum_{a\in A_+, \deg(a)<d} \frac{1}{a^k} \in K.\end{aligned}$$

El polinomio $\binom{x}{q^d}_C$ es un análogo al polinomio binomial $x(x-1)\cdots(x-n+1)/n! \in \mathbb{Q}[x]$ [Tha04, Sección 4.14]. Tenemos los siguientes resultados de Carlitz (vea por ejemplo, [Tha04, 2.5, 5.6] o [Gos96])

$$\begin{aligned}D_n &= \prod_{a\in A_+,\, \deg(a)=n} a,\\ \binom{x}{q^d}_C &= \frac{1}{D_d} \prod_{a\in A,\, \deg(a)<d} (x+a).\end{aligned}$$

Un cálculo simple muestra que $\binom{t^d}{q^d}_C = 1$:

$$\binom{t^d}{q^d}_C = \frac{1}{D_d} \prod_{a\in A,\, \deg(a)<d} (t^d + a) = \frac{1}{D_d} \prod_{b\in A_+,\, \deg(b)=d} b = \frac{D_d}{D_d} = 1.$$

Dado que $(x+a)^{q^i} = x^{q^i} + a^{q^i}$ se sigue que $\binom{x+a}{q^d}_C = \binom{x}{q^d}_C + \binom{a}{q^d}_C$. Por lo tanto, $\binom{x+t^d}{q^d}_C = \binom{x}{q^d}_C + 1$. Por otro lado tenemos

$$\begin{aligned}\binom{x+t^d}{q^d}_C &= \frac{1}{D_d} \prod_{a\in A,\, \deg(a)<d} (x+t^d+a) = \frac{1}{D_d} \prod_{a\in A_+,\, \deg(a)=d} (x+a)\\ &= \frac{1}{D_d} \prod_{\substack{a\in A_+,\\ \deg(a)=d}} a \prod_{\substack{a\in A_+,\\ \deg(a)=d}} (1+\frac{x}{a}) = \prod_{a\in A_+,\, \deg(a)=d} (1+\frac{x}{a}).\end{aligned} \tag{2.1.0.1}$$

Es bien conocido que (o se puede probar fácilmente por inducción en d) que si $f(x) = \prod_{i=1}^{d}(x-\alpha_i)$, entonces

$$\frac{f'(x)}{f(x)} = \sum_{i=1}^{d} \frac{1}{x-\alpha_i}.$$

Dado que $(-1)^{q^i} = -1$ en K, de acuerdo con la primera línea de la ecuación (2.1.0.1) tenemos que las raíces del polinomio $f(x) = D_d(1+\binom{-x}{q^d}_C) = D_d(1-\binom{x}{q^d}_C)$ son todos los polinomios mónicos de grado d en A. Claramente

$f'(x)$ se reduce a $-D_d/\ell_d$. Así, tenemos

$$\frac{f'(x)}{f(x)} = \frac{-1}{\ell_d(1-\binom{x}{q^d}_C)} = \sum_{\substack{a\in A_+\\ \deg(a)=d}}^{d} \frac{1}{x-a}.$$

Luego,

$$\frac{1}{\ell_d(1-\binom{x}{q^d}_C)} = \sum_{\substack{a\in A_+\\ \deg(a)=d}}^{d} \frac{1}{a(1-x/a)} = \sum_{\substack{a\in A_+\\ \deg(a)=d}}^{d} \sum_{k=0}^{\infty} \frac{x^k}{a^{k+1}}$$

$$= \sum_{k=0}^{\infty}\left(\sum_{\substack{a\in A_+\\ \deg(a)=d}}^{d} \frac{1}{a^{k+1}}\right) x^k = \sum_{k=0}^{\infty} S_d(k+1)x^k.$$

Por lo tanto, tenemos la función generadora para $S_d(k+1)$:

$$\frac{x}{\ell_d(1-\binom{x}{q^d}_C)} = \sum_{k=1}^{\infty} S_d(k)x^k. \tag{2.1.0.2}$$

Ahora usamos la Ecuación (2.1.0.2) para calcular $S_d(k+1)$. En virtud de que $\sum_{k=1}^{\infty} S_d(k)x^k = x\sum_{k=0}^{\infty} S_d(k+1)x^k$ vemos que el coeficiente de x^k en la correspondiente suma parcial es $S_d(k+1)$. Comparando ambos lados de la Ecuación (2.1.0.2) vemos que $S_d(k+1)$ también es el coeficiente de x^k en $\sum_{n=0}^{k}\binom{x}{q^d}_C^n/\ell_d$, que es la suma parcial de la serie geométrica $1/\ell_d(1-\binom{x}{q^d}_C)$. De acuerdo con el Teorema Multinomial se tiene

$$\frac{1}{\ell_d}\sum_{n=0}^{k}\binom{x}{q^d}_C^n = \frac{1}{\ell_d}\sum_{n=0}^{k}\sum\binom{n}{k_0,k_1,\ldots,k_d}\frac{x^{k_0q^0+\cdots+k_dq^d}}{D_0^{k_0}\cdots D_d^{k_d}\ell_{d-0}^{k_0q^0}\cdots\ell_{d-d}^{k_dq^d}}$$

donde la suma se extiende sobre todas las $(d+1)$-adas $(k_0,\ldots,k_d)$ de enteros no negativos tales que $k_0+\cdots+k_d=n$. Agrupando los términos x^k vemos que

$$S_d(k+1) = \frac{1}{\ell_d}\sum_{\substack{\sum_{i=0}^{d}k_iq^i=k,\\ k_i\geq 0}}\binom{k_d+\cdots+k_0}{k_d,\ldots,k_0}\prod_{i=0}^{d}\left(\frac{1}{D_i\ell_{d-i}^{q^i}}\right)^{k_i}$$

$$= \frac{1}{\ell_d^{k+1}}\sum_{\substack{\sum_{i=0}^{d}k_iq^i=k,\\ k_i\geq 0}}\binom{k_d+\cdots+k_0}{k_d,\ldots,k_0}\prod_{i=0}^{d}\left(\frac{(\ell_d/\ell_{d-i})^{q^i}}{D_i}\right)^{k_i},$$

$$S_d(k+1) = \frac{1}{\ell_d^{k+1}}\sum_{\substack{\sum_{i=0}^{d}k_iq^i=k,\\ k_i\geq 0}}\binom{k_d+\cdots+k_0}{k_d,\ldots,k_0}\prod_{i=1}^{d}\left(\frac{(-1)^i([d]\cdots[d-i+1])^{q^i}}{D_i}\right)^{k_i}, \tag{2.1.0.3}$$

donde las sumas se toman sobre todas las $(d+1)$-adas $(k_0,\ldots,k_d)$ de enteros no negativos tales que $\sum_{i=0}^d k_i q^i = k$.

Cuando $d=1$, la Ecuación (2.1.0.3) se convierte en:

$$S_1(k+1) = \frac{(-1)^{k+1}}{[1]^{k+1}} \left(1 + \sum_{k_1=1}^{\lfloor k/q \rfloor} \binom{k-k_1(q-1)}{k_1} (-1)^{k_1}[1]^{k_1(q-1)}\right). \tag{2.1.0.4}$$

Un caso especial de (2.1.0.3) es:

$$S_d(ap^n) = 1/\ell_d^{ap^n}, \quad \text{si } a \leq q. \tag{2.1.0.5}$$

Podemos deducir la fórmula (2.1.0.5) de la Ecuación (2.1.0.3) observando que cuando $k+1 = a \leq q$, tenemos exactamente una $(d+1)$-ada: $(a-1,0,\ldots,0)$. Así, la Ecuación (2.1.0.3) se convierte en $S_d(a) = 1/\ell_d^a$.

Análogamente, usando el polinomio $D_d\binom{x}{q^d}_C$ obtenemos la función generadora para $S_{<d}(k)$ cuando k es “par”:

$$\frac{x}{\ell_d\binom{x}{q^d}_C} = 1 + \sum_{k>0,\text{“par”}} S_{<d}(k)x^k. \tag{2.1.0.6}$$

El lado izquierdo de la Ecuación (2.1.0.6) es igual a $(1-\Sigma)^{-1}$, donde

$$\Sigma = \sum_{i=1}^d \frac{-\ell_d x^{q^i-1}}{D_i \ell_{d-i}^{q^i}}.$$

Expandiendo la serie geométrica obtenemos

$$S_{<d}(k) = \frac{1}{\ell_d^k} \sum_{\substack{k=\sum_{i=1}^d k_i(q^i-1),\\ k_i\geq 0}} \binom{k_d+\cdots+k_1}{k_d,\ldots,k_1}(-1)^k \prod_{i=1}^d \left(\frac{(-1)^i([d]\cdots[d-i+1])^{q^i}}{D_i}\right)^{k_i}. \tag{2.1.0.7}$$

Para calcular $S_{<d}(k)$, ahora comparamos los dos lados de la Ecuación (2.1.0.6). Observamos que el lado izquierdo de (2.1.0.6) es igual a $(1-\Sigma)^{-1}$, donde $\Sigma = \sum_{i=1}^d \frac{-\ell_d x^{q^i-1}}{D_i\ell_{d-i}^{q^i}}$. Concluimos que el coeficiente de x^k en la serie $1+\Sigma+\Sigma^2+\cdots$ es igual a $S_{<d}(k)$.

A continuación tenemos un caso especial de la función generadora (2.1.0.6):

$$\begin{aligned} S_{<d}(q^i-1) &= \frac{\ell_{d+i-1}}{\ell_i \ell_{d-1}^{q^i}} = \frac{1}{\ell_d^{q^i-1}} \frac{\ell_d^{q^i-1}\ell_{d+i-1}}{\ell_i\ell_{d-1}^{q^i}} \\ &= (-1)^{q^i-1}\frac{1}{\ell_d^{q^i-1}} \frac{[d+i-1][d+i-2]\cdots[d]^{q^i}}{[i][i-1]\cdots[1]}. \end{aligned} \tag{2.1.0.8}$$

La siguiente fórmula se puede deducir de la función generadora (2.1.0.2), pero también se sigue de la Ecuación (2.1.0.8) y tomando en cuenta que $S_{<(d+1)}(k) = S_{<d}(k) + S_d(k)$.

$$S_d(q^i-1) = \frac{\ell_{d+i-1}}{\ell_{i-1}\ell_d^{q^i}} = \frac{[d+i-1]\cdots[d+1]}{[i-1]\cdots[1]\ell_d^{q^i-1}}. \tag{2.1.0.9}$$

2.2. La restricción "par"

En [Tha09b], Thakur conjetura que en la identidad $\zeta(a)\zeta(b) = \zeta(a+b) + \zeta(a,b) + \zeta(b,a) + \sum f_i\zeta(a_i, b_i)$ los índices b_i deben ser "pares" y da algunas razones heurísticas para ello. El siguiente teorema prueba la conjetura de la paridad de Thakur. Una prueba diferente se da en la Sección 2.4 (como un corolario del Teorema 2.4.11).

El siguiente teorema mejora el Teorema 1.4.1.

Teorema 2.2.1. *Sea $A = \mathbb{F}_q[t]$. Dados $a, b \in \mathbb{Z}_+$, existen $f_i \in \mathbb{F}_p$ y $a_i \in \mathbb{Z}_+$, tales que*

$$S_1(a)S_1(b) - S_1(a+b) = \sum f_i S_1(a_i). \tag{2.2.1.1}$$

Más aún, $a + b - a_i$ es "par" para cada a_i.

Demostración. La primera parte de este teorema ya está probado en [Tha10]. Siguiendo la prueba dada ahí, aquí probaremos la segunda parte.

Para simplificar un poco la notación, haremos el cambio $U \longleftrightarrow \frac{1}{[1]}$. La ecuación (2.1.0.4) se convierte en

$$\begin{aligned} S_1(a) &= (-1)^a U^a \left(1 + \sum_{i=1}^{n_a} \binom{a-1-i(q-1)}{i} (-1)^i U^{-i(q-1)}\right) \\ &= \alpha_{a,0}U^{\varphi_a(0)} + \alpha_{a,1}U^{\varphi_a(1)} + \cdots + \alpha_{a,n_a}U^{\varphi_a(n_a)}, \end{aligned}$$

donde $\varphi_a(i) = a - i(q-1)$, $0 \le i \le n_a = \lfloor (a-1)/q \rfloor$, y

$$\alpha_{a,i} = \begin{cases} (-1)^a & \text{si } i = 0, \\ \binom{\varphi_{a-1}(i)}{i}(-1)^{a+i} & \text{para } i = 1, \dots, n_a. \end{cases}$$

Así, $S_1(a)$ es una $\mathbb{F}_p$-combinación lineal de potencias de U y, por lo tanto, $\Delta(a,b)$ también lo es. Más precisamente, dado que $\varphi_a(i) + \varphi_b(j) = \varphi_{a+b}(i+j)$, y $\alpha_{a,0}\alpha_{b,0} = \alpha_{a+b,0} = (-1)^{a+b}$, se tiene que

$$\begin{aligned} S_1(a)S_1(b) - S_1(a+b) &= \left(\sum_{i=0}^{n_a} \alpha_{a,i}U^{\varphi_a(i)}\right)\left(\sum_{j=0}^{n_b} \alpha_{b,j}U^{\varphi_b(j)}\right) - \sum_{l=0}^{n_{a+b}} \alpha_{a+b,l}U^{\varphi_{a+b}(l)} \\ &= \sum_{k=0}^{n_a+n_b} \beta_k U^{\varphi_{a+b}(k)} - \sum_{l=0}^{n_{a+b}} \alpha_{a+b,l}U^{\varphi_{a+b}(l)} \\ &= \sum_{k=1}^{n_a+n_b} \beta_k U^{\varphi_{a+b}(k)} - \sum_{k=1}^{n_{a+b}} \alpha_{a+b,k}U^{\varphi_{a+b}(k)}, \end{aligned}$$

donde $\beta_k = \sum_{i+j=k} \alpha_{a,i}\alpha_{b,j}$. Note que

$$a + b - \varphi_{a+b}(k) = (a+b) - (a+b) + k(q-1) = k(q-1).$$

Por lo tanto, $S_1(a)S_1(b) - S_1(a+b)$ es un polinomio en U con coeficientes en $\mathbb{F}_p$ de grado menor que $a+b$, tal que $a+b-i$ es "par" para cada potencia i de U. Escribamos

$$S_1(a)S_1(b) - S_1(a+b) = \theta_n U^n + \cdots + \theta_0 U^0,$$

donde $\theta_n \neq 0$, $n < a+b$. Sean $f_1 = (-1)^n \theta_n$ y $a_1 = n$. Cada potencia de U en $S_1(a_1)$ es de la forma $\varphi_{a_1}(i) = a_1 - i(q-1)$. Dado que $q-1$ divide a $a+b-a_1$, $q-1$ divide a $a+b-a_1+i(q-1) = a+b-\varphi_{a_1}(i)$. Entonces, $S_1(a)S_1(b) - S_1(a+b) - f_1 S_1(a_1)$ es nuevamente un polinomio en U con coeficientes en $\mathbb{F}_p$ de grado menor que n, y cada potencia de U satisface la condición "par". Continuamos de esta manera inductivamente hasta que la suma sea vacía. □

Teorema 2.2.2. *Sea q una potencia de p. Sea K un campo de funciones de una variable con campo de constantes $\mathbb{F}_q$; sea ∞ un lugar racional de K, es decir un lugar de grado uno*[1]*, y sea A el anillo de los elementos de K que no tienen polos excepto posiblemente en ∞. Dados $a, b \in \mathbb{Z}_+$, existen $f_i \in \mathbb{F}_p$ y $a_i \in \mathbb{Z}_+$ tales que*

$$\zeta(a)\zeta(b) - \zeta(a+b) - \zeta(a,b) - \zeta(b,a) = \sum f_i \zeta(a_i, a+b-a_i),$$

con $a+b-a_i$ "par".

Demostración. De acuerdo con el Teorema 2.2.1, existen $f_i \in \mathbb{F}_p$ y $a_i \in \mathbb{Z}_+$ tales que la Ecuación (2.2.1.1) es válida, y los $a+b-a_i$ son "pares". Por el Teorema 1.4.2, tenemos que

$$S_d(a)S_d(b) - S_d(a+b) = \sum f_i S_d(a_i, a+b-a_i)$$

es válido para $d \geq 0$. De esto se sigue el teorema. □

2.3. Prueba de la conjetura principal

En esta sección probaremos la parte de la Conjetura Principal 1.4.7 que se refiere a la recursión, excepto la parte que concierne a los valores iniciales.

Sean $a, b \in \mathbb{Z}_+$. Sea $r_a = p^m(q-1)$, donde m es el entero más pequeño tal que $a \leq p^m$. Sea $j \in \{0, 1, \ldots, p^m - a\}$. Dado que p^m y $q-1$ son primos relativos, p^m es una unidad en $\mathbb{Z}/(q-1)\mathbb{Z}$; así, la congruencia $j \equiv -ip^m$ mód $(q-1)$ siempre tiene solución. Más aún, existe exactamente una solución en el rango $0 \leq i < q-1$ (cuando $q = 2$, i siempre es 0).

Definición 2.3.1. Sea i_j el único entero $0 \leq i_j < q-1$ tal que $j + i_j p^m \equiv 0$ mód $(q-1)$. Sea l_j el entero no negativo definido por

$$l_j = \frac{j + i_j p^m}{q-1}.$$

En general, la correspondencia $j \mapsto i_j$ entre los conjuntos $\{0, 1, \ldots, p^m - a\}$ y $\{0, 1, \ldots, q-2\}$ no es ni inyectiva ni suprayectiva. Para la inyectividad, si $j + i_j p^m \equiv 0$ mód $(q-1)$ y $l \neq 0$ es tal que $0 \leq j + l(q-1) \leq p^m - a$, entonces $(j + l(q-1)) + i_j p^m \equiv 0$ mód $(q-1)$ (vea el Ejemplo 2.3.2 a continuación). Cuando $q = 9$ y $a = 21, \ldots, 27$, la correspondencia no es suprayectiva (vea el Ejemplo 2.3.3).

[1]El grado de un lugar es el grado de la extensión del campo residual con respecto al infinito sobre el campo de constantes.

Ejemplo 2.3.2. Sean $q = 9$ y $a = 17$. Entonces, $m = 3$. Si $j = 4$, $i_4 = 4$ ya que $4 + 4(27) = 112 = 14(q-1)$. Si $i = 5$, entonces hay dos j's (1 y 9) tales que $j + 5p^m \equiv 0 \text{ mód } (q-1)$. En la siguiente tabla, en la entrada (j, i_j) aparece $j + i_j p^m$, $j = 0, 1, \ldots, p^m - a$.

$j \setminus i_j$	0	1	2	3	4	5	6	7
0	0							
1						136		
2			56					
3								192
4					112			
5		32						
6							168	
7				88				
8	8							
9						144		
10			64					

Ejemplo 2.3.3. Sean $q = 9$ y $a = 21$. Entonces $m = 3$. En la entrada (j, i_j) de la siguiente tabla aparece $j + i_j p^m$ para $j = 0, 1, \ldots, p^m - a$.

$j \setminus i_j$	0	1	2	3	4	5	6	7
0	0							
1						136		
2			56					
3								192
4					112			
5		32						
6							168	

La correspondencia $j \mapsto i_j$ no es suprayectiva porque cuando $i = 3$ no existe una $j \in \{0, 1, \ldots, 6\}$ tal que $j + 3p^m \equiv 0 \text{ mód } (q-1)$.

Ejemplo 2.3.4. Sea $q = 5$ y $a = 16$. Entonces $m = 2$.

$j \setminus i_j$	0	1	2	3
0	0			
1				76
2			52	
3		28		
4	4			
5				80
6			56	
7		32		
8	8			
9				84

Este ejemplo sugiere que cuando q es primo, i_j es fácil de calcular.

La siguiente proposición nos dice cómo calcular i_j cuando q es primo. Esto será usado en la prueba de la Proposición 2.3.11.

Proposición 2.3.5. *Sea q primo (de tal manera que $q = p$). Si $j \in \{1, \dots, p^m - a\}$, entonces*

$$i_j = \begin{cases} q-1-r & \text{si } r > 0, \\ 0 & \text{si } r = 0. \end{cases}$$

donde $j \equiv r \text{ mód } (q-1)$, $0 \leq r < q-1$.

Demostración. Dado $j > 0$, calculamos i_j como sigue. Primero escribimos $j = l(q-1) + r$, $0 \leq r < q-1$. Si $r > 0$, entonces

$$j + (q-1-r)p^m = (l + p^m)(q-1) + r(1-p^m) \equiv 0 \text{ mód } (q-1),$$

y $0 < q-1-r < q-1$. Si $r = 0$, entonces $j \equiv 0 \text{ mód } (q-1)$. De la definición se sigue que i_j es como se afirmó. □

Proposición 2.3.6. *El mapeo*

$$\begin{array}{ccc} \{0, 1, \dots, p^m - a\} & \to & \{l(q-1) \mid 0 \leq l \leq j_{a,\text{máx}}\} \\ j & \mapsto & j + i_j p^m \end{array}$$

es inyectivo.

Demostración. Dado que $0 \leq j \leq p^m - a$ y $0 \leq i_j \leq q-2$, se sigue que $0 \leq j + i_j p^m \leq p^m - a + p^m(q-2) = r_a - a$. Esto prueba que el mapeo está bien definido. Si $a = p^m$, entonces el mapeo claramente es inyectivo. Supongamos que $a < p^m$. En particular, esto implica que $m \geq 1$. Si $j_1 + i_{j_1}p^m = j_2 + i_{j_2}p^m$, entonces $p^m \mid j_1 - j_2$. Dado que $0 \leq j_1, j_2 \leq p^m - a < p^m$, concluimos que $j_1 = j_2$. □

Cuando $q = 2$, el mapeo de la Proposición 2.3.6 es una biyección, pero en general el mapeo no es suprayectivo. Vea los Ejemplos 2.3.2, 2.3.3, y 2.3.4.

Necesitamos la siguiente proposición.

Proposición 2.3.7. *Las siguientes afirmaciones son válidas en $\mathbb{F}_p$:*

a) *Si $0 \leq i \leq q-1$, entonces*

$$\binom{q-1}{i} = (-1)^i. \tag{2.3.7.1}$$

b) *Si $0 \leq i \leq p-2$, entonces*

$$\binom{p-2}{i} = (-1)^i(i+1).$$

c) *El número de j's, $0 \leq j \leq p^m - a$, tales que $\binom{p^m-a}{j}$ no es cero módulo p es t_a.*

Demostración. a) Consideremos primero el caso $0 \leq i \leq p-1$. Entonces $(p-1)!$, $i!$, y $(p-1-i)!$ son distintos de cero módulo p; por lo tanto, en $\mathbb{F}_p$, se tiene

$$\begin{aligned} \binom{p-1}{i} &= \frac{(p-1)(p-2)\cdots(p-i)}{i!} \\ &= \frac{(-1)(-2)\cdots(-i)}{i!} \\ &= (-1)^i. \end{aligned}$$

Así, la igualdad (2.3.7.1) es válida en este caso especial.

Para una i general, sea $i = \sum_{l=0}^{s-1} i_l p^l$ la descomposición en base p de i. La expansión en base p de $q-1$ es $\sum_{l=0}^{s-1}(p-1)p^l$. Note que $(-1)^{a_l} = (-1)^{a_l p^l}$. Por el Teorema de Lucas concluimos

$$\binom{q-1}{i} = \prod_{l=0}^{s-1}\binom{p-1}{i_l} = \prod_{l=0}^{s-1}(-1)^{i_l p^l} = (-1)^i.$$

Así, (2.3.7.1) es válida en general.

b) Para la segunda parte, dado que $(p-2)!$, $i!$, y $(p-2-i)!$ no son cero módulo p, obtenemos

$$\begin{aligned} \binom{p-2}{i} &= \frac{(p-2)(p-3)\cdots(p-2-(i-1))}{i!} \\ &= \frac{(-2)(-3)\cdots(-(i+1))}{i!} \\ &= (-1)^i(i+1). \end{aligned}$$

c) Sea t'_a el número de j's en $\{0,1,\ldots,p^m-a\}$ tales que $\binom{p^m-a}{j} \not\equiv 0 \text{ mód } p$. Probaremos que $t'_a = t_a$. Como $a \leq p^m$, entonces $a-1 \leq p^m - 1 = \sum_{l=0}^{m-1}(p-1)p^l$. Sean $a-1 = \sum_{l=0}^{m-1} a_l p^l$ y $j = \sum_{l=0}^{m-1} b_l p^l$ las descomposiciones en base p de $a-1$ y j, respectivamente. Como $p^m - 1 - (a-1) = p^m - a$, la descomposición en base p de $p^m - a$ es $\sum_{l=0}^{m-1}(p-1-a_l)p^l$. Por el Teorema de Lucas,

$$\binom{p^m-a}{j} \equiv \prod_{l=0}^{m-1}\binom{p-1-a_l}{b_l} \text{ mód } p.$$

Ya que $\binom{\alpha}{\beta}$ es cero módulo p si $\beta > \alpha$, eligiendo b_l en el conjunto $\{0,1,\ldots,p-1-a_l\}$, garantizamos que $\binom{p^m-a}{j}$ no se hace cero módulo p. Por lo tanto,

$$t'_a = \prod_{l=0}^{m-1}(p-a_l) = \prod_{k=0}^{p-2}(p-k)^{\mu_k} = t_a,$$

donde μ_k es el número de k's en la descomposición en base p de $a-1$. $\square$

Proposición 2.3.8. *Sea $q = 2$. Entonces $j_{a,\text{máx}} = 0$ si y sólo si $a = p^m$. Si $q > 2$, entonces $j_{a,\text{máx}} = 0$ si y sólo si $a = 1$.*

Demostración. Recordemos que $j_{a,\text{máx}} = \left\lfloor \frac{r_a - a}{q-1} \right\rfloor$. Dado que $2 \leq q$ y $a \leq p^m$ tenemos $a \leq p^m(q-1) = r_a$. Como consecuencia, $0 \leq r_a - a$ y $0 \leq \frac{r_a-a}{q-1}$ (si $q \geq 3$, entonces $2a \leq p^m(q-1)$, y por tanto $0 < 1 \leq a \leq p^m(q-1) - a = r_a - a$).

Si $q = 2$, tenemos $\frac{r_a-a}{q-1} = p^m - a$ y así $j_{a,\text{máx}} = 0$ si y sólo si $a = p^m$.

Supongamos que $q \geq 3$. Sea $a = 1$. Consecuentemente, $m = 0$ y $0 \leq \frac{r_a-a}{q-1} = p^0 - \frac{1}{q-1} < 1$. Así, $j_{a,\text{máx}} = 0$.

Recíprocamente, supongamos que $j_{a,\text{máx}} = 0$, es decir, $0 \leq \frac{r_a-a}{q-1} = p^m - \frac{a}{q-1} < 1$. Entonces,

$$p^m - 1 < \frac{a}{q-1} \leq a \leq p^m.$$

Luego, $a = p^m$. Se tiene $p^m - \frac{p^m}{q-1} = p^m \left(\frac{q-2}{q-1}\right) < 1$. Ya que $q \geq 3$,

$$p^m < \frac{q-1}{q-2} = 1 + \frac{1}{q-2} < 2.$$

Entonces $m = 0$ y $a = 1$. $\square$

Definición 2.3.9. Para cada j, $0 \leq j \leq p^m - a$, sea $f_{a,j} \in \mathbb{F}_p$ definida por

$$f_{a,j} = \binom{p^m - a}{j}(-1)^j. \tag{2.3.9.1}$$

Proposición 2.3.10. *El número de j's tales que $f_{a,j} \neq 0$ es t_a.*

Demostración. Se sigue inmediatamente de la Proposición 2.3.7(c). $\square$

Cuando q es primo, tenemos otra descripción para $f_{a,j}$ la cual es consistente con la afirmación 3 de la Conjetura 1.4.7 (vea la Observación 2.3.21 (1)).

Proposición 2.3.11. *Si q es primo, entonces para $j \in \{1, 2, \ldots, p^m - a\}$*

$$f_{a,j} = \left\lceil \frac{j + i_j p^m}{j_{a,\text{máx}}} \right\rceil^{-1} \binom{r_a - a}{j + i_j p^m} = c_{a,l_j},$$

donde c_{a,l_j} es como se definió en 1.4.5.

Demostración. Ya que $0 \leq j \leq p^m - a$ y $0 \leq i_j \leq q-2$, se sigue que $0 \leq j + i_j p^m \leq p^m - a + p^m(q-2) = r_a - a$. Entonces $0 \leq l_j \leq \frac{r_a-a}{q-1}$. Siendo l_j un entero, obtenemos que $0 \leq l_j \leq j_{a,\text{máx}}$. Luego, l_j está en el dominio de definición de $c_{a,k}$.

Afirmamos que (A): $i_j + 1 = \left\lceil \frac{j + i_j p^m}{j_{a,\text{máx}}} \right\rceil$, $(j > 0)$, lo cual es equivalente a probar

$$i_j j_{a,\text{máx}} < j + i_j p^m \leq (i_j + 1) j_{a,\text{máx}}.$$

Es suficiente probar la última desigualdad de la derecha, ya que

$$j_{a,\text{máx}} = \left\lfloor p^m - \frac{a}{q-1} \right\rfloor \leq p^m - \frac{a}{q-1} < p^m,$$

implica $i_j j_{a,\text{máx}} \leq i_j p^m < j + i_j p^m$. Notemos que $j + i_j p^m < j' + i_{j'} p^m$ si y sólo si $i_j < i_{j'}$ o $i_j = i_{j'}$ y $j < j'$. Por lo tanto, es suficiente probar que $\lambda + i_j p^m \leq (i_j+1) j_{a,\text{máx}}$ donde $\lambda = \text{máx}\{j' \mid i_{j'} = i_j\}$. Escribamos $j = l(q-1)+r$, $0 \leq r < q-1$. Por la Proposición 2.3.5 sabemos que $i_j = q-1-r$ si $r > 0$ e $i_j = 0$, en otro caso. Observe que $0 \leq i_j \leq q-2$, así que $i_j + 1$ es distinto de cero en $\mathbb{F}_p$. Escribamos $a = l'(q-1) + a'$, $0 \leq a' < q-1$. Entonces $j_{a,\text{máx}} = p^m - l' - y$, donde $y = 0$ si $a' = 0$ y $y = 1$ en otro caso. Consideremos primero el caso $j \not\equiv 1 \text{ mód } (q-1)$. Así $i_j \neq q-2$. Sea $j_0 \in \{2, \ldots, p^m - a\} \cap \{2, \ldots, q-1\}$ tal que $i_j = i_{j_0}$. Entonces $j_0 = q - u$ para algún u, $1 \leq u \leq q-2$ y $i_{j_0} = u-1$, $0 \leq i_{j_0} < q-2$. Entonces

$$\begin{aligned}
j + i_j p^m &\leq j_0 + i_{j_0} p^m + (q-1) \left\lfloor \frac{p^m - a + i_j p^m - (j_0 + i_{j_0} p^m)}{q-1} \right\rfloor \\
&= q - u + (u-1)p^m + (q-1) \left\lfloor \frac{p^m - a - j_0}{q-1} \right\rfloor \\
&= q - u + (u-1)p^m + p^m - 1 - l'(q-1) - z(q-1),
\end{aligned}$$

donde $z = 1$ si $0 < (a' + j_0 - 1)/(q-1) \leq 1$ y $z = 2$ si $1 < (a' + j_0 - 1)/(q-1) < 1 + (q-2)/(q-1)$. Puesto que $u \leq q-1$, se tiene $l'u \leq l'(q-1) \leq l'(q-1) + (z-1)(q-1)$. Luego

$$\begin{aligned}
j + i_j p^m &= up^m - u - l'(q-1) - (z-1)(q-1) \leq up^m - l'u - yu \\
&= (i_j + 1) j_{a,\text{máx}}.
\end{aligned}$$

Por otro lado, si $j \equiv 1 \text{ mód } (q-1)$, entonces $i_j + 1 = q-1$. Ya que $j \leq p^m - a$, tenemos $j + i_j p^m \leq r_a - a$. Ahora,

$$\frac{j + i_j p^m}{i_j + 1} = \frac{j + i_j p^m}{q-1} \leq \frac{r_a - a}{q-1}.$$

La afirmación se sigue en virtud de que el lado izquierdo es un entero.

Sean $j = b_0 + b_1 p + \cdots + b_{m-1} p^{m-1}$ y $a - 1 = a_0 + a_1 p + \cdots + a_{m-1} p^{m-1}$ las descomposiciones en base p de j y $a-1$, respectivamente. La descomposición en base p de $p^m(p-1) - 1$ es $\sum_{l=0}^{m-1} (p-1)p^l + (p-2)p^m$. En consecuencia, la descomposición en base p de $r_a - a = r_a - 1 - (a-1)$ es $\sum_{l=0}^{m-1} (p-1-a_l)p^l + (p-2)p^m$. Finalmente, la descomposición en base p de $j + i_j p^m$ es $\sum_{l=0}^{m-1} b_l p^l + i_j p^m$.

Note que $j + i_j \equiv j + i_j p^m \equiv 0 \text{ mód } (q-1)$, así que (B): $(-1)^{i_j} = (-1)^j$. Por el Teorema de Lucas, la parte b) de la Proposición 2.3.7, y (A), (B) respectivamente, tenemos

$$\begin{aligned}
\binom{r_a - a}{j + i_j p^m} &= \binom{p-1-a_0}{b_0} \cdots \binom{p-1-a_{m-1}}{b_{m-1}} \binom{p-2}{i_j} \\
&= \binom{p^m - a}{j} (-1)^{i_j} (i_j + 1) \\
&= f_{a,j} \left\lceil \frac{j + i_j p^m}{j_{a,\text{máx}}} \right\rceil. \qquad \square
\end{aligned}$$

Proposición 2.3.12. *Sean q una potencia de p y $a \in \mathbb{Z}_+$. Para cada $n \in A_{1+}$, sea g_n definido por*

$$g_n = -\frac{[1]^{p^m-a}}{n^{p^m-a}}[1]^a S_1(a).$$

Entonces,

$$g_n = 1 + \sum_{j=1}^{p^m-a} f_{a,j} n^{r_a-(j+i_j p^m)},$$

donde $f_{a,j}$ es como en la Definición 2.3.9 e i_j es el único entero $0 \leq i_j < q-1$, tal que $j + i_j p^m \equiv 0 \text{ mód } (q-1)$.

Demostración. Dado que $\theta^q = \theta$ para $\theta \in \mathbb{F}_q$, tenemos que $[1] = n^q - n = n\left(n^{q-1} - 1\right)$ para $n \in A_{1+}$. Entonces,

$$\frac{[1]}{n} = n^{q-1} - 1 \text{ o equivalentemente } 1 + \frac{[1]}{n} = n^{q-1}.$$

Tenemos

$$-\frac{[1]^{p^m-a}}{n^{p^m-a}} = -(n^{q-1}-1)^{p^m-a} = \sum_{j_1=0}^{p^m-a} \binom{p^m-a}{j_1} (-1)^{p^m-a-j_1+1} n^{j_1(q-1)}.$$

Por otro lado,

$$\begin{aligned}
[1]^a S_1(a) &= (-1)^a + \sum_{j_2}^{n_a} \alpha_{a,j_2} [1]^{j_2(q-1)} \\
&= (-1)^a + \sum_{j_2}^{n_a} \alpha_{a,j_2} n^{j_2(q-1)} (n^{q-1}-1)^{j_2(q-1)}.
\end{aligned}$$

donde n_a y α_{a,j_2} son como se definieron en la Sección 2.2. Dado que

$$n^{j_1(q-1)} n^{j_2(q-1)} (n^{q-1}-1)^{j_2(q-1)} = \sum_{j_3=0}^{j_2(q-1)} \binom{j_2(q-1)}{j_3} (-1)^{j_2(q-1)-j_3} n^{(j_1+j_2+j_3)(q-1)},$$

vemos que

$$g_n = -\frac{[1]^{p^m-a}}{n^{p^m-a}}[1]^a S_1(a) = -(n^{q-1}-1)^{p^m-a}[1]^a S_1(a)$$

es un polinomio en n con coeficientes en $\mathbb{F}_p$ (cuando lo vemos como un polinomio en t, entonces $g_n \in \mathbb{F}_q[t]$). Todas las potencias de n son "pares". Si $n = t - \theta$ para algún $\theta \in \mathbb{F}_q$, entonces $g_n(t+\theta) = g_t$. Si $g_n = \sum_j c_{n,j} n^{j(q-1)}$, se sigue que $c_{n,j} = c_{t,j}$ para toda j. Ahora es suficiente calcular $c_{t,j}$. Para hacerlo, pongamos $h_\theta = (t-\theta)^{p^m-a}\left((t-\theta)^{q-1}-1\right)^{p^m}$, $\theta \in \mathbb{F}_q^*$. Entonces,

$$\begin{aligned}
h_\theta &= \sum_{j=0}^{p^m-a} \binom{p^m-a}{j} t^{p^m-a-j}\theta^j(-1)^j \left(\sum_{i=0}^{q-1} \binom{q-1}{i}^{p^m} t^{p^m(q-1-i)}\theta^{ip^m}(-1)^i - 1\right) \\
&= \sum_{j=0}^{p^m-a} f_{a,j} t^{p^m-a-j} \left(\sum_{i=0}^{q-1} t^{p^m(q-1-i)}\theta^{j+ip^m} - \theta^j\right).
\end{aligned}$$

Como $\theta^{q-1} = 1$ para $\theta \in \mathbb{F}_p^*$, se sigue que

$$\begin{aligned}
\sum_{\theta\in\mathbb{F}_q^*} h_\theta &= \sum_{j=0}^{p^m-a} f_{a,j} t^{p^m-a-j} \left(\sum_{i=0}^{q-1} t^{p^m(q-1-i)} \sum_{\theta\in\mathbb{F}_q^*} \theta^{j+ip^m} - \sum_{\theta\in\mathbb{F}_q^*}\theta^j\right) \\
&= \sum_{j=0}^{p^m-a} f_{a,j} t^{p^m-a-j} \left(\sum_{i=0}^{q-2} t^{p^m(q-1-i)} \sum_{\theta\in\mathbb{F}_q^*} \theta^{j+ip^m}\right) \\
&= \sum_{j=0}^{p^m-a} f_{a,j} t^{p^m-a-j} \left(t^{p^m(q-1-i_j)}(-1)\right) \\
&= -\sum_{j=0}^{p^m-a} f_{a,j} t^{r_a-a-(j+i_jp^m)+p^m}.
\end{aligned}$$

Aquí, usamos que $\sum_{\theta\in\mathbb{F}_q^*}\theta^l$ es 0 si $q-1$ no divide a l, y -1 si $l \geq 0$ es divisible por $q-1$. Ahora, para cualquier $n \in A_{1+}$, $[1]^{p^m} = \left(n(n^{q-1}-1)\right)^{p^m}$; así,tenemos

$$\begin{aligned}
[1]^{p^m} S_1(a) &= \sum_{n\in A_{1+}} \frac{[1]^{p^m}}{n^a} = \sum_{n\in A_{1+}} n^{p^m-a}\left(n^{q-1}-1\right)^{p^m} \\
&= t^{p^m-a}(t^{r_a}-1) + \sum_{\theta\in\mathbb{F}_q^*} h_\theta.
\end{aligned}$$

Se sigue que

$$\begin{aligned}
g_t = -\frac{1}{t^{p^m-a}}[1]^{p^m} S_1(a) &= -t^{r_a} + 1 + \sum_{j=0}^{p^m-a} f_{a,j} t^{r_a-(j+i_jp^m)} \\
&= -t^{r_a} + 1 + f_{a,0}t^{r_a} + \sum_{j=1}^{p^m-a} f_{a,j} t^{r_a-(j+i_jp^m)} \\
&= 1 + \sum_{j=1}^{p^m-a} f_{a,j} t^{r_a-(j+i_jp^m)}. \qquad \square
\end{aligned}$$

Ejemplo 2.3.13. Sean $q = 9$ y $a = 17$. Entonces, $m = 3$ y $r_a = 27(8) = 216$. Dado que $a - 1 = 1 + 2p + p^2$, tenemos $t_a = 3^0 2^2 = 4$. Las j's para las cuales $f_{a,j} \neq 0$ son 0, 1, 9, y 10. Usando la tabla del Ejemplo 2.3.2, tenemos

$$g_t = 1 + f_{a,1}t^{216-136} + f_{a,9}t^{216-144} + f_{a,10}t^{216-64} = 1 + 2t^{80} + 2t^{72} + t^{152}.$$

Entonces, $g_{t-\theta} = 1 + 2(t-\theta)^{80} + 2(t-\theta)^{72} + (t-\theta)^{152}$ para cualquier $\theta \in \mathbb{F}_q$. Dado que $136 = 17(q-1)$, $144 = 18(q-1)$ y $64 = 8(q-1)$, el conjunto T_{17} es

$$\begin{aligned} T_{17} &= \{(0,\phi(0)),(1,\phi(17)),(9,\phi(18)),(10,\phi(8))\} \\ &= \{(0,199),(1,63),(9,55),(10,135)\}. \end{aligned}$$

El siguiente teorema prueba las partes 1 y 7 de la Conjetura 1.4.7, y es más preciso en el sentido de que da una descripción completa para cualquier q.

Teorema 2.3.14. *Sea q una potencia de un número primo p. Sean $a, b \in \mathbb{Z}_+$; sean $r_a, t_a, i_j, f_{a,j}$ como en las Definiciones*1.4.5, 2.3.1, 2.3.9. *Entonces*

$$\Delta(a, b + r_a) - \Delta(a, b) = \sum_{j=0}^{p^m - a} f_{a,j} S_1(a + b + (j + i_j p^m)),$$

En particular, los conjuntos $S(a, b)$ se pueden hallar recursivamente con longitud de recursión r_a, por

$$S(a, b + r_a) = S(a, b) \cup T(a, b + r_a),$$

donde $S(a, b)$ es como se definió en 1.4.4, *y*

$$T(a, b + r_a) = \{(f_{a,j}, a + b + (j + i_j p^m)) \mid 0 \le j \le p^m - a, f_{a,j} \ne 0\},$$

o equivalentemente,

$$T(a, b + r_a) = \{(f_{a,j}, b + r_a - \phi(l_j)) \mid 0 \le j \le p^m - a, f_{a,j} \ne 0\},$$

donde $l_j = (j + i_j p^m)/(q-1)$ y $\phi(l_j) = r_a - a - l_j(q-1)$. La cardinalidad del conjunto $T(a, b + r_a)$ es t_a.

Demostración. De la definición para $\Delta_d(a, b)$, se sigue que

$$\begin{aligned} \Delta_d(a, b) &= \sum_{n_1, n_2 \in A_{d+}} \frac{1}{n_1^a n_2^b} - S_d(a + b) \\ &= \sum_{\substack{n_1 \ne n_2 \\ n_1, n_2 \in A_{d+}}} \frac{1}{n_1^a n_2^b} + \sum_{\substack{n_1 = n_2 \\ n_1 \in A_{d+}}} \frac{1}{n_1^{a+b}} - S_d(a + b) \\ &= \sum_{\substack{n_1 \ne n_2 \\ n_1, n_2 \in A_{d+}}} \frac{1}{n_1^a n_2^b}. \end{aligned}$$

Por lo tanto tenemos

$$\begin{aligned}
\Delta(a,b+r_a) &= \sum_{\substack{n_1\neq n_2\\ n_1,n_2\in A_{1+}}} \frac{1}{n_1^a n_2^{b+r_a}} = \sum_{n_2\in A_{1+}} \frac{1}{n_2^{b+r_a}} \sum_{\substack{n_1\neq n_2\\ n_1\in A_{1+}}} \frac{1}{n_1^a}\\
&= \sum_{n_2\in A_{1+}} \frac{1}{n_2^{b+r_a}} \left(\sum_{n_1\in A_{1+}} \frac{1}{n_1^a} - \frac{1}{n_2^a}\right)\\
&= \sum_{n_2\in A_{1+}} \frac{1}{n_2^{b+r_a}} \left(S_1(a) - \frac{1}{n_2^a}\right)
\end{aligned}$$

Por la Proposición 2.3.12, para cada $n \in A_{1+}$, tenemos

$$g_n = 1 + \sum_{j=1}^{p^m-a} f_{a,j} n^{r_a-(j+i_j p^m)}.$$

Sea $\Sigma = \sum_{j=1}^{p^m-a} f_{a,j} S_1(b+r_a-\phi(l_j))$. Entonces,

$$\begin{aligned}
\Sigma &= \sum_{n_2\in A_{1+}} \sum_{j=1}^{p^m-a} \frac{f_{a,j}}{n_2^{b+r_a-(r_a-a+(j+i_j p^m))}}\\
&= \sum_{n_2\in A_{1+}} \frac{1}{n_2^{b+r_a}} \frac{1}{n_2^a} \sum_{j=1}^{p^m-a} f_{a,j} n_2^{r_a-(j+i_j p^m)}.
\end{aligned}$$

Usando esto llegamos a

$$\begin{aligned}
\Delta(a,b+r_a) - \Sigma &= \sum_{n_2\in A_{1+}} \frac{S_1(a)}{n_2^{b+r_a}} \left(1 - \frac{1}{S_1(a) n_2^a}\left(1 + \sum_{j=1}^{p^m-a} f_{a,j} n_2^{r_a-(j+i_j p^m)}\right)\right)\\
&= \sum_{n_2\in A_{1+}} \frac{S_1(a)}{n_2^{b+r_a}} \left(1 - \frac{1}{S_1(a) n_2^a} g_{n_2}\right)\\
&= \sum_{n_2\in A_{1+}} \frac{S_1(a)}{n_2^{b+r_a}} \left(1 + \frac{1}{S_1(a) n_2^a} \frac{[1]^{p^m-a}}{n_2^{p^m-a}} [1]^a S_1(a)\right)\\
&= \sum_{n_2\in A_{1+}} \frac{S_1(a)}{n_2^{b+r_a}} \left(1 + \frac{[1]^{p^m}}{n_2^{p^m}}\right)\\
&= \sum_{n_2\in A_{1+}} \frac{S_1(a)}{n_2^{b+r_a}} \left(1 + \frac{[1]}{n_2}\right)^{p^m}\\
&= \sum_{n_2\in A_{1+}} \frac{S_1(a)}{n_2^{b+r_a}} \left(n_2^{q-1}\right)^{p^m}\\
&= S_1(a) \sum_{n_2\in A_{1+}} \frac{n_2^{r_a}}{n_2^{b+r_a}}\\
&= S_1(a) S_1(b).
\end{aligned}$$

Por lo tanto, $\Delta(a, b+r_a) - S_1(a)S_1(b) = \Sigma$. De aquí obtenemos

$$\begin{aligned}\Delta(a, b+r_a) - \Delta(a,b) &= \Delta(a, b+r_a) - S_1(a)S_1(b) + S_1(a+b)\\ &= \Sigma + S_1(a+b)\\ &= \sum_{j=1}^{p^m-a} f_{a,j} S_1(b+r_a-\phi(l_j))) + S_1(b+r_a-\phi(0))\\ &= \sum_{j=0}^{p^m-a} f_{a,j} S_1(b+r_a-\phi(l_j)).\end{aligned}$$

Esto prueba que $T(a, b+r_a)$ es exactamente como se afirmó. De la Proposición 2.3.10 se sigue que la cardinalidad de $T(a, b+r_a)$ es precisamente t_a. □

Observaciones 2.3.15.

(1) El conjunto T_a de los pares $(f_{a,j}, \phi(l_j))$ con $f_{a,j} \neq 0$ es claramente independiente de b como se predijo en la Conjetura 1.4.7 (1c) que no tenía una descripción tan precisa como la dada en el teorema.

(2) El número de términos t_a que deben ser añadidos en cada paso de la recursión depende de a, p y q.

Podemos enunciar el teorema anterior en términos de zetas como sigue.

Teorema 2.3.16. *Sea q una potencia de un número primo p. Sean $a, b \in \mathbb{Z}_+$; sean $r_a, t_a, i_j, f_{a,j}$ como en las Definiciones*1.4.5, 2.3.1, 2.3.9. *Si se tiene que*

$$\zeta(a)\zeta(b) = \zeta(a+b) + \zeta(a,b) + \zeta(b,a) + \sum f_i \zeta(a_i, b_i)$$

para algunos $f_i \in \mathbb{F}_p$ y $a_i \in \mathbb{Z}_+$, entonces

$$\begin{aligned}\zeta(a)\zeta(b+r_a) = \zeta(a+b+r_a) + \zeta(a, b+r_a) + \zeta(b+r_a, a) + \sum f_i \zeta(a_i, r_a+b_i)\\ + \sum_{j=0}^{p^m-a} f_{a,j} \zeta(a+b+(j+i_j p^m), r_a - (j+i_j p^m)).\end{aligned}$$

El número de coeficientes $f_{a,j}$ distintos de cero es t_a.

Ejemplos 2.3.17 (Índices especiales grandes, p. 2338 [Tha09b])**.** Sea $q = 2$.

(1) Sea $a = 2^n - 1$. Entonces $m = n$ y $a - 1 = 2 + \cdots + 2^{n-1}$. Como hay exactamente un cero en la descomposición en base 2 de $a-1$ se tiene $t_a = (2-0)^1 = 2$. En cada paso de la recursión se deben añadir dos términos. Más aún, $T_a = \{(1, r_a - a), (1, r_a - a - 1)\}$ porque en este caso $l_j = j$ para $j = 0, 1$.

(2) Si $a = 2^n + 1$, se deben añadir en cada paso de la recursión 2^n términos. Entonces, $m = n + 1$. La descomposición en base 2 de $a - 1$ tiene n ceros así que $t_a = 2^n$. Como en el apartado anterior, para cualquier j, $0 \le j \le 2^n - 1$, $i_j = 0$, y $l_j = j$. Así, $T_a = \{(1, r_a - a - j) \mid 0 \le j \le 2^n - 1\}$.

Ejemplo 2.3.18 (Ejemplo p. 2337, [Tha09b]). Sean $q = 2$ y $a = 19$. Entonces, $m = 5$, $t_{19} = 8$, y $r_{19} = 32$. En este caso, $i_j = 0$, y $l_j = j$ para toda j. Las j's para las cuales $f_{19,j} \neq 0$ son 0, 1, 4, 5, 8, 9, 12, y 13. El polinomio g_t es $g_t = 1 + t^{31} + t^{28} + t^{27} + t^{24} + t^{23} + t^{20} + t^{19}$. Por lo tanto,

$$\begin{aligned}\Delta(19, b+32) - \Delta(19, b) &= \sum_{j=0}^{13} S_1(19+b+j)\\ &= S_1(b+19) + S_1(b+20) + S_1(b+23) + S_1(b+24)\\ &\quad + S_1(b+27) + S_1(b+28) + S_1(b+31) + S_1(b+32).\end{aligned}$$

El siguiente corolario prueba las partes 2, 5 y 6 de la Conjetura 1.4.7.

Corolario 2.3.19. *Seguimos usando la misma notación.*

a) $(1, \phi(0)) = (1, r_a - a) \in T_a$.

b) $T_a = \{(1, \phi(0))\}$ *si y sólo si* $a = p^m$.

c) *Si* $a' = p^{m'}a$, *entonces*

$$T_{a'} = \left\{ \left(f_{a,j}, p^{m'}\phi(l_j)\right) \mid 0 \leq j \leq p^m - a, f_{a,j} \neq 0 \right\}.$$

d) *Si q es primo,*

$$T_a = \left\{ \left(c_{a,l_j}, \phi(l_j)\right) \mid 0 \leq j \leq p^m - a, f_{a,j} \neq 0 \right\}.$$

Demostración. Para probar a), sólo tenemos que notar que $f_{a,0} = 1$.

b) Si $a = p^m$, entonces $g_n = 1$ y así, $T_a = \{(1, r_a - a)\}$. Recíprocamente, dado que $t_a = 1$, de la definición de t_a, se sigue que $a - 1 = \sum_{i=0}^{m-1}(p-1)p^i = p^m - 1$.

c) Sea $a' = p^{m'}a$ para algún entero $m' \in \mathbb{Z}_+$. Entonces, $m + m'$ es el entero más pequeño tal que $a' \leq p^{m+m'}$. Ahora bien,

$$\begin{aligned}-\frac{[1]^{p^{m+m'}}}{n^{p^{m+m'}-a'}} S_1(a') &= \left(-\frac{[1]^{p^m}}{n^{p^m-a}} S_1(a)\right)^{p^{m'}}\\ &= (g_n)^{p^{m'}}\\ &= \left(1 + \sum_{j=1}^{p^m-a} f_{a,j} n^{r_a-(j+i_jp^m)}\right)^{p^{m'}}\\ &= 1 + \sum_{j=1} f_{a,j}^{p^{m'}} n^{p^{m'}(r_a-(j+i_jp^m))}\\ &= 1 + \sum_{j=1} f_{a,j} n^{p^{m'}(r_a-(j+i_jp^m))}.\end{aligned}$$

d) Si q es primo, de la Proposición 2.3.11 se sigue la igualdad $f_{a,j} = c_{a,l_j}$. $\square$

Proposición 2.3.20. *Si* $\binom{r_a-a}{l(q-1)} \neq 0$ *en* $\mathbb{F}_p$ *para algún* l, $0 \leq l \leq j_{a,\text{máx}}$, *entonces existe* j, $0 \leq j \leq p^m - a$, *tal que* $l(q-1) = j + i_j p^m$ *y* $\binom{p^m-a}{j} \neq 0$.

Demostración. Primero notamos que

$$\begin{aligned} q-2 = p^s - 1 - 1 &= (p-1) + (p-1)p + \cdots (p-1)p^{s-1} - 1 \\ &= (p-2) + (p-1)p + \cdots (p-1)p^{s-1}. \end{aligned}$$

Análogamente,

$$\begin{aligned} r_a - a &= p^m - a + p^m(q-1) - p^m \\ &= p^m - a + p^m(q-1-1) \\ &= p^m - a + p^m\big((p-1) + (p-1)p + \cdots (p-1)p^{s-1} - 1\big) \\ &= p^m - a + p^m\big((p-2) + (p-1)p + \cdots (p-1)p^{s-1}\big) \\ &= \sum_{k=0}^{m-1}(p-1-a_k)p^k + (p-2)p^m + \sum_{k=m+1}^{m+s-1}(p-1)p^k. \end{aligned}$$

Sea $l(q-1) = \sum_{k=0}^{m+s-1} b_k p^k$ la descomposición en base p de $l(q-1)$. Dado que $\binom{r_a-a}{l(q-1)} \neq 0$, por el Teorema de Lucas, tenemos que $\binom{p-1-a_k}{b_k} \neq 0$ para $k = 0, 1, \ldots, m-1$ y $\binom{p-2}{b_m} \neq 0$. Por lo tanto, $b_k \leq p - 1 - a_k$ para $k = 0, 1, \ldots, m-1$ y $b_m \leq p-2$. Sea $j = \sum_{k=0}^{m-1} b_k p^k$ y $i = \sum_{k=0}^{s-1} b_{m+k} p^k$. Así, $0 \leq j \leq p^m - a$ y $0 \leq i \leq q-2$. Ya que $j + ip^m = l(q-1) \equiv 0 \text{ mód } (q-1)$, se sigue que $i = i_j$. Puesto que la descomposición en base p de $p^m - a$ es $\sum_{k=0}^{m-1}(p-1-a_k)$, se sigue que $\binom{p^m-a}{j} \neq 0$. □

Observaciones 2.3.21.

(1) Como corolario de la Proposición 2.3.20 tenemos la prueba de la Parte 3 de la Conjetura 1.4.7: Si no hay acarreo en base p en la suma de $l(q-1)$ y $\phi(l)$, entonces $\binom{r_a-a}{l(q-1)} \neq 0$ y así, por la Proposición 2.3.20 y el Teorema 2.2.1, $(f_{a,j}, \phi(l_j))$ pertenece a T_a (note que $l_j = l$).

(2) Observe que $\binom{p^m-a}{j} \neq 0$ y $l(q-1) = j + i_j p^m$ no implica que $\binom{r_a-a}{l(q-1)} \neq 0$. Por ejemplo, si $q = 9$, $a = 17$, y $j = 9$, entonces $r_{17} = 216$ y $\binom{10}{9} = 1$, pero $\binom{199}{144} = 0$. Para otro ejemplo, tome $q = 25$, $a = 103$, y $j = 1$. Entonces, $r_{103} = 3000$ y $\binom{22}{1} = 2$, pero $\binom{2897}{2376} = 0$.

Ejemplo 2.3.22 (Teoremas 3 y 7, [Tha09b])**.** Aquí damos otra prueba de los Teoremas 3 y 7 en [Tha09b] usando el Teorema 2.3.14. Sea $q = 2$.

a) Sea $a = 1$. Entonces $m = 0$, $r_1 = 1$, $g_t = 1$, y $t_1 = 1$. Por el Teorema 2.3.14, tenemos $\Delta(1, b+1) - \Delta(1, b) = S_1(1+b)$. Entonces, $\Delta(1,2) = \Delta(1,1) + S_1(2) = S_1(2)$. Repitiendo este proceso obtenemos $\Delta(1,3) = \Delta(1,2) + S_1(3) = S_1(2) + S_1(3)$. Se sigue que $\Delta(1,b) = \sum_{i=2}^{b} S_1(i)$. Por lo tanto

$$\zeta(1)\zeta(b) = \zeta(1+b) + \sum_{i=1}^{b-1} \zeta(i, b+1-i).$$

b) Sea ahora $a = 2$. Entonces $r_2 = 2$, $g_t = 1$, y $t_2 = 1$. Dado que $\Delta(2,1) = S_1(2)$ y $\Delta(2,2) = 0$, procediendo como en la parte a), se sigue que para b

$$\Delta(2,b) = \begin{cases} \sum_{i=1}^{(b-1)/2} S_1(2i+1) + S_1(2) & \text{si } b \text{ es impar,} \\ \sum_{i=2}^{b/2} S_1(2i) & \text{si } b \text{ es par.} \end{cases}$$

2.4. Fórmulas explícitas

En esta sección daremos una descripción simétrica y una no simétrica para escribir $\zeta(a)\zeta(b)$ como una $\mathbb{F}_p$-combinación lineal de valores multizeta.

Hay una conexión cercana entre las relaciones entre los valores multizeta y la descomposición en fracciones parciales de $\Delta(a,b)$. A partir de la expresión de $\Delta(a,b)$ como una combinación lineal de $S_1(a_i)$'s podemos obtener su descomposición en fracciones parciales y viceversa. Por el Teorema 1.4.1, sabemos que existen $f_i \in \mathbb{F}_p$ y $a_i \in \mathbb{Z}_+$ tales que $\Delta(a,b) = \sum_{i=0}^{\delta} f_i S_1(a_i)$. Podemos suponer sin perder generalidad que $a_0 > a_1 > \cdots > a_\delta$. Entonces:

$$\begin{aligned} \Delta(a,b) &= \sum_{\mu\in\mathbb{F}_q} \left(\frac{f_0}{(t-\mu)^{a_0}} + \frac{f_1}{(t-\mu)^{a_1}} + \cdots + \frac{f_\delta}{(t-\mu)^{a_\delta}} \right) \\ &= \sum_{\mu\in\mathbb{F}_q} \frac{f_0 + f_1(t-\mu)^{a_0-a_1} + \cdots + f_{a_\delta}(t-\mu)^{a_0-a_\delta}}{(t-\mu)^{a_0}} \\ &= \sum_{\mu\in\mathbb{F}_q} \frac{h_\mu(t)}{(t-\mu)^{a_0}} \end{aligned} \tag{2.4.0.1}$$

donde $h_\mu(t) = f_0 + f_1(t-\mu)^{a_0-a_1} + \cdots + f_{a_\delta}(t-\mu)^{a_0-a_\delta}$. Luego, (2.4.0.1) es la descomposición en fracciones parciales de $\Delta(a,b)$. La unicidad de esta descomposición nos garantiza la unicidad de los f_i's.

Proposición 2.4.1. *Sea q una potencia de un primo p. Sean $a, b \in \mathbb{Z}_+$. Entonces, la descomposición en fracciones parciales de $\Delta(a,b)$ es de la forma*

$$\Delta(a,b) = \sum_{\mu\in\mathbb{F}_q} \frac{f(t-\mu)}{(t-\mu)^n}, \tag{2.4.1.1}$$

para algún n, donde $f(t) = f_0 + f_1 t + \cdots + f_{n-1}t^{n-1} \in \mathbb{F}_p[t]$ es primo relativo a t. También,

$$\Delta(a,b) = \sum_{i=0}^{n-1} f_i S_1(n-i).$$

Demostración. Para cualesquiera enteros positivos a, b, $\Delta(a,b)$ es un polinomio en $1/[1]$ con coeficientes en $\mathbb{F}_p$ de grado menor que $a+b$. Dado que $k+1-\lfloor k/q \rfloor (q-1) > 0$, tenemos

$$S_1(k+1) = \frac{(-1)^{k+1}}{[1]^{k+1}} \left(1 + \sum_{k_1=1}^{\lfloor k/q \rfloor} \binom{k-k_1(q-1)}{k_1} (-1)^{k_1} [1]^{k_1(q-1)} \right)$$

es un polinomio en $1/[1]$ sin término constante. Por lo tanto, $\Delta(a,b)$ es cero o es un polinomio en $1/[1]$, distinto de cero, con coeficientes en $\mathbb{F}_p$, que no tiene término constante y de grado menor que $a+b$. Si $\Delta(a,b)\neq 0$, escribimos

$$\Delta(a,b)=\frac{\theta_n+\theta_{n-1}[1]+\cdots+\theta_1[1]^{n-1}}{[1]^n}=\frac{P_1(t)}{Q_1(t)}, \tag{2.4.1.2}$$

donde $P_1(t)=\theta_n+\theta_{n-1}[1]+\cdots+\theta_1[1]^{n-1}$, $Q_1(t)=[1]^n$, $\theta_i\in\mathbb{F}_p$, $\theta_n\neq 0$, y $n<a+b$. Ya que $P_1(\mu)=\theta_n\neq 0$ para toda $\mu\in\mathbb{F}_q$, $P_1(t)$ y $Q_1(t)$ son primos relativos. Como $\Delta(a,b)$ es un elemento de K, tiene una única descomposición en fracciones parciales de la forma:

$$\Delta(a,b)=\sum_{\mu\in\mathbb{F}_q}\frac{h_\mu(t)}{(t-\mu)^n},$$

donde $h_\mu(t)\in\mathbb{F}_q[t]$ es primo relativo con $t-\mu$ y $\deg h_\mu<n$. Ahora bien, $\Delta(a,b)$ es invariante respecto de los automorfismos $t\to t+\theta$, $\theta\in\mathbb{F}_q$, de A. Por la unicidad de la descomposición en fracciones parciales tenemos que $h_0(t)=h_\theta(t+\theta)$ para cualquier $\theta\in\mathbb{F}_q$. Entonces, como polinomio en $t-\mu$, h_μ tiene los mismos coeficientes que h_0. Sea $f(t)=h_0(t)=f_0+f_1t+\cdots+f_{n-1}t^{n-1}$. Entonces,

$$\begin{aligned}\Delta(a,b)&=\sum_{\mu\in\mathbb{F}_q}\frac{h_\mu(t)}{(t-\mu)^n}\\&=\sum_{\mu\in\mathbb{F}_q}\frac{h_0(t-\mu)}{(t-\mu)^n}\\&=\sum_{\mu\in\mathbb{F}_q}\sum_{i=0}^{n-1}\frac{f_i(t-\mu)^i}{(t-\mu)^n}\\&=\sum_{\mu\in\mathbb{F}_q}\sum_{i=0}^{n-1}\frac{f_i}{(t-\mu)^{n-i}}\\&=\sum_{i=0}^{n-1}f_i\sum_{\mu\in\mathbb{F}_q}\frac{1}{(t-\mu)^{n-i}}\\&=\sum_{i=0}^{n-1}f_iS_1(n-i).\end{aligned}$$

Por la unicidad de las f_i's y por el Teorema 1.4.1, se sigue que $f_i\in\mathbb{F}_p$. □

Por lo anterior, para expresar $\Delta(a,b)$ como una $\mathbb{F}_p$-combinación lineal de $S_1(a_i)$'s, es suficiente encontrar su descomposición en fracciones parciales. Para hacer esto, procedemos como sigue. Los polinomios t^n y $[1]^n/t^n$ son primos relativos y de aquí que $[1]^n/t^n$ es una unidad módulo t^n. De (2.4.1.1) se sigue que

$$[1]^n\Delta(a,b)=\sum_{\mu\in\mathbb{F}_q}\frac{[1]^n}{(t-\mu)^n}f(t-\mu).$$

Por lo tanto, módulo t^n tenemos que $[1]^n\Delta(a,b) = \frac{[1]^n}{t^n} f(t)$. Luego, módulo t^n tenemos que

$$f(t) = ([1]^n\Delta(a,b) \text{ mód } t^n)\left(\frac{[1]^n}{t^n} \text{ mód } t^n\right)^{-1}.$$

Observación 2.4.2. Note que a priori, no conocemos el valor de n. Más adelante explicaremos cómo tratar este problema (Proposición 2.4.14).

Ejemplo 2.4.3. Sean $q = 3$, $a = 4$, $b = 5$. Un cálculo directo nos muestra que

$$\Delta(4,5) = \frac{1}{[1]^5} = \frac{1}{t^5(t+1)^5(t+2)^5}.$$

Entonces $n = 5$. Así, módulo t^5

$$\begin{aligned} f(t) &= \left([1]^5\Delta(4,5) \text{ mód } t^5\right)\left(\frac{[1]^5}{t^5} \text{ mód } t^5\right)^{-1} \\ &= 1 \cdot \left(t^{10} + t^8 + t^6 + 2t^4 + 2t^2 + 2 \text{ mód } t^5\right)^{-1} \\ &= \left(2t^4 + 2t^2 + 2 \text{ mód } t^5\right)^{-1} \\ &= (t^2 + 2) \text{ mód } t^5. \end{aligned}$$

Luego $f(t) = t^2 + 2$. Así, la descomposición en fracciones parciales de $\Delta(4,5)$ es

$$\begin{aligned} \Delta(4,5) &= \sum_{\mu\in\mathbb{F}_3} \frac{(t-\mu)^2 + 2}{(t-\mu)^5} \\ &= \sum_{\mu\in\mathbb{F}_3} \left(\frac{2}{(t-\mu)^5} + \frac{1}{(t-\mu)^3}\right) \\ &= \frac{2}{t^5} + \frac{1}{t^3} + \frac{2}{(t+1)^5} + \frac{1}{(t+1)^3} + \frac{2}{(t+2)^5} + \frac{1}{(t+2)^3} \\ &= 2S_1(5) + S_1(3). \end{aligned}$$

Ejemplo 2.4.4. Sean $q = 3$, $a = 13$ y $b = 14$. Entonces

$$\Delta(13,14) = \frac{1}{[1]^{11}}.$$

Así, en este caso, $n = 11 < a, b$. El inverso módulo t^{11} de $[1]^{11}/t^{11}$ es $t^8 + 2t^6 + t^2 + 2$. Luego, $f(t) = t^8 + 2t^6 + t^2 + 2$. Por lo tanto

$$\Delta(13,14) = 2S_1(11) + S_1(9) + 2S_1(5) + S_1(3).$$

Antes de explicar el caso general, explicaremos primero el caso $q = 2$, que es cuando podemos simplificar significativamente las cuentas y obtener una expresión relativamente sencilla. Sabemos que si $a = b$, entonces $\Delta(a,b) = 0$ [Tha09b, Teorema 8]. Por definición, $S(a,b) = S(b,a)$; así, podemos suponer sin pérdida de generalidad que $a > b$.

Teorema 2.4.5. *Sea $q = 2$. Si $a > b \geq 1$, entonces*

$$\zeta(a)\zeta(b) - \zeta(a+b) - \zeta(a,b) - \zeta(b,a) = \sum_{k=0}^{a-1} f_k \zeta(a-k, b+k)$$

donde

$$f_k = \sum_{\substack{i+j=k \\ i \leq 2^m - a \\ j \leq a-b-1}} \binom{2^m - a}{i} \binom{a-b}{j},$$

y m es el entero más pequeño tal que $a \leq 2^m$.

Demostración. De acuerdo con el Teorema 1.4.2, es suficiente probar que

$$\Delta(a,b) = \sum_{k=0}^{a-1} f_k S_1(a-k).$$

Como $a > b$,

$$\Delta(a,b) = \frac{1}{t^a (t+1)^b} + \frac{1}{(t+1)^a t^b} = \frac{(t+1)^{a-b} + t^{a-b}}{t^a (t+1)^a} = \frac{S_1(b-a)}{[1]^a}.$$

El grado del numerador de $\Delta(a,b)$ es menor que $a - b$ y, por lo tanto, menor que el grado del denominador. A continuación, aplicamos el método explicado previamente para escribir $\Delta(a,b)$ como una suma $\frac{h_0(t)}{t^a} + \frac{h_0(t-1)}{(t-1)^a}$. Puesto que $(t+1)^{p^m - a}(t+1)^a \equiv 1 \text{ mód } t^a$ tenemos que $(t+1)^{2^m - a} \text{ mód } t^a$ es el inverso de $(t+1)^a \text{ mód } t^a$. Entonces, $h_0(t) \text{ mód } t^a = (t+1)^{2^m - a} S_1(b-a) \text{ mód } t^a$. El único representante de grado menor que a de $(t+1)^{2^m - a} \text{ mód } t^a$ es $(t+1)^{2^m - a}$ ya que $a > 2^{m-1}$. El único representante de grado menor que a de $S_1(b-a) \text{ mód } t^a$ es $S_1(b-a)$. Ahora,

$$(t+1)^{2^m - a} = \sum_{i=0}^{2^m - a} \binom{2^m - a}{i} t^i,$$

$$S_1(b-a) = t^{a-b} + (t+1)^{a-b} = \sum_{j=0}^{a-b-1} \binom{a-b}{j} t^j.$$

El grado de $(t+1)^{2^m - a} S_1(b-a)$ es a lo más $2^m - b - 1$. Tomando como $h_0(t)$ el resto de $(t+1)^{2^m - a} S_1(b-a)$ al ser dividido por t^a obtenemos

$$h_0(t) = \sum_{k=0}^{a-1} f_k t^k$$

donde

$$f_k = \sum_{\substack{i+j=k \\ i \leq p^m - a \\ j \leq a-b-1}} \binom{p^m - a}{i} \binom{a-b}{j}.$$

$\square$

Observaciones 2.4.6.

(1) Observe que $S(a,b) = \{(f_k, a-k) \mid f_k \neq 0,\ 0 \leq k \leq a-1\}$.

(2) Si $b \geq 2^m - a$, entonces $2^m - b - 1 < a$ y por lo tanto, no es necesario dividir por t^a.

(3) Si $k = 0$, entonces $i = j = 0$ y $f_0 = \binom{2^m-a}{0}\binom{a-b}{0} = 1$.

Ejemplo 2.4.7 (Ambos índices grandes, [Tha09b, p. 2338])**.** Usaremos el Teorema 2.4.5 para probar dos conjeturas formuladas por Thakur. Sea $q = 2$.

a) Sean $a = 2^n + 1$ y $b = 2^n - 1$. Entonces,

$$\Delta_d(a,b) = \sum_{i=2}^{2^n+1} S_d(i, 2^n + 1 - i).$$

b) Sean $a = 2^n + 1$ y $b = 2^{n-1}$. Entonces,

$$\Delta_d(a,b) = S_d(a,b) + \sum_{i=2}^{2^{n-1}+1} S_d(i, 3 \cdot 2^{n-1} + 1 - i).$$

Demostración. De acuerdo con el Teorema 1.4.2, será suficiente probar las igualdades para el caso $d = 1$.

a) En este caso, $m = n+1$, $p^m - a = 2^n - 1$, y $a - b - 1 = 1$. Para $k = 1, \ldots, 2^n - 1$,

$$\begin{aligned} f_k &= \sum_{\substack{j=0 \\ k-j \leq 2^n-1 \\ j \leq 1}}^{k} \binom{2^n-1}{k-j}\binom{2}{j} \\ &= \binom{2^n-1}{k}\binom{2}{0} + \binom{2^n-1}{k-1}\binom{2}{1} \\ &= \binom{2^n-1}{k}\binom{2}{0} \\ &= 1, \end{aligned}$$

porque $\binom{2}{1}$ es cero módulo 2 y $\binom{2^n-1}{k} = 1$ de acuerdo con la Proposición 2.3.7 (a). Para $k = a - 1 = 2^n$,

$$f_{a-1} = \binom{2^n-1}{2^n-1}\binom{2}{1} = 0.$$

Del Teorema 2.4.5, obtenemos

$$\Delta(2^n+1, 2^n-1) = \sum_{k=0}^{2^n-1} S_1(2^n + 1 - k) = \sum_{k=2}^{2^n+1} S_1(k).$$

b) Ahora, $m = n+1$, $p^m - a = 2^n - 1$, y $a - b = 2^{n-1} + 1$. Examinando las descomposiciones en base 2 de j y $2^{n-1} + 1$, y usando el Teorema de Lucas, vemos que los valores de j, $0 \leq j \leq 2^{n-1}$, tales que $\binom{2^{n-1}+1}{j} \neq 0$ son $j = 0, 1, 2^{n-1}$. Por otro lado, $\binom{2^n-1}{i} \neq 0$ para $i = 0, 1, \ldots, 2^n - 1$. Ya sabemos que $f_0 = 1$. Para $k = 1, \ldots, 2^n$,

$$f_k = \sum_{\substack{j=0 \\ i \leq 2^n - 1 \\ j \leq 2^{n-1}+1}}^{k} \binom{2^n - 1}{k - j}\binom{2^{n-1} + 1}{j}.$$

Para $1 \leq k \leq 2^n - 1$, tenemos que

$$f_k = \binom{2^n - 1}{k}\binom{2^{n-1} + 1}{0} + \binom{2^n - 1}{k - 1}\binom{2^{n-1} + 1}{1} + \binom{2^n - 1}{k - 2^{n-1}}\binom{2^{n-1} + 1}{2^{n-1}}.$$

Por lo tanto, $f_k = 0$ para $1 \leq k < 2^{n-1}$ y $f_k = 1$ para $2^{n-1} \leq k \leq 2^n - 1$. Si $k = a - 1 = 2^n$,

$$f_k = \binom{2^n - 1}{k - 1}\binom{2^{n-1} + 1}{1} + \binom{2^n - 1}{k - 2^{n-1}}\binom{2^{n-1} + 1}{2^{n-1}} = 0.$$

Se sigue que $S(a, b) = \{(f_0, a - 0)\} \cup \big\{(f_k, a - k) \mid 2^{n-1} \leq k \leq 2^n - 1\big\}$. Entonces

$$\begin{aligned}\Delta(a, b) &= S_1(2^n + 1) + \sum_{k=2^{n-1}}^{2^n - 1} S_1(2^n + 1 - k) \\ &= S_1(2^n + 1) + \sum_{k=2}^{2^{n-1}+1} S_1(k).\end{aligned}$$ □

Algunos casos especiales del Teorema 2.4.5 vienen en el siguiente corolario.

Corolario 2.4.8. *Sea $q = 2$.*

a) *Si $b < 2^m$, entonces*

$$\zeta(2^m)\zeta(b) - \zeta(2^m + b) - \zeta(2^m, b) - \zeta(b, 2^m) = \sum_{k=0}^{2^m - b - 1} \binom{2^m - b}{k}\zeta(2^m - k, b + k).$$

Si no hay acarreo en base 2 en la suma de k y $b - 1$ tenemos que $\binom{2^m - b}{k} \neq 0$.

b) *Si $a \geq 2$, entonces*

$$\begin{aligned}&\zeta(a)\zeta(a - 1) - \zeta(2a - 1) - \zeta(a, a - 1) - \zeta(a - 1, a) \\ &\qquad = \sum_{k=0}^{2^m - a} \binom{2^m - a}{k}\zeta(a - k, a - 1 - k),\end{aligned}$$

donde m es el entero más pequeño tal que $a \leq 2^m$. El número de coeficientes distintos de cero es t_a.

Demostración. a) De acuerdo con el Teorema 1.4.2, es suficiente probar que

$$\Delta(2^m, b) = \sum_{k=0}^{2^m-b-1} \binom{2^m - b}{k} S_1(2^m - k).$$

Si $a = 2^m$, entonces $i = 0$ y $\binom{2^m-a}{0} = 1$. Así, $f_k = \binom{2^m-b}{k}$ para $0 \leq k \leq 2^m - b - 1$. Sean $b - 1 = b_0 + b_1 2 + \cdots + b_{m-1} 2^{m-1}$ y $k = k_0 + k_1 2 + \cdots + k_{m-1} 2^{m-1}$ las descomposiciones en base 2 de $b-1$ y k, respectivamente. Entonces, la descomposición en base 2 de $2^m - b$ es $\sum(1 - b_l)2^l$. Si $k \leq 2^m - b - 1$ y no existe acarreo base 2 en la suma de k y $b - 1$, entonces $f_k \neq 0$ en virtud del Teorema de Lucas.

b) Es suficiente probar que

$$\Delta(a, a-1) = \sum_{k=0}^{2^m-a} \binom{2^m - a}{k} S_1(a - k).$$

Si $b = a - 1$, entonces $a - b - 1 = 0$ y así, $j = 0$. Por lo tanto, $f_k = \binom{2^m-a}{k}$ para $0 \leq k \leq 2^m - a$. En este caso especial, el número de $f_k \neq 0$ es t_a por la Proposición 2.3.7 (c). □

Ejemplo 2.4.9. Usaremos el Corolario 2.4.8 para probar las siguientes conjeturas [Tha09b, Sección 4.1.3]:

$$\Delta_d(2^n, 2^n - 1) = S_d(2^n, 2^n - 1) \tag{2.4.9.1}$$

$$\Delta_d(2^n + 1, 2^n) = \sum_{i=2}^{2^n+1} S_d(i, 2^{n+1} + 1 - i). \tag{2.4.9.2}$$

Cuando $l < n - 1$,

$$\Delta_d(2^n - 2^l, 2^n - 2^l - 1) = S_d(2^n - 2^l, 2^n - 2^l - 1) + S_d(2^n - 2^{l+1}, 2^n - 1). \tag{2.4.9.3}$$

De acuerdo con el Teorema 1.4.2, en todos los casos, es suficiente probar (2.4.9.1), (2.4.9.2) y (2.4.9.3) para $d = 1$. La Conjetura 2.4.9.1 se sigue inmediatamente ya sea de *a*) o *b*) del Corolario 2.4.8, tomando $a = 2^n$ y $b = a - 1$. Para la Conjetura 2.4.9.2, tomemos $a = 2^n + 1$ y $b = 2^n$. Entonces $m = n + 1$. Por la Proposición 2.3.11 (b), tenemos $\binom{2^n-1}{k} = 1$ para $k = 0, 1, \ldots, 2^n - 1$. Luego,

$$\Delta(2^n + 1, 2^n) = \sum_{k=0}^{2^n-1} S_1(2^n + 1 - k) = \sum_{k=2}^{2^n+1} S_1(k).$$

Finalmente, para la Conjetura 2.4.9.3, sean $a = 2^n - 2^l$ y $b = a - 1$. Entonces $m = n$ y $p^m - a = 2^l$. Así,

$$\Delta(a, b) = \sum_{k=0}^{2^l} \binom{2^l}{k} S_1(a - k) = S_1(2^n - 2^l) + S_1(2^n - 2^l - 2^l) + \sum_{k=1}^{2^l-1} \binom{2^l}{k} S_1(a - k).$$

La valuación 2-ádica de $\binom{2^l}{k}$ es $\ell(k) + \ell(2^l - k) - \ell(2^l)$, donde $\ell(k)$ es la suma de los dígitos de k en base $q = 2$. Ya que $k \neq 0$ y $2^l - k \neq 0$, tenemos que $\ell(k) + \ell(2^l - k) - \ell(2^l) \geq 1 + 1 - 1 = 1$ y $\binom{2^l}{k} = 0$ para $k = 1, \ldots, 2^l - 1$ y se sigue el resultado.

Ejemplo 2.4.10. Continuamos con el Ejemplo 2.3.18. Calculemos $S(19,20)$. Sean $a = 20$ y $b = 19$. Entonces $m = 5$ y $a-b-1 = 0$. Entonces, $f_k = \binom{12}{k}$ para $k = 0, 1, \ldots, 12$. Las k's para las cuales $f_k \neq 0$ son $0, 4, 8$ y 12. Entonces $S(19,20) = S(20,19) = \{(1,20), (1,16), (1,12), (1,8)\}$. La cardinalidad de $S(19,20)$ es $4 = t_{20}$.

Ahora daremos fórmulas explicitas para el producto de valores zeta que generalizan el caso $q = 2$.

Teorema 2.4.11. *Sea q una potencia de un primo p. Sean $a, b \in \mathbb{Z}_+$ tales que $a \geq b \geq 1$; sea m el entero más pequeño tal que $a \leq p^m$. Entonces*

$$\zeta(a)\zeta(b) - \zeta(a+b) - \zeta(a,b) - \zeta(b,a) = \sum_{i=0}^{a-1} f_i \zeta(a-i, b+i),$$

donde $f(t) := f_0 + f_1 t + \cdots + f_{a-1}t^{a-1} \in \mathbb{F}_p[t]$ está dado por

$$-\left(t^{q-1}-1\right)^{p^m-a} \sum_{\theta \in \mathbb{F}_q} \sum_{\mu \in \mathbb{F}_q^*} \left(\sum_{j=1}^{q-1} \mu^{q-1-j} (t+\theta)^{j-1} \right)^a (t+\theta-\mu)^{a-b} \text{ mód } t^a.$$

Equivalentemente, $f(t)$ está dado por

$$\sum_{i_3=0}^{p^m-a} \sum_{k} \sum_{i_1=0}^{a-b} \sum_{i_2=0}^{\sigma(k)+i_1-1} \binom{p^m-a}{i_3} \binom{a}{k_1, \ldots, k_{q-1}} \binom{a-b}{i_1} \binom{\sigma(k)+i_1}{i_2} \times (-1)^{b+i_1+i_3} t^{i_2+i_3(q-1)}, \quad (2.4.11.1)$$

donde la segunda suma se toma sobre todos las $(q-1)$-adas $k = (k_1, \ldots, k_{q-1})$ de enteros no negativos tales que $k_1 + \cdots + k_{q-1} = a$; $\sigma(k) = \sum_{j=1}^{q-1}(j-1)k_j$, $\tau(k) = \sum_{j=1}^{q-1}(q-1-j)k_j$; los índices i_1, i_2, i_3 están sujetos a las condiciones $i_2 + i_3(q-1) < a$ y

$$(\sigma(k) + i_1 - i_2) \equiv 0 \text{ mód } (q-1),$$
$$(\tau(k) + a - b - i_1) \equiv 0 \text{ mód } (q-1).$$

Demostración. De acuerdo con el Teorema 1.4.2, es suficiente probar que

$$\Delta(a,b) = \sum_{i=0}^{a-1} f_i S_1(a-i).$$

Tenemos que

$$\begin{aligned} \Delta(a,b) &= \sum_{\theta \in \mathbb{F}_q} \sum_{\mu \in \mathbb{F}_q^*} \frac{1}{(t+\theta)^a (t+\theta-\mu)^b} \\ &= \frac{1}{[1]^a} \sum_{\theta \in \mathbb{F}_q} \sum_{\mu \in \mathbb{F}_q^*} \frac{[1]^a}{(t+\theta)^a (t+\theta-\mu)^a} (t+\theta-\mu)^{a-b} \\ &= \frac{P(t)}{Q(t)}, \end{aligned} \quad (2.4.11.2)$$

donde

$$P(t) = \sum_{\theta \in \mathbb{F}_q} \sum_{\mu \in \mathbb{F}_q^*} \frac{[1]^a}{(t+\theta)^a (t+\theta-\mu)^a} (t+\theta-\mu)^{a-b} \in \mathbb{F}_q[t]$$

$Q(t) = [1]^a$, $\deg P(t) \leq a(q-2)+a-b$, y $\deg Q(t) = aq$. En particular, $\deg P < \deg Q$. Comparando (2.4.1.2) y (2.4.11.2), obtenemos $PQ_1 = P_1 Q$. Entonces, Q_1 divide a $P_1 Q$ y por tanto $Q_1 \mid Q$ ya que Q_1 y P_1 son primos relativos. Entonces $n \leq a$ y $P(t)$ es un polinomio en $[1]$ de grado menor que a. Por lo tanto la descomposición en fracciones parciales de $\Delta(a,b)$ es de la forma

$$\Delta(a,b) = \sum_{\mu \in \mathbb{F}_q} \frac{f(t-\mu)}{(t-\mu)^n}, \tag{2.4.11.3}$$

donde $f(t) \in \mathbb{F}_p[t]$ es primo relativo a t^n, y $\deg f < n$. De (2.4.11.3) se sigue que

$$[1]^a \Delta(a,b) \text{ mód } t^a = \left(t^{a-n} g(t) \text{ mód } t^a\right) \left(\frac{[1]^a}{t^a} \text{ mód } t^a\right).$$

Dado que $[1]^a/t^a$ es una unidad módulo t^a, éste tiene un inverso módulo t^a. Por lo tanto,

$$t^{a-n} g(t) \text{ mód } t^a = ([1]^a \Delta(a,b) \text{ mód } t^a) \left(\frac{[1]^a}{t^a} \text{ mód } t^a\right)^{-1}.$$

Tenemos

$$\frac{[1]^{p^m-a}}{t^{p^m-a}} \frac{[1]^a}{t^a} = \frac{[1]^{p^m}}{t^{p^m}} = \left(t^{q-1}-1\right)^{p^m} = t^{r_a} - 1,$$

y $a \leq r_a$, entonces $-\left(t^{r_a}-1\right) \text{ mód } t^a = 1 \text{ mód } t^a$. De aquí que,

$$\left(\frac{[1]^a}{t^a} \text{ mód } t^a\right)^{-1} = -\frac{[1]^{p^m-a}}{t^{p^m-a}} \text{ mód } t^a = -\left(t^{q-1}-1\right)^{p^m-a} \text{ mód } t^a.$$

Ahora,

$$-\left(t^{q-1}-1\right)^{p^m-a} = \sum_{i_3=0}^{p^m-a} \binom{p^m-a}{i_3} t^{(q-1)i_3} (-1)^{(p^m-a-i_3+1)}. \tag{2.4.11.4}$$

A continuación calcularemos $[1]^a \Delta(a,b)$. Sean $\theta, \mu \in \mathbb{F}_q$, con $\mu \neq 0$. Ahora

$$\begin{aligned}
\frac{[1]}{(t+\theta)(t+\theta-\mu)} &= \frac{(t+\theta-\mu)^{q-1}-1}{t+\theta} \\
&= \frac{1}{t+\theta}\left(\sum_{j=0}^{q-1} \binom{q-1}{j} (t+\theta)^j (-\mu)^{q-1-j} - 1\right) \\
&= \frac{1}{t+\theta} \sum_{j=1}^{q-1} (-1)^j (t+\theta)^j (-1)^{q-1-j} \mu^{q-1-j} \\
&= \sum_{j=1}^{q-1} \mu^{q-1-j} (t+\theta)^{j-1}.
\end{aligned}$$

Tenemos que $(t+\theta)^{\sigma(k)} = \prod_{j=1}^{q-1}(t+\theta)^{(j-1)k_j}$ ya que $\sigma(k) = \sum_{j=1}^{q-1}(j-1)k_j$. El Teorema Multinomial implica

$$\frac{[1]^a}{(t+\theta)^a(t+\theta-\mu)^a} = \sum_{k_1+\cdots+k_{q-1}=a} \binom{a}{k_1,\ldots,k_{q-1}} \mu^{\tau(k)}(t+\theta)^{\sigma(k)},$$

donde $\tau(k) = \sum_{j=1}^{q-1}(q-1-j)k_j$. Dado que

$$(t+\theta-\mu)^{a-b} = \sum_{i_1=0}^{a-b} \binom{a-b}{i_1} (t+\theta)^{i_i} (-\mu)^{a-b-i_1},$$

se sigue que

$$\frac{[1]^a}{(t+\theta)^a(t+\theta-\mu)^b} = \sum_k \sum_{i_1=0}^{a-b} \binom{a}{k}\binom{a-b}{i_1}(-1)^{a-b-i_1}\mu^{\tau(k)+a-b-i_1}(t+\theta)^{\sigma(k)+i_1},$$

donde $\binom{a}{k}$ denota al coeficiente multinomial $\binom{a}{k_1,\ldots,k_{q-1}}$. Puesto que $\sum_{\theta\in\mathbb{F}_q^*} 1 = -1$, notamos que

$$\begin{aligned}
\sum_{\theta\in\mathbb{F}_q}(t+\theta)^{\sigma(k)+i_1} &= t^{\sigma(k)+i_1} + \sum_{\theta\in\mathbb{F}_q^*}(t+\theta)^{\sigma(k)+i_1} \\
&= t^{\sigma(k)+i_1} + \sum_{\theta\in\mathbb{F}_q^*}\sum_{i_2=0}^{\sigma(k)+i_1} \binom{\sigma(k)+i_1}{i_2} t^{i_2}\theta^{\sigma(k)+i_1-i_2} \\
&= t^{\sigma(k)+i_1} + \sum_{i_2=0}^{\sigma(k)+i_1} \left(\sum_{\theta\in\mathbb{F}_q^*}\theta^{\sigma(k)+i_1-i_2}\right) \binom{\sigma(k)+i_1}{i_2} t^{i_2} \\
&= \sum_{i_2=0}^{\sigma(k)+i_1-1} \left(\sum_{\theta\in\mathbb{F}_q^*}\theta^{\sigma(k)+i_1-i_2}\right) \binom{\sigma(k)+i_1}{i_2} t^{i_2}.
\end{aligned}$$

Por lo tanto,

$$\begin{aligned}
[1]^a\Delta(a,b) = \sum_k \sum_{i_1=0}^{a-b} \sum_{i_2=0}^{\sigma(k)+i_1-1} &\left(\sum_{\mu\in\mathbb{F}_q^*}\mu^{\tau(k)+a-b+i_1}\right)\left(\sum_{\theta\in\mathbb{F}_q^*}\theta^{\sigma(k)+i_1-i_2}\right) \\
&\times \binom{a}{k}\binom{a-b}{i_1}\binom{\sigma(k)+i_1}{i_2}(-1)^{a-b-i_1}t^{i_2}.
\end{aligned}$$

Usando la Ecuación (2.4.11.4) y el hecho que $\sum_{\xi\in\mathbb{F}_q^*}\xi^l$ es 0 si $q-1$ no divide a l, y -1 si $l\geq 0$ es divisible por $q-1$, obtenemos que $h(t) = t^{a-n}f(t)$ es igual a

$$\sum_{i_3}^{p^m-a}\sum_k\sum_{i_1}^{a-b}\sum_{i_2}^{\sigma(k)+i_1-1} \binom{p^m-a}{i_3}\binom{a}{k}\binom{a-b}{i_1}\binom{\sigma(k)+i_1}{i_2}(-1)^{b+i_1+i_3}t^{i_2+i_3(q-1)},$$

donde la segunda suma se toma sobre todas las $(q-1)$-adas $k = (k_1, \ldots, k_{q-1})$ de enteros no negativos tales que $k_1 + \cdots + k_{q-1} = a$, $\sigma(k)$, y $\tau(k)$, a, b, i_1, i_2 e i_3 satisfacen que $\sigma(k) + i_1 - i_2$ y $\tau(k) + a - b - i_1$ son "pares", e $i_2 + i_3(q-1) < a$. Sea $v_t(\cdot)$ la valuación en t. Dado que $f(t)$ y t^n son primos relativos tenemos que $v_t(f) = 0$. Luego $a - n = v_t(h)$. Por lo tanto, para obtener $f(t)$ solamente dividimos a $h(t)$ por $t^{v_t(h)}$. Sean $f(t) = f_0 + f_1 t + \cdots + f_{n-1} t^{n-1}$ y $h(t) = h_0 + h_1 t + \cdots + h_{a-1} t^{a-1}$, entonces $h_j = 0$ para $j = 0, \ldots a-n-1$ y $h_{a-n+j} = f_j$ para $j = 0, \ldots, n-1$. □

Observaciones 2.4.12.

(1) De la prueba del teorema tenemos que para cualesquiera $a, b \in \mathbb{Z}_+$, $\Delta(a, b)$ es un polinomio en $1/[1]$ de grado menor o igual que $\max\{a, b\}$.

(2) Sea $q = 2$. Entonces, $a > 2^m - a$ porque $a > 2^{m-1}$. El único coeficiente multinomial es $\binom{a}{a} = 1$, y así, $\sigma(k) = 0 = \tau(k)$. Tenemos que

$$\sum_{\theta \in \mathbb{F}_q} (t + \theta - 1)^{a-b} = \sum_{\theta \in \mathbb{F}_q} (t + \theta)^{a-b} = \sum_{i_1=0}^{a-b-1} \binom{a-b}{i_1} t^{i_1}.$$

Por otro lado,

$$\begin{aligned} \sum_{\theta \in \mathbb{F}_q} (t + \theta - 1)^{a-b} &= \sum_{\theta \in \mathbb{F}_q} \sum_{i_1=0}^{a-b} \binom{a-b}{i_1} (t+\theta)^{i_1} \\ &= \sum_{i_1=0}^{a-b} \sum_{\theta \in \mathbb{F}_q} \binom{a-b}{i_1} (t+\theta)^{i_1} \\ &= \sum_{i_1=0}^{a-b} \sum_{i_2=0}^{i_1-1} \binom{a-b}{i_1} \binom{i_1}{i_2} t^{i_2}. \end{aligned}$$

Entonces,

$$\sum_{i_1=0}^{a-b-1} \binom{a-b}{i_1} t^{i_1} = \sum_{i_1=0}^{a-b} \sum_{i_2=0}^{i_1-1} \binom{a-b}{i_1} \binom{i_1}{i_2} t^{i_2}.$$

Por lo tanto, en la Ecuación (2.4.11.1) en vez de cuatro sumas y cuatro coeficientes multinomiales, tenemos dos sumas y dos coeficientes binomiales y la fórmula se reduce a la fórmula que obtuvimos previamente para $q = 2$.

(3) Por el Teorema de Lucas tenemos que los coeficientes binomiales o multinomiales en (2.4.11.1) son cero si hay acarreo en base p en la suma correspondiente. Así solamente necesitan ser tomados en consideración aquellos términos en los que no hay acarreo en base p.

Ya se ha probado en la Sección 2.2 la conjetura relativa a la paridad formulada por D. Thakur [Tha09b, 5.3]. Como corolario del Teorema 2.4.11, damos otra prueba de esta conjetura.

Corolario 2.4.13. *Sea q una potencia de p; sean $a \geq b \geq 1$. Dados $a, b \in \mathbb{Z}_+$, con $a \geq b \geq 1$, existen $f_i \in \mathbb{F}_p$ y $i \in \mathbb{Z}_+$ tales que*

$$\zeta(a)\zeta(b) - \zeta(a+b) - \zeta(a,b) - \zeta(b,a) = \sum f_i \zeta(a-i, b+i),$$

donde cada $b+i$ es "par".

Demostración. Cada i es de la forma $i_2 + i_3(q-1)$. Dado que las dos sumas $\sum_{j=1}^{q-1}(j-1)k_j + i_1 - i_2$ y $\sum_{j=1}^{q-1}(q-1-j)k_j + a - b - i_1$ son "pares", y $\sum_{j=1}^{q-1}(j-1)k_j + \sum_{j=1}^{q-1}(q-1-j)k_j + a = a(q-1)$, se sigue que $a(q-1)-(b+i_2)$ es "par". Entonces, $b+i_2$ también es "par". Por lo tanto, $b+i = b+i_2+i_3(q-1)$ es "par". □

2.4.1. Fórmulas simétricas

En esta sección daremos fórmulas simétricas para calcular los pares (f_i, a_i) del Teorema 1.4.1.

Ya sabemos que $\Delta(a,b)$ es un polinomio en $1/[1]$ de grado $n < a+b$. Pero en general, no sabemos con precisión el valor de n. La siguiente proposición nos dice cómo tratar el problema.

Proposición 2.4.14. *Sea q una potencia de p. Sean $a, b \in \mathbb{Z}_+$. Sea n la potencia común de los polinomios mónicos de grado uno que aparecen en el denominador de la descomposición en fracciones parciales de $\Delta(a,b)$. Sea $l \in \mathbb{Z}_+$ tal que $n \leq l$ y sea m_l un entero tal que $l \leq p^{m_l}$. Entonces,*

$$\Delta(a,b) = \sum_{i=0}^{l-1} g_i S_1(l-i),$$

donde $g(t) = g_0 + \cdots + g_{l-1}t^{l-1} \in \mathbb{F}_p[t]$ está dado por

$$g(t) = -\frac{[1]^{p^{m_l}-l}}{t^{p^{m_l}-l}} \left([1]^l \Delta(a,b)\right) \text{ mód } t^l,$$

o equivalentemente,

$$g(t) = -\left(t^{q-1}-1\right)^{p^{m_l}-l} \left([1]^l \Delta(a,b)\right) \text{ mód } t^l.$$

Demostración. Aplicaremos la Proposición 2.4.1. Sea

$$\Delta(a,b) = \sum_{\mu \in \mathbb{F}_p} \frac{f(t-\mu)}{(t-\mu)^n}, \tag{2.4.14.1}$$

la descomposición en fracciones parciales de $\Delta(a,b)$, donde $f(t) = f_0 + f_1 t + \cdots + f_{n-1}t^{n-1} \in \mathbb{F}_p[t]$ es primo relativo a $t-\mu$. Para determinar f, procedemos como sigue. Para cualquier $r \geq 1$, los polinomios t^r y $[1]^r/t^r$ son primos relativos y de aquí que $[1]^r/t^r$ es una unidad módulo t^r. Más aún, dado que $l \leq p^{m_l}$,

$$\frac{[1]^{p^{m_l}-l}}{t^{p^{m_l}-l}} \frac{[1]^l}{t^l} = \frac{[1]^{p^{m_l}}}{t^{p^{m_l}}} = \left(t^{q-1}-1\right)^{p^{m_l}} = t^{p^{m_l}(q-1)} - 1,$$

y $l \leq p^{m_l}(q-1)$, tenemos $-\left(t^{p^{m_l}(q-1)}-1\right)$ mód $t^l = 1$ mód t^l. Luego,

$$\left(\frac{[1]^l}{t^l} \text{ mód } t^l\right)^{-1} = -\frac{[1]^{p^{m_l}-l}}{t^{p^{m_l}-l}} \text{ mód } t^l = -\left(t^{q-1}-1\right)^{p^{m_l}-l} \text{ mód } t^l.$$

De (2.4.14.1) se sigue que

$$\begin{aligned}[1]^l\Delta(a,b) &= \sum_{\mu\in\mathbb{F}_q} \frac{[1]^l}{(t-\mu)^l}(t-\mu)^{l-n}f(t-\mu)\\ &= \frac{[1]^l}{t^l}t^{l-n}f(t) + \sum_{\mu\in\mathbb{F}_q^*}\frac{[1]^l}{(t-\mu)^l}(t-\mu)^{l-n}f(t-\mu).\end{aligned}$$

Por lo tanto, módulo t^l tenemos que

$$[1]^l\Delta(a,b) = \frac{[1]^l}{t^l}g(t),$$

donde $g(t) = t^{l-n}f(t)$. Así,

$$g(t) \text{ mód } t^l = \left([1]^l\Delta(a,b) \text{ mód } t^l\right)\left(\frac{[1]^l}{t^l} \text{ mód } t^l\right)^{-1}.$$

Para finalizar la prueba, dividimos $g(t)$ por t^{l-n}. Sea $v_t(\cdot)$ la valuación en t. Entonces $v_t(g(t)) = l-n$ ya que $v_t(f(t)) = 0$. Entonces, para obtener $f(t)$ sólo tenemos que dividir $g(t)$ por $t^{v_t(g)}$. Note que $g(t) = g_{l-n}t^{l-n} + \cdots + g_{l-1}t^{l-1}$ ya que $v_t(g(t)) = l-n$; también $g_{l-n+i} = f_i$ para $0 \leq i \leq n-1$ y $g_i = 0$ para $i = 0,\ldots,l-n-1$. Por lo tanto,

$$\begin{aligned}\Delta(a,b) &= \sum_{i=0}^{n-1} f_iS_1(n-i)\\ &= \sum_{i=0}^{n-1} g_{l-n+i}S_1(l-(l-n+i))\\ &= \sum_{i=l-n}^{l-1} g_iS_1(l-i)\\ &= \sum_{i=0}^{l-1} g_iS_1(l-i).\end{aligned}$$

□

Observación 2.4.15. Del Teorema Binomial se sigue que

$$-\frac{[1]^{p^{m_l}-l}}{t^{p^{m_l}-l}} = -\left(t^{q-1}-1\right)^{p^{m_l}-l} = \sum_{j=0}^{p^{m_l}-l}\binom{p^{m_l}-l}{j}t^{(q-1)j}(-1)^{(l+j)}. \tag{2.4.15.1}$$

Ejemplo 2.4.16. Sean $q = 3$, $a = 4$ y $b = 5$. Por un cálculo directo

$$\Delta(4,5) = \frac{1}{[1]^5} = \frac{1}{t^5(t+1)^5(t+2)^5}.$$

Entonces $n=5$. Si tomamos $l=n=5$ y $m_l=2$, entonces $-(t^2-1)^4=2t^8+t^6+t^2+2$. Entonces, $g(t)$ módulo t^5 es igual a

$$-\frac{[1]^4}{t^4}\left([1]^5\Delta(a,b)\right) \text{ mód } t^5 = t^2+2.$$

Note que en este caso $g(t)=f(t)=t^2+2$. Luego,

$$\Delta(4,5)=2S_1(5)+S_1(3).$$

Si ahora usamos $l=a+b=9$ y $m_l=2$, entonces $-(t^2-1)^0=-1$ y $[1]^9\Delta(4,5)=[1]^4=t^{12}+2t^{10}+2t^6+t^4$, luego

$$g(t)=[1]^9\Delta(4,5) \text{ mód } t^9 = (t^6+2t^4) \text{ mód } t^9 = t^6+2t^4.$$

Observe que $f(t)=g(t)/t^4$ donde $v_t(g(t))=4$. Ahora

$$\Delta(a,b)=\sum_{i=0}^{9} g_i S_1(l-i)=2S_1(5)+S_1(3)$$

y obtenemos el mismo resultado.

Teorema 2.4.17. *Sea $q=2$. Sean $a,b\in\mathbb{Z}_+$ y sea m el entero más pequeño tal que $a+b\leq 2^m$. Entonces*

$$\begin{aligned}\zeta(a)\zeta(b)-\zeta(a+b)-\zeta(a,b)-\zeta(b,a)&\\ &=\sum_{i=0}^{a-1}\binom{2^m-b}{i}\zeta(a-i,b+i)+\sum_{j=0}^{b-1}\binom{2^m-a}{j}\zeta(b-j,a+j).\end{aligned}$$

Demostración. Es suficiente probar

$$\Delta(a,b)=\sum_{i=0}^{a-1}\binom{2^m-b}{i}S_1(a-i)+\sum_{j=0}^{b-1}\binom{2^m-a}{j}S_1(b-j).$$

Aplicaremos la Proposición 2.4.14 con $l=a+b$ y $m_l=m$. Entonces,

$$\Delta(a,b)=\sum_{i=0}^{a+b-1} g_i S_1(a+b-i),$$

donde $g(t)\in\mathbb{F}_p[t]$ está dado por

$$g(t)=-\frac{[1]^{p^m-a-b}}{t^{p^m-a-b}}[1]^{a+b}\Delta(a,b) \text{ mód } t^{a+b},$$

o equivalentemente

$$g(t)=(t+1)^{2^m-a-b}[1]^{a+b}\Delta(a,b) \text{ mód } t^{a+b}.$$

Ahora,

$$(t+1)^{2^m-a-b}[1]^{a+b}\Delta(a,b) = (t+1)^{2^m-a-b}\left((t+1)^a t^b + t^a(t+1)^b\right).$$

Por lo tanto

$$g(t) = \left((t+1)^{2^m-b}t^b + (t+1)^{2^m-a}t^a\right) \text{ mód } t^{a+b}.$$

Dado que $a \leq 2^m - b$ y $b \leq 2^m - a$, se sigue que

$$g(t) = \sum_{i=0}^{a-1}\binom{2^m-b}{i}t^{b+i} + \sum_{j=0}^{b-1}\binom{2^m-a}{j}t^{a+j}.$$

Sean $h_i = \binom{2^m-b}{i}$ y $f_j = \binom{2^m-a}{j}$. Supongamos que $a \leq b$. Entonces

$$\begin{aligned}
g(t) &= \sum_{i=0}^{b-1} f_i t^{i+a} + \sum_{i=0}^{a-1} h_i t^{i+b} \\
&= \sum_{i=a}^{a+b-1} f_{i-a}t^i + \sum_{i=b}^{a+b-1} h_{i-b}t^i \\
&= \sum_{i=a}^{b-1} f_{i-a}t^i + \sum_{i=b}^{a+b-1}(f_{i-a}+h_{i-b})t^i.
\end{aligned}$$

Por lo tanto

$$\begin{aligned}
\Delta(a,b) &= \sum_{i=a}^{b-1} f_{i-a}S_1(a+b-i) + \sum_{i=b}^{a+b-1}(f_{i-a}+h_{i-b})S_1(a+b-i) \\
&= \sum_{i=a}^{a+b-1} f_{i-a}S_1(a+b-i) + \sum_{i=b}^{a+b-1} h_{i-b}S_1(a+b-i) \\
&= \sum_{i=0}^{b-1} f_i S_1(b-i) + \sum_{i=0}^{a-1} h_i S_1(a-i).
\end{aligned}$$
□

Observación 2.4.18. Para obtener el conjunto $S(a,b)$ basta tomar la diferencia simétrica de los conjuntos $\{(f_i, b-i) \mid 0 \leq i < b, f_i \neq 0\}$ y $\{(h_i, a-i) \mid 0 \leq i < a, h_i \neq 0\}$, donde f_i y h_j son como en el Teorema 2.4.17.

Teorema 2.4.19. *Sea q una potencia arbitraria de p. Sean $a, b \in \mathbb{Z}_+$ y m el entero más pequeño tal que $a+b \leq p^m$. Entonces*

$$\zeta(a)\zeta(b) - \zeta(a+b) - \zeta(a,b) - \zeta(b,a) = \sum_{i=0}^{b-1} f_i\zeta(b-i, a+i) + \sum_{j=0}^{a-1} g_j\zeta(a-j, b+j),$$

donde $f(t) = H_{a,b}(t) = f_0 + f_1 t + \cdots + f_{b-1} t^{b-1}$, $g(t) = H_{b,a}(t) = g_0 + g_1 t + \cdots + g_{a-1} t^{a-1}$, $H_{a,b}(t)$ *está dado por*

$$H_{a,b}(t) = \frac{1}{t^a}\left(-(t^{q-1}-1)^{p^m-a}\sum_{\theta\in\mathbb{F}_q,\theta\neq 0}\left((t+\theta)^{q-1}-1\right)^a \text{ mód } t^{a+b}\right)$$

y $H_{b,a}$ *se obtiene intercambiando* a *y* b*. Equivalentemente*

$$H_{a,b}(t) = \sum_{j=0}^{p^m-a}\sum_{\substack{\sum k_i=a\\ q-1|\sigma(k)}}\binom{p^m-a}{j}\binom{a}{k_1,\ldots,k_{q-1}}(-1)^{a+j+1}t^{j(q-1)+\sigma(k)-a}, \quad (2.4.19.1)$$

donde $\sigma(k) := k_1 + 2k_2 + \cdots + (q-1)k_{q-1}$*, y* j*,* $\sigma(k)$ *satisfacen la condición* $j(q-1) + \sigma(k) < a + b$*.*

También, $H_{a,b}(t)$ *está dado por*

$$H_{a,b}(t) = \sum_{j=0}^{p^m-a}\sum_{i=0}^{a}\sum_{k_1=0}^{i}\binom{p^m-a}{j}\binom{a}{i}\binom{i(q-1)}{k_1(q-1)}(-1)^{a-i}t^{(k_1+j)(q-1)-a},$$

y k_1, j *son tales que* $(k_1+j)(q-1)$ *es menor que* $a+b$*.*

Demostración. De acuerdo con el Teorema 1.4.2, es suficiente probar

$$\Delta(a,b) = \sum_{i=0}^{b-1} f_i S_1(b-i) + \sum_{j=0}^{a-1} g_j S_1(a-j).$$

Aplicaremos la Proposición 2.4.14, con $l = a+b$. Así, necesitamos calcular módulo t^{a+b} el polinomio

$$P(t) = -\frac{[1]^{p^m-a-b}}{t^{p^m-a-b}}[1]^{a+b}\Delta(a,b).$$

Hacemos esto como sigue:

$$P(t) = -\frac{[1]^{p^m-a-b}}{t^{p^m-a-b}}\sum_{\substack{\theta,\mu\in\mathbb{F}_q\\ \theta\neq\mu}}\frac{[1]^a}{(t+\theta)^a}\frac{[1]^b}{(t+\mu)^b} = P_a(t) + P_b(t) + P_{a,b}(t),$$

donde

$$P_a(t) = -\frac{[1]^{p^m-a-b}}{t^{p^m-a-b}}\sum_{\theta\neq 0}\frac{[1]^b}{t^b}\frac{[1]^a}{(t+\theta)^a} = -\frac{[1]^{p^m-a}}{t^{p^m-a}}\sum_{\theta\neq 0}\frac{[1]^a}{(t+\theta)^a},$$

$$P_b(t) = -\frac{[1]^{p^m-a-b}}{t^{p^m-a-b}}\sum_{\mu\neq 0}\frac{[1]^a}{t^a}\frac{[1]^b}{(t+\mu)^b} = -\frac{[1]^{p^m-b}}{t^{p^m-b}}\sum_{\mu\neq 0}\frac{[1]^b}{(t+\mu)^b},$$

y

$$P_{a,b}(t) = -\frac{[1]^{p^m-a-b}}{t^{p^m-a-b}} \sum_{\substack{\theta\neq 0\neq\mu \\ \theta\neq\mu}} \frac{[1]^a}{(t+\theta)^a}\frac{[1]^b}{(t+\mu)^b}.$$

Para $\xi \in \mathbb{F}_q, \xi \neq 0$ y $l \in \mathbb{Z}_+$, la valuación en t de $[1]^l/(t+\xi)^l$ es l. Dado que la valuación en t de $[1]/t$ es cero, se sigue que $v_t(P_a(t)) \geq a$, $v_t(P_b(t)) \geq b$ y $v_t(P_{a,b}(t)) \geq a+b$. Así $P_{a,b}(t) = 0$ módulo t^{a+b}. Entonces, módulo t^{a+b} tenemos que

$$-\frac{[1]^{p^m-a-b}}{t^{p^m-a-b}}[1]^{a+b}\Delta(a,b) = P_a(t) + P_b(t).$$

Sea $H_{a,b}(t)$ igual a $1/t^a$ veces el resto que resulta al dividir $P_a(t)$ entre t^{a+b}, esto es,

$$H_{a,b}(t) = \frac{1}{t^a}\left(P_a(t) \text{ mód } t^{a+b}\right).$$

Note que

$$H_{b,a}(t) = \frac{1}{t^b}\left(P_b(t) \text{ mód } t^{a+b}\right).$$

Sean $f(t) = H_{a,b}(t) = f_0 + f_1 t + \cdots + f_{b-1}t^{b-1}$ y $g(t) = H_{b,a}(t) = g_0 + g_1 t + \cdots + g_{a-1}t^{a-1}$. Supongamos que $\text{mín}\{a,b\} = a$. Entonces $P_a(t) + P_b(t)$ módulo t^{a+b} es igual a

$$\begin{aligned} t^a f(t) + t^b g(t) &= \sum_{i=0}^{b-a-1} f_i t^{i+a} + \sum_{i=b-a}^{b-1} f_i t^{i+a} + \sum_{i=0}^{a-1} g_i t^{i+b} \\ &= \sum_{i=a}^{b-1} f_{i-a} t^i + \sum_{i=b}^{a+b-1} f_{i-a} t^i + \sum_{i=b}^{a+b-1} g_{i-b} t^i \\ &= \sum_{i=a}^{b-1} f_{i-a} t^i + \sum_{i=b}^{a+b-1} (f_{i-a} + g_{i-b}) t^i. \end{aligned}$$

Por lo tanto, de la Proposición 2.4.14 obtenemos

$$\begin{aligned} \Delta(a,b) &= \sum_{i=a}^{b-1} f_{i-a} S_1(a+b-i) + \sum_{i=b}^{a+b-1} (f_{i-a} + g_{i-b}) S_1(a+b-i) \\ &= \sum_{i=0}^{b-a-1} f_i S_1(b-i) + \sum_{i=b-a}^{b-1} (f_i + g_{i+a-b}) S_1(b-i) \\ &= \sum_{i=0}^{b-1} f_i S_1(b-i) + \sum_{i=b-a}^{b-1} g_{i+a-b} S_1(b-i) \\ &= \sum_{i=0}^{b-1} f_i S_1(b-i) + \sum_{i=0}^{a-1} g_i S_1(a-i). \end{aligned}$$

A continuación calculamos $H_{a,b}(t)$. Como $\binom{q-1}{i} = (-1)^i$, de la Proposición 2.3.7 (a), tenemos que para $\theta \in \mathbb{F}_q^*$

$$(t+\theta)^{q-1} - 1 = \sum_{i=1}^{q-1} \binom{q-1}{i} t^i \theta^{q-1-i} = \sum_{i=1}^{q-1} (-t)^i \theta^{q-1-i}.$$

Por el Teorema Multinomial,

$$\begin{aligned}
\sum_{\theta \neq 0} \frac{[1]^a}{(t+\theta)^a} &= \sum_{\theta \neq 0} \left((t+\theta)^{q-1} - 1\right)^a \\
&= \sum_{\theta \neq 0} \sum_k \binom{a}{k} \prod_{i=1}^{q-1} \left((-t)^i \theta^{q-1-i}\right)^{k_i} \\
&= \sum_k \binom{a}{k} (-t)^{\sigma(k)} \sum_{\theta \neq 0} \theta^{\tau(k)},
\end{aligned}$$

donde la primera suma es sobre todas las $(q-1)$-adas $k = (k_1, \ldots, k_{q-1})$ de enteros no negativos tales que $k_1 + \cdots + k_{q-1} = a$, $\sigma(k) := \sum_{i=1}^{q-1} ik_i$ y $\tau(k) = \sum_{i=1}^{q-1} k_i(q-1-i)$. Note que $\tau(k) = (q-1)\sum_{i=1}^{q-1} k_i - \sigma(k) = a(q-1) - \sigma(k)$. Usando el hecho de que $\sum_{\xi \in \mathbb{F}_q^*} \xi^l$ es -1 o 0 dependiendo de si l es "par" o no, obtenemos

$$\begin{aligned}
P_a(t) &= \sum_{j=0}^{p^m-a} \binom{p^m-a}{j} (-1)^{p^m-a-j+1} t^{j(q-1)} \sum_{\substack{k \\ q-1 | \sigma(k)}} \binom{a}{k} (-1) t^{\sigma(k)} \\
&= \sum_{j=0}^{p^m-a} \sum_{\substack{k \\ q-1 | \sigma(k)}} \binom{p^m-a}{j} \binom{a}{k} (-1)^{a+j+1} t^{j(q-1)+\sigma(k)}.
\end{aligned}$$

El resto que se obtiene al dividir $P_a(t)$ entre t^{a+b} tiene valuación en t mayor o igual que a. De aquí se sigue que $H_{a,b}(t)$ es igual al lado derecho de la Ecuación (2.4.19.1).

Desarrollando $P_a(t)$ en forma diferente, obtenemos la otra descripción para $H_{a,b}(t)$.

$$\begin{aligned}
\sum_{\theta \neq 0} \frac{[1]^a}{(t+\theta)^a} &= \sum_{\theta \neq 0} \left((t+\theta)^{q-1} - 1\right)^a \\
&= \sum_{\theta \neq 0} \sum_{i=0}^{a} \binom{a}{i} (t+\theta)^{i(q-1)} (-1)^{a-i} \\
&= \sum_{i=0}^{a} \sum_{k_1=0}^{i(q-1)} \binom{a}{i} \binom{i(q-1)}{k_1} (-1)^{a-i} t^{k_1} \sum_{\theta \neq 0} \theta^{i(q-1)-k_1}.
\end{aligned}$$

Observamos que $l(q-1) - u \equiv 0 \text{ mód } (q-1)$ si y sólo si $u \equiv 0 \text{ mód } (q-1)$. Usando el hecho de que $\sum_{\chi \in \mathbb{F}_q^*} \chi^l$ es 0 si $q-1$ no divide a l, y -1 si $l \geq 0$ es divisible por $q-1$, se sigue que

$$P_a(t) = \sum_{j=0}^{p^m-a} \binom{p^m-a}{j} (-1)^{p^m-a-j+1} t^{j(q-1)} \sum_{i=0}^{a} \sum_{k_1=0}^{i} \binom{a}{i} \binom{i(q-1)}{k_1(q-1)} (-1)^{a-i+1} t^{k_1(q-1)}$$
$$= \sum_{j=0}^{p^m-a} \sum_{i=0}^{a} \sum_{k_1=0}^{i} \binom{p^m-a}{j} \binom{a}{i} \binom{i(q-1)}{k_1(q-1)} (-1)^{a-i} t^{(k_1+j)(q-1)}.$$

De aquí obtenemos la otra descripción para $H_{a,b}(t)$. □

Observaciones 2.4.20.

(1) De acuerdo con la Proposición 2.4.14, en los Teoremas 2.4.17 y 2.4.19 somos libres de usar cualquier m tal que $a+b \leq p^m$, en lugar de usar $\lceil \log_p(a+b) \rceil$. Lo mismo se aplica para los Teoremas 2.4.5 y 2.4.11, y también para los teoremas en la siguiente subsección.

(2) Cuando $q = 2$, la Ecuación (2.4.19.1) se convierte en $H_{a,b}(t) = \sum_{j=0}^{b-1} \binom{p^m-a}{j} t^j$. Por lo tanto, obtenemos el Teorema 2.4.17 como un corolario del Teorema 2.4.19.

(3) Ya hemos probado la conjetura de Thakur [Tha09b, 5.3] relativa a la paridad (vea la Sección 2.2 y el corolario del Teorema 2.4.11). Como corolario del Teorema 2.4.19, tenemos otra prueba de esta conjetura.

2.4.2. Otras fórmulas simétricas

En esta subsección daremos otras fórmulas simétricas para expresar el producto $\zeta(a)\zeta(b)$ como una suma de valores multizeta. Las fórmulas que se dan en los Teoremas 2.4.21, 2.4.22 y 2.4.23 son más complicadas que la fórmula que se presenta en el Teorema 2.4.19. De hecho, los teoremas presentados en esta subsección en realidad son versiones previas del Teorema 2.4.19.

Teorema 2.4.21. *Sea q una potencia de p. Sean $a, b \in \mathbb{Z}_+$ y m el entero más pequeño tal que $a+b \leq p^m$. Entonces*

$$\zeta(a)\zeta(b) - \zeta(a+b) - \zeta(a,b) - \zeta(b,a) = \sum_{i=0}^{a+b-1} f_i \zeta(a+b-i, i),$$

donde $f(t) = f_0 + f_1 t + \cdots + f_{a+b-1} t^{a+b-1}$ está dado por

$$-\left(t^{q-1}-1\right)^{p^m-a-b} \sum_{\theta \in \mathbb{F}_q} \sum_{\mu \in \mathbb{F}_q^*} \left((t+\theta)^{q-1}-1\right)^a \left((t+\theta-\mu)^{q-1}-1\right)^b \text{ mód } t^{a+b}.$$

Equivalentemente, $f(t)$ está dado por

$$\sum_{i_5=0}^{p^m-a-b} \sum_{i_1=0}^{a} \sum_{i_2=0}^{b} \sum_{i_3=0}^{i_2(q-1)} \sum_{i_4=0}^{i_1(q-1)+i_3-1} \binom{p^m-(a+b)}{i_5} \binom{a}{i_1} \binom{b}{i_2} \binom{i_2(q-1)}{i_3}$$
$$\times \binom{i_1(q-1)+i_3}{i_4} (-1)^{i_1+i_2+i_3+i_5} t^{i_4+i_5(q-1)}$$

donde i_1, i_2, i_3, i_4 están sujetos a que $i_1(q-1)+i_3-i_4$, $i_2(q-1)-i_3$ sean ambos "pares" e $i_4+i_5(q-1) < a+b$.

Demostración. Aplicaremos la Proposición 2.4.14 con $l = a+b$ y $m_l = m$. Calculemos $[1]^{a+b}\Delta(a,b)$ como sigue. Para $\theta, \mu \in \mathbb{F}_q$, con $\mu \neq 0$, tenemos

$$\begin{aligned}
\frac{[1]^a}{(t+\theta)^a}\frac{[1]^b}{(t+\theta-\mu)^b} &= \left((t+\theta)^{q-1}-1\right)^a \left((t+\theta-\mu)^{q-1}-1\right)^b \\
&= \sum_{i_1=0}^{a}\sum_{i_2=0}^{b}\binom{a}{i_1}\binom{b}{i_2}(t+\theta)^{i_1(q-1)}(t+\theta-\mu)^{i_2(q-1)}(-1)^{a+b-i_1-i_2} \\
&= \sum_{i_1=0}^{a}\sum_{i_2=0}^{b}\sum_{i_3=0}^{i_2(q-1)}\binom{a}{i_1}\binom{b}{i_2}\binom{i_2(q-1)}{i_3} \\
&\qquad \times (t+\theta)^{i_1(q-1)+i_3}\mu^{i_2(q-1)-i_3}(-1)^{a+b-i_1-i_2+i_2(q-1)-i_3}.
\end{aligned}$$

Usando el hecho de que $\sum_{\theta\in\mathbb{F}_q^*} 1 = -1$, obtenemos

$$\begin{aligned}
\sum_{\theta\in\mathbb{F}_q}(t+\theta)^l = t^l + \sum_{\theta\neq 0}(t+\theta)^l &= t^l + \sum_{\theta\neq 0}\sum_{i_4=0}^{l}\binom{l}{i_4}t^{i_4}\theta^{l-i_4} \\
&= t^l + \sum_{i_4=0}^{l}\left(\sum_{\theta\neq 0}\theta^{l-i_4}\right)t^{i_4} = \sum_{i_4=0}^{l-1}\sum_{\theta\neq 0}\theta^{l-i_4}t^{i_4}.
\end{aligned}$$

Tomando la suma sobre $\theta \in \mathbb{F}_q$, $\mu \in F_q^*$, se sigue que $[1]^{a+b}\Delta(a,b)$ es igual a

$$\begin{aligned}
&\sum_{i_1=0}^{a}\sum_{i_2=0}^{b}\sum_{i_3=0}^{i_2(q-1)}\sum_{i_4=0}^{i_1(q-1)+i_3-1}\binom{a}{i_1}\binom{b}{i_2}\binom{i_2(q-1)}{i_3}\binom{i_1(q-1)+i_3}{i_4} \\
&\qquad \times \left(\sum_{\theta\in\mathbb{F}_q^*}\theta^{i_1(q-1)+i_3-i_4}\right)\left(\sum_{\mu\in\mathbb{F}_q^*}\mu^{i_2(q-1)-i_3}\right)(-1)^{a+b-i_1-i_2+i_2(q-1)-i_3}t^{i_4}.
\end{aligned}$$

Multiplicando la Ecuación (2.4.15.1) tomando $l = a+b$ y $m_l = m$, y usando el hecho de que $\sum_{\xi\in\mathbb{F}_q^*}\xi^l$ es -1 o 0, dependiendo de que l sea "par" o no, obtenemos que $f(t)$ es exactamente como se afirmó. □

Teorema 2.4.22. *Sea q una potencia de p. Sean $a, b \in \mathbb{Z}_+$ y m el entero más pequeño tal que $a+b \leq p^m$. Entonces*

$$\zeta(a)\zeta(b) - \zeta(a+b) - \zeta(a,b) - \zeta(b,a) = \sum_{i=0}^{a+b-1} f_i\zeta(a+b-i,i),$$

donde $f(t) := f_0 + f_1 t + \cdots + f_{a+b-1}t^{a+b-1}$ está dado por

$$-\left(t^{q-1}-1\right)^{p^m-a-b}\sum_{\substack{\mu,\theta\in\mathbb{F}_q\\ \mu\neq\theta}}\left((t+\theta)^{q-1}-1\right)^a\left((t+\mu)^{q-1}-1\right)^b \text{ mód } t^{a+b}.$$

Equivalentemente, $f(t)$ está dado por

$$\sum_{i_5=0}^{p^m-a-b}\sum_{i_1=0}^{a}\sum_{i_2=0}^{b}\binom{p^m-(a+b)}{i_5}\binom{a}{i_1}\binom{b}{i_2}(-1)^{i_1+i_2+i_5}P(i_1,i_2,t)$$

donde

$$P(i_1,i_2,t)=\sum_{i_3=0}^{i_1-1}\sum_{i_4=0}^{i_2-1}\binom{i_1(q-1)}{i_3(q-1)}\binom{i_2(q-1)}{i_4(q-1)}t^{(i_3+i_4+i_5)(q-1)} + \sum_{j=0}^{i_1+i_2-1}\binom{(i_1+i_2)(q-1)}{j(q-1)}t^{(j+i_5)(q-1)}$$

e i_3, i_4, i_5, j están sujetos a que $(i_3+i_4+i_5)(q-1)$, $(j+i_5)(q-1)$ sean ambos menores que $a+b$.

Demostración. Aplicaremos la Proposición 2.4.14, con $l = a+b$ y $m_l = m$. Calculemos $[1]^{a+b}\Delta(a,b)$ como sigue. Para $\theta,\mu \in \mathbb{F}_q$, con $\theta \neq \mu$, tenemos

$$\begin{aligned}
[1]^{a+b}\Delta(a,b) &= \sum_{\substack{\theta,\mu\in\mathbb{F}_q\\ \theta\neq\mu}} \frac{[1]^a}{(t+\theta)^a}\frac{[1]^b}{(t+\mu)^b}\\
&= \sum_{\substack{\theta,\mu\in\mathbb{F}_q\\ \theta\neq\mu}} \left((t+\theta)^{q-1}-1\right)^a\left((t+\mu)^{q-1}-1\right)^b\\
&= \sum_{i_1=0}^{a}\sum_{i_2=0}^{b}\binom{a}{i_1}\binom{b}{i_2}(-1)^{a+b-i_1-i_2}P(i_1,i_2,t)
\end{aligned}$$

donde

$$P(i_1,i_2,t)=\sum_{\substack{\theta,\mu\in\mathbb{F}_q\\ \theta\neq\mu}}(t+\theta)^{i_1(q-1)}(t+\mu)^{i_2(q-1)}.$$

Ahora,

$$P(i_1,i_2,t)=\sum_{\theta,\mu\in\mathbb{F}_p}(t+\theta)^{i_1(q-1)}(t+\mu)^{i_2(q-1)}-\sum_{\theta=\mu}(t+\theta)^{(i_1+i_2)(q-1)}.$$

Más aún, $P(i_1,i_2,t)$ es igual a

$$\sum_{\mu\neq0}t^{i_1(q-1)}(t+\mu)^{i_2(q-1)}+\sum_{\theta\neq0}(t+\mu)^{i_1(q-1)}t^{i_2(q-1)}+ \sum_{\theta\neq0}\sum_{\mu\neq0}(t+\theta)^{i_1(q-1)}(t+\mu)^{i_2(q-1)}-\sum_{\xi\neq0}(t+\xi)^{(i_1+i_2)(q-1)}.$$

Tenemos que

$$\sum_{\mu\neq 0} t^{i_1(q-1)}(t+\mu)^{i_2(q-1)} = t^{i_1(q-1)} \sum_{i_4=0}^{i_2(q-1)} \binom{i_2(q-1)}{i_4} t^{i_4} \sum_{\mu\neq 0} \mu^{i_2(q-1)-i_4},$$

$$\sum_{\theta\neq 0} (t+\mu)^{i_1(q-1)} t^{i_2(q-1)} = t^{i_2(q-1)} \sum_{i_3=0}^{i_1(q-1)} \binom{i_1(q-1)}{i_3} t^{i_3} \sum_{\theta\neq 0} \theta^{i_1(q-1)-i_3},$$

$$\begin{aligned}\sum_{\theta\neq 0}\sum_{\mu\neq 0} (t+\theta)^{i_1(q-1)}(t+\mu)^{i_2(q-1)} = \sum_{i_3=0}^{i_1(q-1)} \sum_{i_4=0}^{i_2(q-1)} &\binom{i_1(q-1)}{i_3}\binom{i_2(q-1)}{i_4} \\ &\times t^{i_3+i_4} \sum_{\theta\neq 0} \theta^{i_1(q-1)-i_3} \sum_{\mu\neq 0} \mu^{i_2(q-1)-i_4},\end{aligned}$$

y

$$\sum_{\xi\neq 0} (t+\xi)^{(i_1+i_2)(q-1)} = \sum_{j=0}^{(i_1+i_3)(q-1)} \binom{(i_1+i_2)(q-1)}{j} t^j \sum_{\xi\neq 0} \xi^{(i_1+i_3)(q-1)-j}.$$

Notamos que $l(q-1)-u \equiv 0 \text{ mód } (q-1)$ si y sólo si $u \equiv 0 \text{ mód } (q-1)$. Usando el hecho de que $\sum_{\xi\in\mathbb{F}_q^*} \xi^l$ es -1 o 0, dependiendo de que l sea "par" o no, obtenemos que $P(i_1,i_2,t)$ es exactamente como se afirmó. Multiplicando por la Ecuación (2.4.15.1) con $l=a+b$ y $m_l=m$, obtenemos que $f(t)$ es como se afirmó. $\square$

Teorema 2.4.23. *Sea q una potencia de p. Sean $a,b\in\mathbb{Z}_+$ y m el entero más pequeño tal que $a+b\le p^m$. Entonces*

$$\zeta(a)\zeta(b)-\zeta(a+b)-\zeta(a,b)-\zeta(b,a) = \sum_{i=0}^{a+b-1} (f_i+g_i)\zeta(a+b-i,i),$$

donde $f(t)=f_0+\cdots+f_{a+b-1}t^{a+b-1}$ y $g(t)=g_0+\cdots+g_{a+b-1}t^{a+b-1}$ están dados por

$$f(t) = -(t^{q-1}-1)^{p^m-a} \sum_{\theta\in\mathbb{F}_q,\theta\neq 0} \left((t+\theta)^{q-1}-1\right)^a \text{ mód } t^{a+b},$$

$$g(t) = -(t^{q-1}-1)^{p^m-b} \sum_{\theta\in\mathbb{F}_q,\theta\neq 0} \left((t+\theta)^{q-1}-1\right)^b \text{ mód } t^{a+b}.$$

Equivalentemente,

$$f(t) = \sum_{i_5=0}^{p^m-a}\sum_{i_1=0}^{a}\sum_{i_3=0}^{i_1} \binom{p^m-a}{i_5}\binom{a}{i_1}\binom{i_1(q-1)}{i_3(q-1)}(-1)^{i_1+i_5+1}t^{(i_3+i_5)(q-1)},$$

$$g(t) = \sum_{i_5=0}^{p^m-b}\sum_{i_2=0}^{b}\sum_{i_4=0}^{i_2} \binom{p^m-b}{i_5}\binom{b}{i_2}\binom{i_2(q-1)}{i_4(q-1)}(-1)^{i_2+i_5+1}t^{(i_4+i_5)(q-1)}$$

e i_3,i_4,i_5 están sujetos a que $(i_3+i_5)(q-1)$, $(i_4+i_5)(q-1)$ sean ambos menores que $a+b$.

Demostración. Aplicaremos la Proposición 2.4.14, con $l = a + b$. Así, necesitamos calcular módulo t^{a+b} el polinomio

$$P(t) = -\frac{[1]^{p^m-a-b}}{t^{p^m-a-b}}[1]^{a+b}\Delta(a,b).$$

Lo hacemos como sigue. Note que

$$P(t) = -\frac{[1]^{p^m-a-b}}{t^{p^m-a-b}} \sum_{\substack{\theta,\mu\in\mathbb{F}_q \\ \theta\neq\mu}} \frac{[1]^a}{(t+\theta)^a}\frac{[1]^b}{(t+\mu)^b} = P_a(t) + P_b(t) + P_{a,b}(t),$$

donde

$$P_a(t) = -\frac{[1]^{p^m-a-b}}{t^{p^m-a-b}} \sum_{\theta\neq 0} \frac{[1]^b}{t^b}\frac{[1]^a}{(t+\theta)^a} = -\frac{[1]^{p^m-a}}{t^{p^m-a}} \sum_{\theta\neq 0} \frac{[1]^a}{(t+\theta)^a},$$

$$P_b(t) = -\frac{[1]^{p^m-a-b}}{t^{p^m-a-b}} \sum_{\mu\neq 0} \frac{[1]^a}{t^a}\frac{[1]^b}{(t+\mu)^b} = -\frac{[1]^{p^m-b}}{t^{p^m-b}} \sum_{\mu\neq 0} \frac{[1]^b}{(t+\theta)^b},$$

y

$$P_{a,b}(t) = -\frac{[1]^{p^m-a-b}}{t^{p^m-a-b}} \sum_{\substack{\theta\neq 0\neq\mu \\ \theta\neq\mu}} \frac{[1]^a}{(t+\theta)^a}\frac{[1]^b}{(t+\mu)^b}.$$

Para $\xi \in \mathbb{F}_q, \xi \neq 0$ y $l \in \mathbb{Z}_+$, la valuación en t de $[1]^l/(t+\xi)^l$ es l. Dado que la valuación en t de $[1]/t$ es cero, se sigue que $v_t(P_a(t)) \geq a$, $v_t(P_b(t)) \geq b$ y $v_t(P_{a,b}(t)) \geq a+b$. Así, $P_{a,b}(t) = 0$ módulo t^{a+b}. Entonces módulo t^{a+b} tenemos

$$-\frac{[1]^{p^m-a-b}}{t^{p^m-a-b}}[1]^{a+b}\Delta(a,b) = P_a(t) + P_b(t).$$

Sea $f(t)$ el resto que se obtiene al dividir $P_a(t)$ por t^{a+b}; análogamente, sea $g(t) = P_b(t)$ mód t^{a+b}.

Por lo tanto, de acuerdo con la Proposición 2.4.14 tenemos que

$$\Delta(a,b) = \sum_{i=0}^{a+b-1}(f_i + g_i)S_1(a+b-i).$$

Desarrollemos $P_a(t)$ como sigue.

$$\begin{aligned}
\sum_{\theta\in\mathbb{F}_q^*} \frac{[1]^a}{(t+\theta)^a} &= \sum_{\theta\in\mathbb{F}_q^*} \left((t+\theta)^{q-1} - 1\right)^a \\
&= \sum_{\theta\in\mathbb{F}_q^*} \sum_{i_1=0}^{a} \binom{a}{i_1}(t+\theta)^{i_1(q-1)}(-1)^{a-i_1} \\
&= \sum_{i_1=0}^{a} \sum_{i_3=0}^{i_1(q-1)} \binom{a}{i_1}\binom{i_1(q-1)}{i_3}(-1)^{a-i_1}t^{i_3} \sum_{\theta\in\mathbb{F}_q^*} \theta^{i_1(q-1)-i_3}.
\end{aligned}$$

Observamos que $l(q-1)-u \equiv 0 \text{ mód } (q-1)$ si y sólo si $u \equiv 0 \text{ mód } (q-1)$. Usando el hecho de que $\sum_{\chi\in\mathbb{F}_q^*}\chi^l$ es 0 si $q-1$ no divide a l, y -1 si $l\geq 0$ es divisible por $q-1$, se sigue que

$$\begin{aligned}P_a(t) &= \sum_{i_5=0}^{p^m-a}\binom{p^m-a}{i_5}(-1)^{-a-i_5}t^{i_5(q-1)}\sum_{i_1=0}^{a}\sum_{i_3=0}^{i_1}\binom{a}{i_1}\binom{i_1(q-1)}{i_3(q-1)}(-1)^{a-i_1+1}t^{i_3(q-1)}\\ &= \sum_{i_5=0}^{p^m-a}\sum_{i_1=0}^{a}\sum_{i_3=0}^{i_1}\binom{p^m-a}{i_5}\binom{a}{i_1}\binom{i_1(q-1)}{i_3(q-1)}(-1)^{i_1+i_5+1}t^{(i_3+i_5)(q-1)}. \qquad \square\end{aligned}$$

2.5. Conjetura recursiva para $q=2$

En [Tha09b, 4.1.4], para $q=2$, Thakur formula una conjetura recursiva de tres pasos para escribir el producto de dos valores zeta como una suma de valores multizeta. A continuación reproducimos aquí la conjetura.

La siguiente definición (siguiendo la notación del artículo de referencia) será usada únicamente en esta sección: Dados los conjuntos A, B definimos $A\oplus B = A\cup B\setminus(A\cap B)$ (Usualmente el símbolo $\oplus$ se usa para denotar la suma directa, pero aquí la estamos usando para denotar la diferencia simétrica).

Conjetura 2.5.1 (Thakur)**.**

(1) *Sea $A=\mathbb{F}_q[t]$. Dados $a,b\in\mathbb{Z}_+$, existen $a_i\in\mathbb{Z}_+$, tales que para toda $d\geq 0$*

$$\Delta_d(a,b)=\sum S_d(a_i,a+b-a_i). \tag{2.5.1.1}$$

El conjunto de a_i's denotado por $S(a,b)$, es independiente de d.

(2) *Los conjuntos $S(a,b)$ se pueden hallar de manera recursiva*

$$S(a,b)=S(a,b-r_a)\oplus T'(a,b).$$

La descripción para $T'(a,b)$ es como sigue.

   a) *Para $a=1$, $S(1,b)=\{2,\ldots,b\}$ y $T'(1,b)=\{b\}$.*

   b) *Para a impar, escriba $a=\sum_1^n 2^{e_i}-\sum_1^n 2^{\overline{e_i}}+2^{e_0}$, con $e_0=0$, $e_n>\overline{e_n}>e_{n-1}>\cdots\overline{e_1}>e_0=0$. (En otras palabras, se toma la expansión en base 2 de $a-1$ y se descompone en bloques de 1's y 0's: más precisamente, esta descomposición consiste de 1's consecutivos entre los lugares e_i-1 y $\overline{e_i}$, y 0's en otra parte). Se da una descripción inductiva en n (el caso $n=0$ está considerado en el paso anterior): Si $a'=a+2^{e_{n+1}}-2^{\overline{e_{n+1}}}$, entonces*

$$T'(a',b)=T'(a,b)\oplus T'(a,b-2^{e_n})\oplus\cdots\oplus T'(a,b-(2^{\overline{e_{n+1}}-e_n}-1)2^{e_n}).$$

   c) *Si $T'(a,b)=\{b,b-b_1,\ldots,b-b_k\}$, entonces*

$$T'(2^m a,b)=\{b,b-2^m b_1,\ldots,b-2^m b_k\}.$$

(3) *Los valores iniciales $S(a,b)$, $b \leq r_a$ de la recursión se calculan de acuerdo a la siguiente fórmula inductiva:*

$$S(a,b) \oplus S(a, b + r_a/2) = T'(a, b + r_a/2) \oplus S(b, \overline{a})$$

donde $a \equiv \overline{a} \mod r_a/2$, $0 < \overline{a} \leq r_a/2$ *y* $0 < b \leq r_a/2$.

El primer paso fue probado de manera general por Thakur [Tha10, Teoremas 1,2]. Los Teoremas 2.4.11, 2.4.19 dan otra prueba del mismo resultado. Aquí probaremos el segundo paso de la conjetura.

Dado que $\mathbb{F}_2^* = \{1\}$, para simplificar la notación en la descripción de $T(a,b)$ escribiremos b_k en vez de $(1, b_k)$.

Teorema 2.5.2. *Sea $q = 2$. Entonces $T(a,b) = T'(a,b)$ para cualquier $a, b \in \mathbb{Z}_+$, donde $T(a,b)$ es como en el Teorema* 2.3.14.

Demostración. Probaremos que $T(a,b)$ satisface las mismas condiciones que $T'(a,b)$. Del Teorema 2.3.14, sabemos que los conjuntos $S(a,b)$ se pueden hallar recursivamente, con longitud de recursión r_a.

(a) Si $a = 1$, entonces $p^m - a = 0$, $r_1 = 1$. Por el Teorema 2.3.14, $\Delta(1, b+1) - \Delta(1,b) = S_1(1+b)$. Dado que $\Delta(1,1) = 0$ [Tha09b, Teorema 8], se sigue que $S(1,b) = \{2, \ldots, b\}$. Por lo tanto $T(1,b) = \{b\}$.

(b) Sea a impar. Escribamos $a = \sum_{i=1}^{n} 2^{e_i} - \sum_{i=1}^{n} 2^{\bar{e}_i} + 2^{e_0}$, con $e_n > \bar{e}_n > e_{n-1} > \bar{e}_{n-1} > \cdots > \bar{e}_1 > e_0$. Sea $a' = a + 2^{e_{n+1}} - 2^{\bar{e}_{n+1}}$, donde $r_a = 2^{e_n}$ y $r_{a'} = 2^{e_{n+1}}$. Sea μ_0 el número de ceros en la descomposición en base 2 de $a - 1$. Como $2^{\bar{e}_{n+1}} - 2^{e_n} = 2^{e_n} + \cdots + 2^{\bar{e}_{n+1}-1}$, se sigue que el número de ceros en la descomposición en base 2 de $a' - 1$ es $\mu_0 + \bar{e}_{n+1} - e_n$. Por lo tanto, $t_{a'} = 2^{\mu_0 + \bar{e}_{n+1} - e_n}$. Sea j, $0 \leq j \leq 2^{e_n} - a$ y $0 \leq z \leq 2^{\bar{e}_{n+1} - e_n} - 1$. Entonces, $0 \leq j + z2^{e_n} \leq 2^{e_n} - a + 2^{\bar{e}_{n+1}} - 2^{e_n} = 2^{e_{n+1}} - a'$. Dado que $2^{e_{n+1}} - a' = 2^{e_n} - a + 2^{\bar{e}_{n+1}} - 2^{e_n}$, del Teorema de Lucas se sigue que

$$\binom{2^{e_{n+1}} - a'}{j + z2^{e_n}} = \binom{2^{e_n} - a}{j} \binom{2^{\bar{e}_{n+1}} - 2^{e_n}}{z2^{e_n}} \mod 2.$$

El último coeficiente binomial a la derecha siempre es distinto de cero módulo 2. Dado que hay $2^{\bar{e}_{n+1} - e_n}$ z's y hay t_a j's tales que $f_{a,j} = 1$, se sigue que el conjunto de j', $0 \leq j' \leq 2^{e_{n+1}} - a'$ tales que $f_{a',j'} = 1$ es

$$\left\{ j + z2^{e_n} \mid 0 \leq j \leq 2^{e_n} - a, f_{a,j} = 1, 0 \leq z \leq 2^{\bar{e}_{n+1} - e_n} - 1 \right\}.$$

Como $q = 2$, tenemos que $l_j = l$. Si $j' = j + z2^{e_n}$, entonces

$$r_{a'} - a' - j' = (2^{\bar{e}_{n+1}} - (1+z)2^{e_n}) + (r_a - a - j) = z'2^{e_n} + r_a - a - j$$

donde $z' = 2^{\bar{e}_{n+1} - e_n} - 1 - z$.

Por lo tanto, por el Teorema 2.3.14,

$$\begin{aligned} T(a', b) &= \left\{ b - (r_{a'} - a' - j') \mid 0 \leq j' \leq 2^{e_{n+1}} - a', f_{a',j'} = 1 \right\} \\ &= \left\{ b - z'2^{e_n} - (r_a - a - j) \mid 0 \leq j \leq 2^{e_n} - a, 0 \leq z' \leq 2^{\bar{e}_{n+1} - e_n} - 1 \right\} \\ &= T(a,b) \cup T(a, b - 2^{e_n}) \cup \cdots \cup T(a, b - (2^{\bar{e}_{n+1} - e_n} - 1)2^{e_n}). \end{aligned}$$

(c) Por el Corolario 2.3.19 (c) tenemos que si $T(a,b) = \{b, b-b_1, \ldots, b-b_k\}$, entonces $T(2^{m'}a, b) = \{b, b-2^{m'}b_1, \ldots, b-2^{m'}b_k\}$.

□

2.6. Relaciones para valores pequeños de a

En esta sección probaremos que los conjuntos $S(a,b)$ se pueden encontrar recursivamente para $1 \leq a \leq p$; también probaremos algunas de las conjeturas para valores pequeños de a formuladas en [Tha09b, Lar10].

Los siguientes resultados serán usados en esta sección.

Teorema 2.6.1. *Sea k un entero positivo. Sea $\ell(k)$ la suma de los dígitos de k en base q.*

a) *Si $d > \ell(k)/(q-1)$, entonces $S_d(-k) = 0$ ([Lee43, Lema 7.1]; vea también [Gek88, Corolario 2.12]).*

b) *$S_d(-(q^{k+d}-1)) = (-1)^d D_{d+k}/L_d D_k^{q^d}$ ([Car39], [Gek88, Teorema 4.1]).*

En particular, cuando $d = 1$, tenemos que $S_1(-(q-1)) = -1$.

A continuación probamos la Conjetura 4.3.1 formulada en [Tha09b].

Teorema 2.6.2. *Para cualquier q, se tiene,*

$$\zeta(1)\zeta(b) = \zeta(1+b) + \zeta(1,b) + \zeta(b,1) + \sum_{i=0}^{\sigma-1} \zeta(b-\phi(i), 1+\phi(i)),$$

donde $\phi(i)$ y r_1 son como en la Definición 1.4.5, *y $b = r_1\sigma + \beta, 0 < \beta \leq r_1$.*

Demostración. Sea $a = 1$. Entonces, $r_1 = q-1$. Por el Teorema 2.3.14 tenemos que $\Delta(1, b+r_1) - \Delta(1,b) = S_1(1+b)$. Ahora, $\Delta(1,b) = 0$ para $1 \leq b \leq q-1$, porque $1+b \leq q$ [Tha09b, Teorema 1]. Por lo tanto, para cualquier $b \in \mathbb{Z}_+$, $\Delta(1,b) = \sum_{i=0}^{\sigma-1} S_1(b-\phi(i))$. El teorema se sigue del Teorema 1.4.2. □

Observación 2.6.3. En [Tha09b], el Teorema 2.6.2 fue probado para $q = 2$ y b arbitraria, y también para q general y b "par".

A continuación aplicaremos el Teorema 2.3.14 a valores pequeños de a.

Teorema 2.6.4. *Sean $a, b \in \mathbb{Z}_+$. Sea r_a como en la Definición* 1.4.5. *Si $2 \leq a \leq p$, entonces*

$$\Delta(a, b+r_a) - \Delta(a,b) = \sum_{j=1}^{p-a} f_{a,j} S_1(a+b+(p-j)(q-1)) + S_1(a+b),$$

donde $f_{a,j} = \binom{a+j-1}{j} = \binom{a+j-1}{a-1}$ es distinto de cero para cualquier j. En particular, los conjuntos $S(a,b)$, $2 \leq a \leq p$, se pueden hallar recursivamente con longitud de recursión r_a:

$$S(a, b+r_a) = S(a,b) \cup T(a, b+r_a),$$

donde

$$T(a, b + r_a) = \{(1, a + b)\} \cup \{(f_{a,j}, a + b + (p - j)(q - 1)) \mid 1 \le j \le p - a\}.$$

Demostración. De acuerdo con el Teorema 2.3.14, es suficiente probar que $j + i_j p = (p - j)(q - 1)$ si $j > 1$, y 0 en otro caso. Dado que $2 \le a \le p$, tenemos $m = 1$, $r_a = p(q - 1)$, y $t_a = p - (a - 1)$. Sea $1 \le j \le p - a$. Como $p \le q$ y $1 \le j$, se tiene que $p \le jq$ o equivalentemente $1 \le j(q/p)$. Por lo tanto, $q - 1 - j(q/p) \le q - 2$. Por otro lado se tiene que $p \le aq$ porque $p \le q$ y $1 < a$. Así $j \le p - a \le p - p/q = (p/q)(q - 1)$; se sigue que $0 \le q - 1 - j(q/p)$. Ya que

$$j + (q - 1 - j(q/p))p = (p - 1)(q - 1) \equiv 0 \text{ mód } (q - 1),$$

tenemos que $i_j = q - 1 - j(q/p)$ si $j > 1$, y $i_j = 0$ en otro caso. Note que por el Teorema de Lucas tenemos que $f_{a,j} \neq 0$. Más aún,

$$\begin{aligned}
f_{a,j} &= \binom{p-a}{j}(-1)^j \\
&= (-1)^j \frac{(p-a)(p-a-1)\cdots(p-a-(j-1))}{j!} \\
&= (-1)^j \frac{(-a)(-a-1)\cdots(-a-(j-1))}{j!} \\
&= (-1)^j(-1)^j \frac{a(a+1)\cdots(a+(j-1))}{j!} \\
&= \binom{a+j-1}{j}.
\end{aligned}$$

□

A continuación aplicaremos el Teorema 2.6.4 a $a = 2$ y $p = 2$ para probar la Conjetura 1.5.1.

Teorema 2.6.5. *Sea q una potencia de $p = 2$. Sean r_2, $\phi(i, j)$ e $\operatorname{Int}(\cdot)$ como en la Definición 1.4.5. Escribamos $b = r_2\sigma + \beta$, $0 < \beta \le r_2$. Entonces*

$$\begin{aligned}
\zeta(2)\zeta(b) = \zeta(2 + b) &+ \zeta(2, b) + \zeta(b, 2) \\
&+ \sum_{i=0}^{\sigma-1} \zeta(b - \phi(i, 0), 2 + \phi(i, 0)) + \operatorname{Int}\left(\frac{b}{q-1}\right)\frac{b}{q-1}\zeta(2, b).
\end{aligned}$$

Demostración. De acuerdo con el Teorema 1.4.2, es suficiente probar que $\Delta(2, b) = D(2, b)$, donde

$$D(2, b) = \sum_{i=0}^{\sigma-1} S_1(b - \phi(i, 0)) + \operatorname{Int}\left(\frac{b}{q-1}\right)\frac{b}{q-1}S_1(2).$$

Note que $b + r_2 = r_2(\sigma + 1) + \beta$; también $b + r_2 - \phi(i, 0) = b - \phi(i - 1, 0)$. Se tiene

$$\begin{aligned}
D(2, b + r_2) &= \sum_{i=0}^{\sigma} S_1(b - \phi(i - 1, 0)) + \operatorname{Int}\left(\frac{b + r_2}{q-1}\right)\frac{b + r_2}{q-1}S_1(2) \\
&= \sum_{i=-1}^{\sigma-1} S_1(b - \phi(i, 0)) + \operatorname{Int}\left(\frac{b + r_2}{q-1}\right)\frac{b + r_2}{q-1}S_1(2).
\end{aligned}$$

Dado que $q-1$ divide a r_2, $q-1$ divide a b si y sólo si $q-1$ divide a $b+r_2$; también $b-\phi(-1,0)=2+b$. Entonces $D(2,b+r_2)-D(2,b)=S_1(2+b)$. Por otro lado, dado que $a=p$, por el Teorema 2.6.4, se tiene $\Delta(2,b+r_2)-\Delta(2,b)=D(2,b+r_2)-D(2,b)$.

Calculemos ahora $\Delta(2,b)$ para $1\le b\le r_2$. Procediendo como en la prueba del Teorema 2.3.14,

$$\begin{aligned}
\Delta(2,b) &= \sum_{n_2\in A_{1+}} \frac{1}{n_2^b} \sum_{\substack{n_1\neq n_2\\ n_1\in A_{1+}}} \frac{1}{n_1^2}\\
&= \sum_{n_2\in A_{1+}} \frac{1}{n_2^b}\left(S_1(2)-\frac{1}{n_2^2}\right)\\
&= \frac{1}{[1]^2}\sum_{n_2\in A_{1+}} \frac{1}{n_2^b}\left(1-\frac{[1]^2}{n_2^2}\right)\\
&= S_1(2)S_1(-(r_2-b)).
\end{aligned}$$

Si $b=r_2=2(q-1)$, entonces $S_1(0)=0$. Si $b=q-1$, entonces, por el Teorema 2.6.1 (b), se sigue que $S_1(-(q-1))=-1$. Supongamos que $1\le b<q-1$. Entonces $r_2-b=(q-2-b)+q$ es la descomposición en base q de r_2-b. Puesto que $\ell(r_2-b)<q-1$, del Teorema 2.6.1 (a) se sigue que $S_1(-(r_2-b))=0$. Ahora, si $q-1<b<r_2$, escribamos $b=(q-1)+\rho$ donde $0<\rho<q-1$. Entonces $r_2-b=q-1-\rho$ es la descomposición en base q de r_2-b. Aplicando otra vez el Teorema 2.6.1 (a) tenemos que $S_1(-(r_2-b))=0$. De aquí que,

$$\Delta(2,b)=\begin{cases}0 & \text{si } b\neq(q-1)\\ S_1(2) & \text{si } b=q-1.\end{cases}$$

Por lo tanto, $\Delta(2,b)=D(2,b)$ para $b=1,\dots,r_2$. Esto concluye la prueba. □

A continuación probaremos al mismo tiempo las Conjeturas 1.5.1 y 1.5.5. De hecho, la Conjetura 1.5.5 se convierte en la Conjetura 1.5.1 cuando $p=2$.

Sea q una potencia de p. Sea $b\in\mathbb{Z}_+$ y $0\le j\le p-1$. Dado que

$$\begin{aligned}
\phi(i,p-1-j) &= r_2(1+i)-2-(p-1-j)(q-1)\\
&= (pi+1+j)(q-1)-2,
\end{aligned}$$

la condición $b-\phi(i,p-1-j)>2$ es equivalente a $n(b,j)\ge i$, donde $n(b,j)=\left\lfloor\frac{b-1-(1+j)(q-1)}{r_2}\right\rfloor$. Más precisamente,

$$\begin{aligned}
b-\phi(i,p-1-j)>2 &\Longleftrightarrow b-\phi(i,p-1-j)\ge 3\\
&\Longleftrightarrow b-(pi+1+j)(q-1)+2\ge 3\\
&\Longleftrightarrow \frac{b-1}{q-1}\ge pi+1+j.
\end{aligned}$$

Ahora, tomemos $p=2$ y escribamos $b=r_2\sigma+\beta$, $0<\beta\leq r_2$.

$$\begin{aligned} n(b,p-1)=n(b,1)&=\left\lfloor \frac{b-1-2(q-1))}{r_2}\right\rfloor \\ &=\left\lfloor \frac{r_2\sigma+\beta-1-r_2}{r_2}\right\rfloor \\ &=\left\lfloor \sigma-1+\frac{\beta-1}{r_2}\right\rfloor \\ &=\sigma-1. \end{aligned}$$

Dado que $2=0$ y $3=1$ en $\mathbb{F}_2$, la Conjetura 1.5.5 se convierte en la Conjetura 1.5.1:

$$\begin{aligned} \sum_{j=0}^{1}(j+2)\sum_{i=0}^{\sigma-1} & S_d(b-\phi(i,1-j),2+\phi(i,1-j))+\operatorname{Int}\left(\tfrac{b}{q-1}\right)\tfrac{b}{q-1}S_d(2,b) \\ &=3\sum_{i=0}^{\sigma-1}S_d(b-\phi(i,0),2+\phi(i,0))+\operatorname{Int}\left(\tfrac{b}{q-1}\right)\tfrac{b}{q-1}S_d(2,b) \\ &=\sum_{i=0}^{\sigma-1}S_d(b-\phi(i,0),2+\phi(i,0))+\operatorname{Int}\left(\tfrac{b}{q-1}\right)\tfrac{b}{q-1}S_d(2,b). \end{aligned}$$

A continuación la prueba de la Conjetura 1.5.5.

Teorema 2.6.6. *Sea p cualquier número primo y q una potencia de p. Entonces*

$$\begin{aligned} \zeta(2)\zeta(b)=\zeta(2+b)&+\zeta(2,b)+\zeta(b,2) \\ &+\sum_{j=0}^{p-1}(j+2)\sum_{b-\phi(i,p-1-j)>2}\zeta(b-\phi(i,p-1-j),2+\phi(i,p-1-j)) \\ &\qquad+\operatorname{Int}\left(\frac{b}{q-1}\right)\frac{b}{q-1}\zeta(2,b), \end{aligned}$$

donde $\phi(i,k)$ e $\operatorname{Int}(\cdot)$ son como en la Definición 1.4.5.

Demostración. Sea $f_b=\operatorname{Int}\left(\frac{b}{q-1}\right)\frac{b}{q-1}$. De acuerdo con el Teorema 1.4.2, es suficiente probar que $\Delta(2,b)=D(2,b)$, donde

$$D(2,b)=\sum_{j=0}^{p-1}(j+2)\sum_{i=0}^{n(b,j)}S_1(b+2-(pi+1+j)(q-1))+f_bS_1(2). \tag{2.6.6.1}$$

Tenemos que $b+r_2+2-(pi+1+j)(q-1)=b+2-(p(i-1)+1+j)(q-1)$ y

$n(b+r_2,j)=n(b,j)+1$. Entonces

$$\begin{aligned}
D(2,b+r_2) &= \sum_{j=0}^{p-1}(j+2)\sum_{i=0}^{n(b+r_2,j)} S_1(b+r_2+2-(pi+1+j)(q-1))+f_{b+r_2}S_1(2)\\
&= \sum_{j=0}^{p-1}(j+2)\sum_{i=0}^{n(b+r_2,j)} S_1(b+2-(p(i-1)+1+j)(q-1))+f_{b+r_2}S_1(2)\\
&= \sum_{j=0}^{p-1}(j+2)\sum_{i=-1}^{n(b,j)} S_1(b+2-(pi+1+j)(q-1))+f_{b+r_2}S_1(2).
\end{aligned}$$

Ahora, $q-1$ divide a b si y sólo si $q-1$ divide a $b+r_2$ porque $q-1$ divide a r_2. Por lo tanto,

$$\begin{aligned}
D(2,b+r_2)-D(2,b) &= \sum_{j=0}^{p-1}(j+2)S_1(2+b+(p-(j+1))(q-1))\\
&= \sum_{j=1}^{p}(j+1)S_1(2+b+(p-j)(q-1)).
\end{aligned}$$

Por otro lado, $f_{2,j}=\binom{j+1}{1}=j+1$ para $1\leq j\leq p-2$, $j+1=0$ cuando $j=p-1$, y $j+1=1$ cuando $j=p$. Del Teorema 2.6.4, se sigue que

$$\begin{aligned}
\Delta(2,b+r_2)-\Delta(2,b) &= \sum_{j=1}^{p-2} f_{2,j}S_1(2+b+(p-j)(q-1))+S_1(2+b)\\
&= D(2,b+r_2)-D(2,b).
\end{aligned}$$

Para finalizar la prueba, probaremos que $\Delta(2,b)=D(2,b)$ para $1\leq b\leq r_2$. Sea $1\leq b\leq r_2$. Si $n(b,j)\geq 1$, entonces $r_2\geq b\geq r_2+(1+j)(q-1)+1$ que implica la contradicción $0\geq (1+j)(q-1)+1\geq 1$. Así, $n(b,j)<1$. Ahora, $n(b,j)=0$ si y sólo si $b-1-(1+j)(q-1)\geq 0$. Así, la Ecuación (2.6.6.1) se convierte en

$$D(2,b)=\sum_{j=0}^{\left\lfloor\frac{b-q}{q-1}\right\rfloor}(j+2)S_1(b+2-(1+j)(q-1))+f_bS_1(2). \tag{2.6.6.2}$$

Escribamos $b=\lambda(q-1)+\rho$ donde $0\leq\rho<q-1$. Si $\rho=0$, tomemos $l=\lambda-1$; si $\rho>0$, sea $l=\lambda$. Así, l es el entero en el conjunto $\{0,1,\ldots,p-1\}$ tal que $l(q-1)+1\leq b\leq (l+1)(q-1)$. Entonces,

$$(l-1)(q-1)\leq b-q\leq l(q-1)-1<l(q-1).$$

Por lo tanto, $\left\lfloor \frac{b-q}{q-1} \right\rfloor = l-1$. Ahora, reescribimos la Ecuación (2.6.6.2) como sigue:

$$\begin{aligned} D(2,b) &= \sum_{n\in A_{1+}} \sum_{j=0}^{l-1} \frac{j+2}{n^{b+2-(1+j)(q-1)}} + \sum_{n\in A_{1+}} \frac{f_b}{n^2} \\ &= \sum_{n\in A_{1+}} \frac{1}{n^{b+2-(q-1)}} \left(\sum_{j=0}^{l-1} \frac{(j+2)n^{b+2-(q-1)}}{n^{b+2-(1+j)(q-1)}} + f_b n^{b-(q-1)} \right) \\ &= \sum_{n\in A_{1+}} \frac{P_n}{n^{b+2-(q-1)}}, \end{aligned}$$

donde $P_n = \sum_{j=0}^{l-1} (j+2)n^{j(q-1)} + f_b n^{b-(q-1)}$. Dado

$$\Delta(2,b) = \sum_{n\in A_{1+}} \frac{1}{n^b} \left(\sum_{n\in A_{1+}} \frac{1}{n^2} - \frac{1}{n^2} \right) = \sum_{n\in A_{1+}} \frac{1}{n^b} \left(\frac{1}{[1]^2} - \frac{1}{n^2} \right),$$

obtenemos

$$\begin{aligned} \Delta(2,b) - D(2,b) &= \sum_{n\in A_{1+}} \left(\frac{n^2-[1]^2}{n^{b+2}[1]^2} - \frac{P_n}{n^{b+2-(q-1)}} \right) \\ &= \sum_{n\in A_{1+}} \frac{n^2-[1]^2-n^{q-1}[1]^2P_n}{n^{b+2}[1]^2}. \end{aligned}$$

Ahora calcularemos $(n^{q-1}-1)^2P_n$. Primeramente, notemos que

$$\begin{aligned} n^{2(q-1)} \sum_{j=0}^{l-1} (j+2)n^{j(q-1)} &= \sum_{j=0}^{l-1} (j+2)n^{(j+2)(q-1)}, \\ -2n^{q-1} \sum_{j=0}^{l-1} (j+2)n^{j(q-1)} &= -\sum_{j=0}^{l-1} 2(j+2)n^{(j+1)(q-1)} \\ &= -\sum_{j=-1}^{l-1} 2(j+3)n^{(j+2)(q-1)}, \end{aligned}$$

y

$$\sum_{j=0}^{l-1} (j+2)n^{j(q-1)} = \sum_{j=-2}^{l-1} (j+4)n^{(j+2)(q-1)}.$$

Por lo tanto, $(n^{q-1}-1)^2P_n$ es igual a

$$2 - n^{q-1} - (l+2)n^{l(q-1)} + (l+1)n^{(l+1)(q-1)} + (n^{q-1}-1)^2 f_b n^{b-(q-1)}.$$

Dado que $n^{q-1}[1]^2P_n = n^{q+1}(n^{q-1}-1)^2P_n$, se sigue que $n^{q-1}[1]^2P_n$ es igual a

$$2n^{q+1} - n^{2q} - (l+2)n^{(l+1)(q-1)+2} + (l+1)n^{(l+2)(q-1)+2} + n^{q-1}[1]^2 f_b n^{b-(q-1)}.$$

Usando que $n^2 - [1]^2 = -n^{2q} + 2n^{q+1}$, obtenemos

$$\begin{aligned} n^2 - [1]^2 - n^{q-1}[1]^2P_n = (l+2)&n^{(l+1)(q-1)+2} \\ &- (l+1)n^{(l+2)(q-1)+2} - n^{q-1}[1]^2 f_b n^{b-(q-1)}. \end{aligned}$$

Dividiendo $n^2 - [1]^2 - n^{q-1}[1]^2P_n$ por n^{b+2} obtenemos

$$\frac{n^2 - [1]^2 - n^{q-1}[1]^2P_n}{n^{b+2}} = (l+2)n^{(l+1)(q-1)-b} - (l+1)n^{(l+2)(q-1)-b} - \frac{[1]^2 f_b}{n^2}.$$

Sumando sobre todas las $n \in A_{1^+}$, obtenemos

$$[1]^2\left(\Delta(2,b) - D(2,b)\right) = (l+2)S_1(-k_1) - (l+1)S_1(-k_2) - f_b,$$

donde $k_1 = (l+1)(q-1)-b$ y $k_2 = (l+2)(q-1)-b$. Ahora, si $b \equiv 0 \text{ mód } (q-1)$, entonces $l = \frac{b}{q-1} - 1$. Así $k_1 = 0$ y $k_2 = q-1$. Del Teorema 2.6.1 (b) tenemos que $S_1(-(q-1)) = -1$. Dado que $S_1(0) = 0$ y $f_b = \frac{b}{q-1} = l+1$, se sigue que $(\Delta(2,b) - D(2,b)) = 0$. Supongamos que $b \not\equiv 0 \text{ mód } (q-1)$. Entonces, $f_b = 0$. En este caso, $b = l(q-1)+\rho$ con $0 < \rho < q-1$. Por lo tanto, $k_1 = q-1-\rho$ y $k_2 = (q-2-\rho)+q$. Note que las expresiones anteriores para k_1 y k_2 son sus descomposiciones en base q porque $q-1-\rho < q-1$ y $q-2-\rho < q-1$. Entonces, $\ell(k_1) = \ell(k_2) = q-1-\rho$. Puesto que $\ell(k_1) = \ell(k_2) < (q-1)$, del Teorema 2.6.1 (a), se sigue que $S_1(-k_1) = S_1(-k_2) = 0$. Por lo tanto, $\Delta(a,b) - D(2,b) = 0$ para $1 \leq b \leq r_2$. Esto concluye la prueba. □

A continuación, probaremos la Conjetura 1.5.2.

Teorema 2.6.7. *Sea $q = 2$. Para $b \in \mathbb{Z}_+$, se tiene*

$$\begin{aligned} \zeta(3)\zeta(b) = \zeta(b+3) &+ \zeta(3,b) + \zeta(b,3) \\ &+ \sum_{i=0}^{\lfloor (b-5)/4 \rfloor} \zeta(b-1-4i, 4+4i) + \sum_{i=0}^{\lfloor (b-4)/4 \rfloor} \zeta(b-4i, 3+4i) \\ &+ \sum_{i=1}^{2} \operatorname{Int}\left(\frac{b-i}{r_3}\right)(\zeta(2,b+1) + \zeta(3,b)). \end{aligned}$$

Demostración. Es suficiente probar que $\Delta(3,b) = D(3,b)$, donde

$$\begin{aligned} D(3,b) = \sum_{i=0}^{\lfloor (b-5)/4 \rfloor} S_1(b-1-4i) &+ \sum_{i=0}^{\lfloor (b-4)/4 \rfloor} S_1(b-4i) \\ &+ \sum_{i=1}^{2} \operatorname{Int}\left(\frac{b-i}{r_3}\right)(S_1(2) + S_1(3)). \end{aligned}$$

Sea $a = 3$. Entonces, $m = 2$, $r_3 = 4$, $p^m - a = 1$. El mapeo $i_j\colon \{0,1\} \to \{0\}$ está dado por $i_0 = i_1 = 0$; también $f_{2,1} = \binom{p^m-a}{1}(-1)^1 = 1$. Por el Teorema 2.3.14, se tiene que $\Delta(3, b+4) - \Delta(3, b) = S_1(3+b+1) + S_1(3+b)$. Otra prueba de este hecho es la siguiente. Tenemos que

$$\begin{aligned}\Delta(3, b+4) - \Delta(3, b) &= \sum_{n\in A_{1+}} \frac{1}{n^{b+4}}\left(S_1(3) - \frac{1}{n^3}\right) - \sum_{n\in A_{1+}} \frac{1}{n^b}\left(S_1(3) - \frac{1}{n^3}\right)\\ &= \sum_{n\in A_{1+}} \frac{1}{n^{b+4}}\left(S_1(3) - \frac{1}{n^3} - n^4 S_1(3) - n\right).\end{aligned}$$

Por otro lado,

$$S_1(3) = \frac{1}{[1]^3} + \frac{1}{[1]^2} = \frac{1+[1]}{[1]^3} = \frac{1+n(n+1)}{n^3(n+1)^3}.$$

Entonces,

$$\begin{aligned}S_1(3) - \frac{1}{n^3} - n^4 S_1(3) &= \frac{1}{[1]^3}\left(1 + n(n+1) + (n+1)^3 + n^4(1+n(n+1))\right)\\ &= \frac{1}{n^3(n+1)^3}\left(n^3 + n^4 + n^5 + n^6\right) = \frac{n^3(n+1)^3}{n^3(n+1)^3} = 1.\end{aligned}$$

Usando el hecho que $\lfloor x+1\rfloor = \lfloor x\rfloor + 1$, obtenemos $\lfloor (b-5)/4\rfloor = \lfloor (b-1)/4\rfloor - 1$ y $\lfloor (b-4)/4\rfloor = \lfloor b/4\rfloor - 1$. Entonces

$$\sum_{i=0}^{\lfloor (b-1)/4\rfloor} S_1(b+4-1-4i) = \sum_{i=0}^{\lfloor (b-1)/4\rfloor} S_1(b-1-4(i-1)) = \sum_{i=-1}^{\lfloor (b-5)/4\rfloor} S_1(b-1-4i),$$

$$\sum_{i=0}^{\lfloor b/4\rfloor} S_1(b+4-4i) = \sum_{i=0}^{\lfloor b/4\rfloor} S_1(b-4(i-1)) = \sum_{i=-1}^{\lfloor (b-4)/4\rfloor} S_1(b-4i).$$

Como $(b-i) \equiv 0 \bmod 4$ si y sólo si $(b+4-i) \equiv 0 \bmod 4$, se sigue que

$$D(3, b+4) - D(3, b) = S_1(b+3) + S_1(b+4) = \Delta(3, b+4) - \Delta(3, b).$$

Un cálculo directo prueba que $\Delta(3, b) = D(3, b)$ para $b = 1, 2, 3, 4$. Esto completa la prueba. □

Observación 2.6.8. Sean $q = 2$ y $a = 3$. En este caso, $\phi(i, j) = 1 - j + 4i$. La condición $b - \phi(i, 0) > 3$ es equivalente a $i \le (b-5)/4$. Como $j_{3,\text{máx}} = 1$, la condición $b - \phi(i, j_{3,\text{máx}}) > 3$ es equivalente a $i \le (b-4)/4$. Por lo tanto la prueba del Teorema 2.6.7 confirma la Conjetura 1.5.2.

Proposición 2.6.9. *Sean $p = 2$ y $q = p^s$ con $s > 1$. Entonces $\Delta(3, b + r_3) - \Delta(3, b) = D(3, b + r_3) - D(3, b)$ para toda $b \in \mathbb{Z}_+$, donde*

$$
\begin{aligned}
D(3,b) = \sum_{i=0}^{\frac{b-1-r_3}{r_3}} S_1(b-\phi(i,0)) &+ \sum_{i=0}^{\frac{b-q}{r_3}} S_1(b-\phi(i,3)) \\
&+ \operatorname{Int}\left(\frac{b+1}{q-1}\right)\binom{(b+1)/(q-1)+1}{2} S_1(2) \\
&\qquad + \operatorname{Int}\left(\frac{b}{q-1}\right)\left(\binom{b/(q-1)+2}{2} - 1\right) S_1(3).
\end{aligned}
$$

Demostración. Sea $a = 3$. Entonces, $m = 2$, $p^m - a = 1$. Note que $3q - 4 \equiv 0$ mód 4, y $1 + \left(\frac{3q-4}{4}\right) 4 = 3(q-1) \equiv 0$ mód $(q-1)$. Así, el mapeo $i_j \colon \{0,1\} \to \{0,1,\ldots,q-2\}$ está dado por $i_0 = 0$ y $i_1 = (3q-4)/4$. Por lo tanto,

$$
\Delta(3, b + r_3) - \Delta(3, b) = S_1(3 + b + 3(q-1)) + S_1(3 + b).
$$

Por otro lado, se tiene que $\left\lfloor \frac{b-1-r_3}{r_3} \right\rfloor = \left\lfloor \frac{b-1}{r_3} \right\rfloor - 1$ y $\left\lfloor \frac{b-q}{r_3} \right\rfloor = \left\lfloor \frac{b+r_3-q}{r_3} \right\rfloor - 1$, porque $\lfloor x \pm 1 \rfloor = \lfloor x \rfloor \pm 1$. Claramente, $b+1 \equiv 0$ mód $(q-1)$ si y sólo si $b+r_3+1 \equiv 0$ mód $(q-1)$. Análogamente, $b \equiv 0$ mód $(q-1)$ si y sólo si $b + r_3 \equiv 0$ mód $(q-1)$. Luego,

$$
\begin{aligned}
D(3, b + r_3) - D(3, b) &= S_1(b - \phi(-1, 0)) + S_1(b - \phi(-1, 3)) \\
&= S(b + 3) + S_1(b + 3 + 3(q-1)) \\
&= \Delta(3, b + r_3) - \Delta(3, b).
\end{aligned}
$$

□

Observación 2.6.10. Si $a = 3$, entonces $r_3 = 4(q-1)$ y $j_{3,\text{máx}} = \left\lfloor \frac{r_3-3}{r_3} \right\rfloor = \left\lfloor 4 - \frac{3}{q-1} \right\rfloor = 3$. Las condiciones $b - \phi(i,0) > 3$ e $i \leq \frac{b-1-r_3}{r_3}$ son equivalentes así como también lo son las condiciones $b - \phi(i,3) > 3$ e $i \leq \frac{b-1-(q-1)}{r_3}$. Por lo tanto, para probar la Conjetura 1.5.3, solamente falta probar que $\Delta(3,b) = D(3,b)$ para $b = 1, 2, \ldots, 4(q-1)$.

Proposición 2.6.11. *Sea q una potencia de $p = 2$. Entonces $\Delta(4, b + r_3) - \Delta(4, b) = D(4, b + r_3) - D(4, b)$ para toda $b \in \mathbb{Z}_+$, donde*

$$
\begin{aligned}
\Delta(4,b) = \sum_{i=0}^{\frac{b-r_4-1}{r_4}} S_1(b-\phi(i,0)) &+ \operatorname{Int}\left(\frac{b-\text{máx}\{q-3,1\}}{r_4}\right) S_1(2) \\
&+ \operatorname{Int}\left(\frac{b-2q+3}{r_4}\right) S_1(3) + \sum_{i=1}^{3} \operatorname{Int}\left(\frac{b-i(q-1)}{r_4}\right) S_1(4).
\end{aligned}
$$

Demostración. La prueba de esta proposición es análoga a la prueba de la Proposición 2.6.9, por lo que omitimos su justificación. □

2.7. Una relación para índices grandes

En esta sección suponemos que $q = p^s$ para algún $s \geq 1$. Probaremos la Conjetura 1.5.7.1 en tres formas diferentes.

Proposición 2.7.1.

$$S_1(2q^n - 1) = -\frac{1}{[1]^{2q^n-1}}\frac{[1+n]}{[1]} = -\frac{[n+1]}{[1]^{2q^n}}.$$

Demostración. Probaremos que para cualquier k_1, $0 \leq k_1 \leq 2q^{n-1} - 1$,

$$\binom{2q^n - 2 - k_1(q-1)}{k_1}(-1)^{k_1} = \begin{cases} 1 & \text{si } k_1 \in \{0, 1, 1+q, \ldots, 1+q+\cdots+q^{n-1}\}, \\ 0 & \text{en otro caso.} \end{cases}$$

Por el Teorema de Lucas, sólo necesitan ser tomados en cuenta aquellos términos en los que no hay acarreo en base p en la suma de k_1 y $2q^n - 2 - k_1 q$. La descomposición en base p de $2q^{n-1} - 1$ es

$$\begin{aligned} 2q^{n-1} - 1 = q^{n-1} - 1 + q^{n-1} = p^{s(n-1)} - 1 + p^{s(n-1)} &= (p-1)\sum_{i=0}^{s(n-1)-1} p^i + p^{s(n-1)} \\ &= (p-1) + (p-1)p + \cdots + (p-1)p^{s(n-1)-1} + p^{s(n-1)}. \end{aligned}$$

Sea $k_1 = a_0 + a_1 p + \cdots + a_{s(n-1)-1}p^{s(n-1)-1} + a_{s(n-1)}p^{s(n-1)}$ la descomposición en base p de $0 \leq k_1 \leq 2q^{n-1} - 1$, donde $a_{s(n-1)} \in \{0, 1\}$. Por lo tanto, la descomposición en base p de $k_1 q$ es $a_0 p^s + a_1 p^{s+1} + \cdots + a_{s(n-1)-1}p^{sn-1} + a_{s(n-1)}p^{sn}$. Finalmente, la descomposición en base p de $2q^n - 2$ es

$$\begin{aligned} 2q^n - 2 &= -1 + q^n - 1 + q^n \\ &= -1 + (p-1) + (p-1)p + \cdots + (p-1)p^{sn-1} + p^{sn} \\ &= (p-2) + (p-1)p + \cdots + (p-1)p^{sn-1} + p^{sn}. \end{aligned}$$

Denotemos con b_i a los dígitos de $2q^n - 2 - k_1 q$. Dado que los primeros s dígitos de $2q^n - 2$ son $p-2, p-1, \ldots, p-1$, los primeros s dígitos $k_1 q$ son cero, y $k_1 q + (2q^n - 2 - k_1 q) = 2q^n - 2$:

$$\begin{array}{rrrrrrr} p-2+ & (p-1)p+ & \cdots + (p-1)p^{s-1}+ & b_s p^s + & b_{s+1}p^{s+1} & + \cdots + & b_{sn}p^{sn} \\ 0+ & 0p+ & \cdots + \quad 0p^{s-1}+ & a_0 p^s + & a_1 p^{s+1} & + \cdots + & a_{s(n-1)}p^{sn} \\ \hline p-2+ & (p-1)p+ & \cdots + (p-1)p^{s-1}+ & (p-1)p^s + & (p-1)p^{s+1} & + \cdots + & p_{sn} \end{array}$$

Se sigue que los primeros s dígitos de $2q^n - 2 - k_1 q$ son $b_0 = p - 2$ y $b_i = p - 1$, $1 \leq i \leq s - 1$. A continuación determinamos los restantes b_i's suponiendo que no hay acarreo en la suma de $2q^n - 2 - k_1 q$ y k_1:

$$\begin{array}{rlllllll} 2q^n - 2 - k_1 q: & p-2+ & (p-1)p+ & \cdots + (p-1)p^{s-1} & + b_s p^s & + b_{s+1}p^{s+1} & + \cdots \\ k_1: & a_0 & + a_1 p & + \cdots + a_{s-1}p^{s-1} & + a_s p^s & + a_{s+1}p^{s+1} & + \cdots \end{array}$$

De la suposición se sigue inmediatamente que $a_i = 0$ para $1 \leq i \leq s-1$. Así, $b_{s+1} = \cdots = b_{2s-1} = p-1$. Usando otra vez que no hay acarreo en la suma de k_1 y $2q^n - 2 - k_1 q$ obtenemos $a_{s2-1} = \cdots = a_{3s-1} = 0$ y por lo tanto, $b_{2s+1} = \cdots = b_{3s-1} = p-1$. Continuando de esta forma obtenemos que $k_1 = a_0 + a_s p^s + a_{2s}p^{2s} + \cdots + a_{(n-1)s}p^{(n-1)s}$. También, dado que $a_i + b_i \leq p-1$ y $a_i + b_{i+s} = p-1$, tenemos $b_i \leq b_{i+s}$. Como $b_0 = p-2$, concluimos que $a_{si} = 0$ o que $a_{si} = 1$ para $i = 0, 1, \ldots, (n-1)s$.

Razonando de la misma manera, concluimos que si $a_{si} = 0$ para algún i, entonces $a_{sj} = 0$ para $j > i$.

Ahora, si $k_1 = 0$, claramente $\binom{2q^n - 2 - k_1(q-1)}{k_1}(-1)^{k_1} = 0$. Supongamos que $k_1 = 1 + q + \cdots + q^i$ para algún $0 \leq i \leq n-1$. Entonces, $q^{i+1} - 1 = (1 + q + \cdots + q^i)(q-1)$. Por lo tanto,

$$2q^n - 2 - k_1(q-1) = 2q^n - 2 - (q^{i+1} - 1) = q^n - 1 + q^{i+1}(q^{n-i-1} - 1).$$

Los dígitos c_j de $2q^n - 2 - k_1(q-1)$ son

$$c_j = \begin{cases} p-2 & \text{si } j = s(i+1) \\ 1 & \text{si } j = sn, \\ p-1 & \text{de otra manera.} \end{cases}$$

Los dígitos de k_1 son $a_j = 1$ para $j = 0, s, \ldots, si$ y 0 en otro caso. Del Teorema de Lucas se tiene que

$$\binom{2q^n - 2 - k_1(q-1)}{k_1} \equiv \prod_{j=0}^{sn} \binom{c_j}{a_j} \text{ mód } p \equiv (p-1)^{i+1} \text{ mód } p \equiv (-1)^{i+1} \text{ mód } p.$$

Note que $i+1$ y k_1 tienen la misma paridad, así, en $\mathbb{F}_p$ se tiene que $\binom{2q^n-2-k_1 q}{k_1}(-1)^{k_1} = (-1)^{i+1+k_1} = 1$.

Dado que $(-1)^{2q^n-1} = -1$ para cualquier q, que $\left\lfloor \frac{2q^n-2}{q} \right\rfloor = 2q^{n-1} - 1$, y que $\sum_{i=0}^{n} [1]^{q^i} = [n+1]$, de la Ecuación (2.1.0.4) se sigue

$$\begin{aligned} S_1(2q^n - 1) &= -\frac{1}{[1]^{2q^n-1}} \left(1 + \sum_{k_1=1}^{2q^{n-1}-1} \binom{2q^n - 2 - k_1(q-1)}{k_1} (-1)^{k_1} [1]^{k_1(q-1)} \right) \\ &= -\frac{1}{[1]^{2q^n-1}} \left(1 + [1]^{q-1} + [1]^{q^2-1} + \cdots + [1]^{q^n-1} \right) \\ &= -\frac{[1]}{[1]^{2q^n}} \left(1 + [1]^{q-1} + [1]^{q^2-1} + \cdots + [1]^{q^n-1} \right) \\ &= -\frac{1}{[1]^{2q^n}} \left([1] + [1]^{q} + [1]^{q^2} + \cdots + [1]^{q^n} \right) = -\frac{[n+1]}{[1]^{2q^n}}. \end{aligned}$$ □

El siguiente teorema es válido para cualquier q.

Teorema 2.7.2. *Sea q general.*

$$\zeta(q^n)\zeta(q^n - 1) = \zeta(2q^n - 1) + \zeta(q^n - 1, q^n).$$

Demostración 1. De acuerdo con el Teorema 1.4.2 es suficiente probar que

$$S_1(q^n)S_1(q^n-1) = S_1(2q^n-1) - S_1(q^n).$$

De las Fórmulas (2.1.0.5) y (2.1.0.9), y de la Proposición 2.7.1 se tiene

$$\begin{aligned}
S_1(q^n)S_1(q^n-1) - S_1(2q^n-1) &= \frac{1}{\ell_1^{q^n}}\frac{[n]}{[1]\ell_1^{q^n-1}} + \frac{[n+1]}{[1]^{2q^n}} \\
&= -\frac{[n]}{[1]^{2q^n}} + \frac{[n+1]}{[1]^{2q^n}} \\
&= \frac{[n+1]-[n]}{[1]^{2q^n}} = \frac{[1]^{q^n}}{[1]^{2q^n}} \\
&= \frac{1}{[1]^{q^n}} = -S_1(q^n).
\end{aligned}$$

□

Demostración 2. De la definición de $\Delta(a,b)$, se sigue que

$$\begin{aligned}
\Delta(q^n, q^n-1) &= \sum_{a\in A_{1+}} \frac{1}{a^{q^n-1}}\left(S_1(q^n) - \frac{1}{a^{q^n}}\right) \\
&= \sum_{a\in A_{1+}} \frac{1}{a^{q^n-1}}\left(-\frac{1}{[1]^{q^n}} - \frac{1}{a^{q^n}}\right) \\
&= -\frac{1}{[1]^{q^n}} \sum_{a\in A_{1+}} a^{q^{n+1}-2q^n+1} \\
&= -\frac{1}{[1]^{q^n}} S_1(-(q^{n+1}-2q^n+1)) \\
&= S_1(q^n)S_1(-(q^{n+1}-2q^n+1)).
\end{aligned}$$

Para finalizar, probemos que $S_1(-N) = -1$ donde $N = q^{n+1} - 2q^n + 1$.

$$\begin{aligned}
S_1(-N) &= \sum_{\theta\in\mathbb{F}_q} (t+\theta)^N \\
&= t^N + \sum_{\theta\in\mathbb{F}_q^*} (t+\theta)^N \\
&= t^N + \sum_{l=0}^{N} \binom{N}{l} t^{N-l} \sum_{\theta\in\mathbb{F}_q^*} \theta^l.
\end{aligned}$$

Dado que la suma $\sum_{\theta\in\mathbb{F}_q^*}\theta^l$ es 0 si $q-1$ no divide a l, y -1 si $l \geq 0$ es divisible por $q-1$, y $N \equiv 0 \text{ mód } (q-1)$, obtenemos

$$S_1(-N) = -1 - \sum_{l=1}^{\frac{N}{q-1}-1} \binom{N}{l(q-1)} t^{N-l(q-1)}.$$

Sea $a = q^n - 1$; entonces $r_a = q^n(q-1)$, $r_a - a = N$, y $j_{a,\text{máx}} = N/(q-1)$. Por la Proposición 2.3.20, si $\binom{N}{l(q-1)} \neq 0$, entonces existe un j en el conjunto $\{0, 1, \ldots, q^n - a\} = \{0, 1\}$ tal que $j + i_j q^n \equiv 0 \text{ mód } (q-1)$. Ahora bien $1 = \binom{N}{0} = \binom{N}{N} \neq 0$; claramente $i_0 = 0$, y $i_1 = q - 2$ porque $N = 1 + (q-2)q^n$; de la Proposición 2.3.6 se sigue que $\binom{N}{l(q-1)} = 0$ para $1 \leq l < N/(q-1)$. Por lo tanto,

$$S_1(-N) = -1.$$

Esto completa la prueba. □

Demostración 3. Procedemos como en la prueba del Teorema 2.4.11. Sea $a = q^n$, $b = q^n - 1$, y $N = 1 + (q-2)q^n$. Para $\theta \in \mathbb{F}_q$ y $\mu \in \mathbb{F}_q^*$, tenemos que

$$\begin{aligned}
\frac{[1]^a}{(t+\theta)^a(t+\theta-\mu)^b} &= \left(\sum_{j=1}^{q-1} \mu^{q-1-j}(t+\theta)^{j-1}\right)^{q^n} (t+\theta-\mu) \\
&= \sum_{j=1}^{q-1} \mu^{q^n(q-1-j)}(t+\theta)^{q^n(j-1)}(t+\theta-\mu) \\
&= \sum_{j=1}^{q-1} \left(\mu^{q-1-j}(t+\theta)^{q^n(j-1)+1} - \mu^{q-j}(t+\theta)^{q^n(j-1)}\right).
\end{aligned}$$

Sumando sobre todas las $\theta \in \mathbb{F}_q$, $\mu \in \mathbb{F}_q^*$, obtenemos que

$$[1]^a \Delta(a,b) = \sum_{\theta \in \mathbb{F}_q} \sum_{j=1}^{q-1} \left((t+\theta)^{q^n(j-1)+1} \sum_{\mu \neq 0} \mu^{q-1-j} - (t+\theta)^{q^n(j-1)} \sum_{\mu \neq 0} \mu^{q-j} \right).$$

Por lo tanto,

$$[1]^a \Delta(a,b) = \sum_{\theta \in \mathbb{F}_q} \left(-(t+\theta)^N + 1\right) = -\sum_{\theta \in \mathbb{F}_q} (t+\theta)^N = -S_1(-N) = 1.$$

Entonces,

$$\Delta(q^n, q^n - 1) = \frac{1}{[1]^{q^n}} = -\left(\frac{-1}{[1]}\right)^{q^n} = -\frac{1}{\ell_1^{q^n}} = -S_1(q^n).$$

□

Observaciones 2.7.3.

(1) Podemos evitar usar las Proposiciones 2.3.20 y 2.3.6 como sigue.

Sea $q = p^s$ y sea $m = sn$. La descomposición en base p de N es

$$N = 1 + (p-2)p^m + (p-1)p^{m+1} + \cdots + (p-1)p^{m+s-1}.$$

Sea $l(q-1) = \sum_{k=0}^{m+s-1} b_k p^k$ la descomposición en base p de $l(q-1)$. Por el teorema de Lucas, la siguiente igualdad es válida en $\mathbb{F}_p$

$$\binom{N}{l(q-1)} = \binom{1}{b_0}\binom{0}{b_1}\cdots\binom{0}{b_{m-1}}\binom{p-2}{b_m}\binom{p-1}{b_{m+1}}\cdots\binom{p-1}{b_{m+s-1}}.$$

Por lo tanto, $\binom{N}{l(q-1)} \neq 0$ si y solamente si $b_0 \leq 1$, $b_k = 0$ para $k = 1, \ldots, m-1$, y $b_m \leq p-2$.

Dado que p^m y $q-1$ son primos relativos, p^m es una unidad en $\mathbb{Z}/(q-1)\mathbb{Z}$; así, la congruencia $j \equiv -\iota p^m$ mód $(q-1)$ siempre tiene solución. Más aún, hay exactamente una solución en el rango $0 \leq \iota < q-1$. Para $j = 0$ la solución es 0 y para $j = 1$ la solución es $q-2$ porque $N = 1 + (q-2)p^m \equiv 0$ mód $(q-1)$.

Si $\binom{N}{l(q-1)} \neq 0$, entonces $l(q-1) = j + ip^m$, $0 \leq j \leq 1$, $0 \leq i \leq q-2$, donde $i = \displaystyle\sum_{k=0}^{m+s-1} b_{m+k}p^k$. Dado que $l(q-1) > 0$, se sigue que $l(q-1) = N$. Entonces, $\binom{N}{l(q-1)} = 0$ para $1 \leq l < N/(q-1)$. Por lo tanto,

$$S_1(-N) = -\binom{N}{N} t^{N-N} = -1.$$

(2) En [Lar11], el árbitro sugirió que es fácil ver que $\binom{N}{l(q-1)} = 0$ para $1 \leq l < N/(q-1)$ sin usar la Proposición 2.3.20, comparando las expansiones de dos polinomios sobre $\mathbb{F}_q$. Sobre $\mathbb{F}_q$ se tiene

$$(1+x)^N = (1+x)(1+x^{q^n})^{q-2}.$$

Entonces,

$$\sum_{j=0}^{N} \binom{N}{j} x^j = \sum_{i=0}^{q-2} \binom{q-2}{i} \left(x^{iq^n} + x^{iq^n+1}\right).$$

Se sigue que $\binom{N}{j} = 0$ para $j \notin \{iq^n, iq^n+1 \mid 0 \leq i \leq (q-2)q^n\}$. En particular, iq^n y iq^n+1 no son divisibles por $q-1$ para $i = 0, \ldots, q-2$.

CAPÍTULO 3

Relaciones entre los valores multizeta en lugares no racionales

3.1. Introducción

En 1775, Euler introdujo los valores multizeta, esto más de 30 años después de que introdujera los valores zeta. Los valores multizeta han resurgido con renovado interés dado que tienen conexión con otras partes de las matemáticas, por ejemplo, con el programa Grothendieck-Ihara para estudiar el grupo absoluto de Galois a través del grupo fundamental de la recta proyectiva menos tres puntos. Dado que el producto de dos valores multizeta es una combinación lineal de valores multizeta, se sigue que el $\mathbb{Q}$-espacio lineal generado por todos los valores multizeta es una $\mathbb{Z}$-álgebra.

Dinesh Thakur [Tha04, Sección 5.10] define y estudia dos tipos de valores multizeta para campos de funciones, una con valores complejos y la otra con valores en las series de Laurent sobre campos finitos. El primer tipo de valores multizeta generaliza ciertos valores especiales de la función zeta de Artin-Weil. Específicamente, generaliza a la función zeta de Dedekind evaluada en números enteros. El segundo tipo de valores multizeta generaliza los valores zeta de Carlitz. Para $\mathbb{F}_q[t]$, el primer caso está completamente estudiado en [Tha04]. Aquí nos enfocaremos en el segundo tipo de generalización.

Ha sido probado que los valores multizeta definidos por Thakur satisfacen identidades interesantes pero combinatoriamente complejas. Thakur [Tha10] prueba la existencia de relaciones barajeadas entre los valores multizeta en el contexto de los campos de funciones para un anillo de enteros general A cuyo lugar al infinito es de grado uno. En particular, prueba que el producto de valores multizeta se puede expresar como una suma de valores multizeta, de tal manera que el $\mathbb{F}_p$-espacio generado por todos los valores multizeta es una álgebra. En el caso de los campos de funciones, las identidades son mucho más complicadas que las identidades barajeadas del caso clásico. De hecho, hay dos tipos de identidades, una con coeficientes en $\mathbb{F}_p(t)$ y otra con coeficientes en $\mathbb{F}_p$.

Como en el caso clásico, los valores multizeta tienen conexiones con el grupo absoluto de Galois vía los análogos a las series de potencias de Ihara (trabajo en progreso de G.

Anderson y D. Thakur) y también con los períodos de los t-motivos mixtos de Carlitz-Tate-Anderson [And86, AT09].

En su definición, la función zeta de Riemann $\zeta_{\mathbb{Z}}(s) = \sum_{a\in\mathbb{Z}_+} a^{-s}$, ($\mathrm{Re}(s) > 1$), sólo considera a los elementos del anillo de enteros de signo positivo. De manera similar, la función zeta de Carlitz $\zeta_{\mathbb{F}_q[t]}(s) = \sum_{a\in\mathbb{F}_q[t]+} a^{-s}$, ($s \in \mathbb{Z}_+$), solamente considera a los elementos "positivos", es decir, a los polinomios mónicos. Cuando el grado d_∞ del lugar al infinito es mayor que uno, es necesario modificar el concepto de elemento mónico y por lo tanto ajustar la definición de la función multizeta. Una forma de hacer esto es como en el caso de la zeta tal y como se explica en [Tha04, p. 156]. Aquí usaremos dos aproximaciones para definir la función multizeta. Con cualquiera de estas aproximaciones, la evidencia numérica apunta a que, en general, el producto de dos valores zeta no se puede expresar como una $\mathbb{F}_p$-combinación lineal de valores multizeta. Por lo tanto, el $\mathbb{F}_p$-espacio lineal generado por los valores multizeta no es una álgebra. También exploraremos qué relaciones se preservan del caso de grado uno.

3.2. Notación

K	un campo de funciones es una variable con campo de constantes $\mathbb{F}_q$
∞	un lugar de K de cualquier grado
d_∞	el grado de ∞
K_∞	la completación de K con respecto a ∞
A	el anillo de los elementos de K que no tienen polos excepto posiblemente en ∞
A_+	elementos mónicos en A, con respecto a una función signo fija
A_d	elementos de A de grado d
$A_{<d}$	elementos de A de grado menor que d
A_{d+}	$A_d \cap A_+$
$A_{<d+}$	$A_{<d} \cap A_+$

3.3. Antecedentes

Sea $\mathbb{F}_q$ un campo de q elementos, donde q es una potencia de un número primo p. Sea K un campo de funciones de una variable con campo de constantes $\mathbb{F}_q$. Sea ∞ un lugar de K de grado d_∞ y sea A el anillo de enteros de K, esto es, el anillo de los elementos de K que no tienen polos excepto posiblemente en ∞. Luego, su campo residual respecto a ∞ es $\mathbb{F}_\infty = \mathbb{F}_{q^{d_\infty}}$ y su completación K_∞ con respecto a ∞ es isomorfo al campo de las series de Laurent $\mathbb{F}_\infty((u))$, donde u es cualquier uniformizador en ∞, i.e., es un generador del ideal maximal del anillo de valuación en ∞. Así, podemos considerar $K_\infty := \mathbb{F}_{q^{d_\infty}}((u))$ como la completación de K en ∞. Cada elemento distinto de cero $x \in K_\infty$ se puede expresar como una serie de Laurent:

$$x = \sum_{j\geq\nu} a_j u^j$$

donde cada $a_j \in \mathbb{F}$, $a_\nu \neq 0$ y $v_\infty(x) = \nu$, donde v_∞ es la valuación con respecto al divisor primo que estamos tomando como primo al infinito. El grado de x se define por $\deg x = -d_\infty v_\infty(x)$, de tal manera que para a en A, $\deg a$ es precisamente el grado del divisor de ceros de a, i.e., $\deg a = \dim_{\mathbb{F}_q}(A/aA) = \log_q \#(A/aA)$. Observe que el grado siempre es un múltiplo de d_∞. Sea $\operatorname{sgn}(x) = a_\nu$, el coeficiente principal en la expansión de x. Entonces sgn es un homomorfismo de K_∞^* a $\mathbb{F}_\infty^*$ que es trivial en las 1-unidades de K_∞. Es claro que el mapeo sgn depende de la elección del uniformizador u. El número de funciones signo es $|\mathbb{F}_\infty^*| = q^{d_\infty} - 1$.

Fijaremos una función signo $\operatorname{sgn}\colon K_\infty^* \to \mathbb{F}_\infty^*$ que es trivial en las 1-unidades de K_∞ y tal que $\operatorname{sgn}(u) = 1$.

Cuando $d_\infty = 1$, los elementos cuyo signo es 1 son llamados *mónicos* o *positivos*. Cuando el grado d_∞ del lugar al infinito es mayor que uno, para definir el concepto de elemento mónico (y por lo tanto definir la función multizeta), para nuestros propósitos podemos seguir dos aproximaciones. (A1) Podemos fijar un elemento $\theta \in \mathbb{F}_\infty^*$, poner $S = \{\theta\}$, y definir como elemento mónico a aquel elemento cuyo signo es precisamente θ, o (A2) podemos tomar como S a un conjunto fijo de representantes de $\mathbb{F}_\infty^*/\mathbb{F}_q^*$ y definir a un elemento mónico como aquel elemento cuyo signo es un elemento de S. Ambas aproximaciones generalizan de manera natural el caso $d_\infty = 1$.

Sea S un subconjunto de $\mathbb{F}_\infty^*$ elegido en cualquiera de las dos formas explicadas anteriormente. Sea A_+ el conjunto de los elementos mónicos, esto es,

$$A_+ := \{a \in A : \operatorname{sgn}(a) \in S\}.$$

Definamos en primer lugar a las sumas de potencias. Para $s \in \mathbb{Z}$ y $d \in \mathbb{Z}_{\geq 0}$, sea

$$S_d(s) := \sum_{a \in A_{d+}} \frac{1}{a^s} \in K,$$

donde $A_{d+} = \{a \in A_+ \colon \deg(a) = d\}$. Entonces, la función zeta está dada por:

$$\zeta(s) = \sum_{d=0}^{\infty} S_d(s) \in K_\infty.$$

Dados enteros $s_i \in \mathbb{Z}_+$ y $d \geq 0$, pongamos

$$S_d(s_1, \ldots, s_r) = S_d(s_1) \sum_{d > d_2 > \cdots > d_r \geq 0} S_{d_2}(s_2) \cdots S_{d_r}(s_r) \in K.$$

En particular, con la extensión obvia de notación, tenemos

$$S_d(s_1, s_2) = S_d(s_1) \sum_{d > d_2 \geq 0} S_{d_2}(s_2) = S_d(s_1) S_{<d}(s_2).$$

Usando el orden parcial en A_+ determinado por el grado y agrupando los términos de acuerdo con este orden, para $s_i \in \mathbb{Z}_+$, se define el valor multizeta $\zeta(s_1, \ldots, s_r)$

$$\zeta(s_1, \ldots, s_r) := \sum_{d_1 > \cdots > d_r \geq 0} S_{d_1}(s_1) \cdots S_{d_r}(s_r) = \sum \frac{1}{a_1^{s_1} \cdots a_r^{s_r}} \in K_\infty,$$

donde la segunda suma se toma sobre todos los elementos $a_i \in A_+$ de grado d_i tales que $d_1 > \cdots > d_r \geq 0$. Decimos que este valor multizeta o más propiamente que la r-ada $(s_1, \ldots, s_r)$ tiene profundidad r y peso $\sum s_i$.

Para $a, b \in \mathbb{Z}_+$, definamos

$$\Delta_d(a, b) = S_d(a)S_d(b) - S_d(a + b).$$

Escribiremos $\Delta(a, b)$ en vez de $\Delta_{d_\infty}(a, b)$.

Observaciones 3.3.1.

(1) La definición implica inmediatamente que $\Delta_d(a, b) = \Delta_d(b, a)$. Por lo tanto, sin pérdida de generalidad y cuando sea necesario, podemos suponer que $a \leq b$ o $a \geq b$.

(2) Dado que estamos en característica p:

$$S_d(sp^n) = S_d(s)^{p^n}, \quad S_d(s_1p^n, s_2p^n) = S_d(s_1, s_2)^{p^n}.$$

Por tanto, a menudo sin pérdida de generalidad, nos podemos restringir a s's que no sean divisibles por p.

(3) Cuando el lugar al infinito de $K = \mathbb{F}_q(t)$ es el usual, el uniformizador es $1/t$ y consideramos la definición usual de mónico, entonces el anillo de enteros A es $\mathbb{F}_q[t]$ y la función zeta coincide con la función zeta de Carlitz.

3.4. Relaciones entre los valores multizeta en lugares no racionales

En esta sección exploraremos las relaciones entre los valores multizeta cuando el grado del lugar al infinito es mayor que uno, usando las convenciones para el signo A1 o A2 explicadas en la sección anterior.

Primero, consideremos la relación

$$\Delta_d(a, b) = \sum f_i S_d(a_i, a + b - a_i) \tag{3.4.0.1}$$

donde $f_i \in \mathbb{F}_p$.

Recordemos brevemente cual es la situación cuando el lugar es racional, esto es, cuando el grado del lugar al infinito es uno. Sea q una potencia de p. De acuerdo con el Teorema 1.4.1, sabemos que para $\mathbb{F}_q[t]$, dados $a, b \in \mathbb{Z}_+$, siempre existen $f_i \in \mathbb{F}_p$ y $a_i \in \mathbb{Z}_+$ tal que la Relación (3.4.0.1) es válida para $d = 1$. Del Teorema 1.4.2 sabemos que si la Relación 3.4.0.1 es válida para algunos $f_i \in \mathbb{F}_p$ y algunos $a_i \in \mathbb{Z}_+$ cuando $d = 1$ y A es $\mathbb{F}_q[t]$, entonces la relación sigue siendo válida, con los mismos a_i's y los mismos f_i's para toda $d \geq 0$ y para toda A correspondiente a la q dada.

La generalización directa del Teorema 1.4.1 no es válida para lugares de grado mayor que uno como se muestra en los Ejemplos 3.4.1, 3.4.2 y 3.4.3 a continuación. La evidencia numérica sugiere que independientemente de cuál convención para los signos usemos, existen a, b tales que $\zeta(a)\zeta(b)$ no se puede escribir como una $\mathbb{F}_q$-combinación lineal de valores multizeta (todos los cálculos en los ejemplos se hicieron usando software matemático de código abierto Sage [S$^+$11]).

Ejemplo 3.4.1 (S es un conjunto unitario)**.** Sea $K = \mathbb{F}_2(t)$. Sean $a = 1$ y $b = 2$. Para $\mathbb{F}_2[t]$, tenemos que $\Delta_d(a,b) = S_d(b,a)$ para toda $d \geq 0$. Ahora, sea ∞ el único lugar de K de grado dos. La completación respecto de ∞ es $\mathbb{F}_\infty((u))$, donde $\mathbb{F}_\infty = \{0, 1, i, i+1\}$ e $i^2 + i + 1 = 0$.

1) Consideremos el subconjunto $S = \{i\}$ de $\mathbb{F}_\infty^*$. Se tiene que $\Delta_2(a,b) \neq 0$ y $S_2(a,b) = S_2(b,a) = 0$. Por lo tanto, no es posible expresar $\Delta_d(a,b)$ como una $\mathbb{F}_2$-combinación lineal de $S_d(a_i, b_i)$'s, con peso $a_i + b_i = 3$, donde $d = d_\infty = 2$.

2) Si ahora tomamos $S = \{1\}$, entonces $\Delta_2(a,b) = S_2(b,a)$ pero $\Delta_d(a,b) \neq S_d(b,a)$ para $d = 2d_\infty, 3d_\infty, 4d_\infty$. Así, $\Delta_{d_\infty}(a,b) = S_{d_\infty}(b,a)$ no implica $\Delta_d(a,b) = S_d(b,a)$ para toda $d \geq 0$.

Una situación similar ocurre cuando mónico significa un elemento cuyo signo pertenece a un conjunto de representantes de $\mathbb{F}_\infty^*/\mathbb{F}_q^*$.

Ejemplo 3.4.2 (S es un conjunto de representantes de $\mathbb{F}_\infty^*/\mathbb{F}_q^*$)**.** Sea $K = \mathbb{F}_2(t)$ y sea $P_\infty = t^2 + t + 1$. Entonces $\mathbb{F}_\infty = \mathbb{F}_2(i)$ donde $i^2 + i + 1 = 0$. Entonces $S = \{1, i, i+1\}$. Sea $\mathcal{B}$ el conjunto de los pares $(1,2)$, $(1,3)$, $(1,4)$, $(1,5)$, $(1,6)$, $(1,7)$, $(1,8)$, $(2,5)$, $(2,7)$, $(3,4)$, $(3,5)$, $(3,6)$, $(3,7)$, $(3,8)$, $(4,5)$, $(5,6)$, $(5,7)$, $(5,8)$. Para cada par $(a,b) \in \mathcal{B}$, es posible escribir $\Delta(a,b)$ como una combinación lineal de $S_{d_\infty}(a_i, b_i)$'s, pero la correspondiente combinación lineal no es válida para $d = 2d_\infty = 4$.

1) Sea $(a,b) = (1,2)$. Un cálculo directo muestra que $\Delta(a,b) = 0$. Ninguna de las $\mathbb{F}_2$-combinaciones lineales de $S_d(1,2)$ y $S_d(2,1)$ coincide con $\Delta_d(a,b)$, cuando $d = 2d_\infty, 3d_\infty, 4d_\infty$. Observe que para $\mathbb{F}_2[t]$, la relación $\Delta_d(a,b) = S_d(2,1)$ es válida para toda $d \geq 0$.

2) Sea ahora $(a,b) = (1,3)$. Entonces, $\Delta(1,3) = 0$, pero no existen $f_1, f_2, f_3 \in \mathbb{F}_2$ tales que $\Delta_d(1,3) = f_1 S_d(1,3) + f_2 S_d(2,2) + f_3 S_d(3,1)$ cuando $d = 4, 6, 8$. Por otro lado, para $\mathbb{F}_2[t]$, la relación $\Delta_d(a,b) = S_d(2,2) + S_d(3,1)$ es válida para toda $d \geq 0$.

3) La igualdad $\Delta_d(1,4) = S_d(2,3) + S_d(3,2)$, es válida para $d = d_\infty$, pero no para $d = 2d_\infty, 3d_\infty, 4d_\infty$. Más aún, cuando $d = 2d_\infty$, no existen $f_1, f_2, f_3, f_4 \in \mathbb{F}_2$ que satisfagan la relación $\Delta_d(1,4) = f_1 S_d(1,4) + f_2 S_d(2,3) + f_3 S_d(3,2) + f_4 S_d(4,1)$.

Ejemplo 3.4.3 (S es un conjunto de representantes de $\mathbb{F}_\infty^*/\mathbb{F}_q^*$)**.** Sean $q = 3$, $P_\infty = t^2 + 1$ y $S = \{1, 2i, i+1, i+2\}$. No es posible escribir $\Delta_d(a,b)$ como una combinación lineal de $S_d(1, a+b-1), \ldots, S_d(a+b-1, 1)$ para $d = d_\infty = 2$ cuando (a,b) es alguno de los siguientes: $(1,1)$, $(1,2)$, $(1,3)$, $(1,4)$, $(1,5)$, $(1,6)$, $(1,7)$, $(1,8)$, $(2,3)$, $(2,5)$, $(3,4)$, $(3,5)$, $(4,4)$. Si $(a,b) = (1,3)$, ninguna combinación lineal de $S_d(1,3), S_d(2,2), S_d(3,1)$ coincide con $\Delta_d(a,b)$, $d = \nu d_\infty = 2, 4, 6$.

3.4.1. Aproximación 1

En esta subsección exploraremos las relaciones entre los valores multizeta cuando el grado del lugar al infinito es mayor que uno y S es un subconjunto unitario de $\mathbb{F}_\infty^*$. Con esta aproximación, parece ser que la única relación que sobrevive del caso racional es la relación clásica $\zeta(a)\zeta(b) = \zeta(a+b) + \zeta(a,b) + \zeta(b,a)$.

Consideremos la relación

$$\Delta_d(a,b) = S_d(a)S_d(b) - S_d(a+b) = 0. \tag{3.4.3.1}$$

El Teorema 3.4.4 a continuación y el Teorema 3.4.12 en la siguiente subsección, fueron conjeturados por el autor y la pruebas fueron sugeridas posteriormente por D. Thakur.

Teorema 3.4.4. *Sea q general. Si $a, b \in \mathbb{Z}_+$ son tales que la Relación* (3.4.3.1) *es válida para $\mathbb{F}_q[t]$ cuando $d = 1$, entonces, la Relación* (3.4.3.1) *es válida para toda $d \geq 0$ para cualquier A con ∞ de cualquier grado. En este caso se tiene la relación clásica*

$$\zeta(a)\zeta(b) = \zeta(a+b) + \zeta(a,b) + \zeta(b,a). \tag{3.4.4.1}$$

Demostración. La prueba fue sugerida por Thakur [Tha12] y se sigue de la primera parte de la prueba del Teorema 2 en [Tha10].

Note que si d_∞ no divide a d, entonces A_{d+} es vacío (pero $A_{<d+}$ podría no serlo) y así $\Delta_d(a,b) = 0$. Note que e s posib le que A_{d+} sea no vacío pero $A_{<d+} = \emptyset$.

Sea A arbitraria. Considere $n, n' \in A_{d+}$, $m, m' \in A_{<d+}$. Defina

$$S_{n,m} := \{(n+\theta m, n+\mu m) \colon \theta, \mu \in \mathbb{F}_q, \theta \neq \mu\},$$
$$n \sim_m n' \leftrightarrow n' = n + \theta m, \text{ para algún } \theta \in \mathbb{F}_q.$$

Entonces, los conjuntos $S_{n,m}$ y $S_{n',m'}$, los cuales son iguales o disjuntos, son las clases de equivalencia de $\sim$ y particionan al conjunto $\{(n_1, n_2) \colon n_i \in A_{d+}, n_1 \neq n_2\}$. Sea $d > 0$ divisible por d_∞. Haciendo $t = n/m$, tenemos

$$\begin{aligned}
\sum_{(n_1,n_2)\in S_{n,m}} \frac{1}{n_1^a n_2^b} &= \sum_{\theta\neq\mu\in\mathbb{F}_q} \frac{1}{(n+\theta m)^a (n+\mu m)^b} \\
&= \frac{1}{m^{a+b}} \sum_{\theta\neq\mu\in\mathbb{F}_q} \frac{1}{(t+\theta)^a (t+\mu)^b} \\
&= \frac{1}{m^{a+b}}(0) \\
&= 0.
\end{aligned}$$

La tercera igualdad se sigue de (3.4.3.1). Sumando sobre la partición llegamos a que $\Delta_d(a,b) = 0$. Dado que también se tiene $\Delta_d(a,b) = 0$ para $d = 0$, el teorema queda probado. □

Observaciones 3.4.5.

(1) Excepto por la relación (3.4.4.1), la evidencia numérica que hemos calculado con valores pequeños de los parámetros sugiere que no hay otra relación del tipo "el producto de dos valores zeta es igual a una combinación lineal de multizetas con coeficientes en $\mathbb{F}_p$" que sobreviva para lugares al infinito de grados superiores.

(2) En [Tha09b, Teorema 1, p. 2324] Thakur provee una lista no exhaustiva de condiciones en $a, b \in \mathbb{Z}_+$ tales que $\Delta(a, b) = 0$. Sería interesante tener una caracterización de tales a, b. Note que de acuerdo con [Tha09b, 2.1] si $p = 2$ y $a = b$, entonces $\zeta(a)\zeta(b) = \zeta(a + b) = \zeta(a + b) + \zeta(a, b) + \zeta(b, a)$. Del Teorema 8 en [Tha09a] sabemos que para $\mathbb{F}_2[t]$, $\Delta_d(a, b) = 0$ si y solamente si $a = b$. Pero observe que si $a = 2$ y $b = 3$, entonces para toda $d \geq 0$ se tiene $\Delta_d(a, b) = -S_d(a, b) - S_d(b, a)$ y por lo tanto, $\zeta(a)\zeta(b) = \zeta(a + b) + \zeta(a, b) + \zeta(b, a) - \zeta(a, b) - \zeta(b, a) = \zeta(a + b)$, con $a \neq b$ y $q = 2$.

Ahora trataremos de caracterizar los pares (a, b) tales que la suma barajeada clásica sea válida. El caso $q = 2$ y algunos resultados generales parciales se mencionaron anteriormente.

Teorema 3.4.6. *Sea q general. Considere los siguientes casos:*

(1) $a = a_n q^n$ *y* $b = b_n q^n - 1$, *con* $1 \leq a_n \leq q - 2$, $2 \leq b_n \leq q - 1$ *y* $a_n + b_n \leq q$,

(2) $a = q^n - (q - 1)$ *y* $b = q^n - 1$,

Si $a, b \in \mathbb{Z}_+$ satisfacen (1) o (2), entonces para $A = \mathbb{F}_q[t]$ se tiene la suma barajeada clásica

$$\zeta(a)\zeta(b) = \zeta(a + b) + \zeta(a, b) + \zeta(b, a).$$

Demostración. De acuerdo con el Teorema 1.4.2, en cada caso es suficiente probar $\Delta(a, b) = 0$. Ahora,

$$\Delta(a, b) = \sum_{\substack{n_1 \neq n_2 \\ n_1, n_2 \in A_{1+}}} \frac{1}{n_1^a n_2^b} = \sum_{n_2 \in A_{1+}} \frac{1}{n_2^b} \left(S_1(a) - \frac{1}{n_2^a} \right). \tag{3.4.6.1}$$

Para cualquier $n_2 \in A_{1+}$ tenemos $[1] = n_2^q - n_2$.

(1) De (2.1.0.5) sabemos que $S_d(ap^s) = 1/\ell_d^{ap^s}$ siempre que $a \leq q$. Tomando $a = a_n q^n$ y $b = b_n q^n - 1$ en (3.4.6.1), se tiene

$$\begin{aligned}
\Delta(a_n q^n, b_n q^n - 1) &= \sum_{n_2 \in A_{1+}} \frac{1}{n_2^b} \left(\frac{1}{(-[1])^a} - \frac{1}{n_2^a} \right) \\
&= \frac{1}{\ell_1^a} \sum_{n_2 \in A_{1+}} \frac{1}{n_2^{a+b}} \left(n_2^{a_n} - (-1)^{a_n} (n_2^q - n_2)^{a_n} \right)^{q^n} \\
&= \frac{1}{\ell_1^a} \sum_{n_2 \in A_{1+}} \frac{1}{n_2^{a+b}} \left(\sum_{j=1}^{a_n} \binom{a_n}{j} (-1)^{2a_n - j + 1} n_2^{qj + a_n - j} \right)^{q^n} \\
&= \frac{1}{\ell_1^a} \sum_{n_2 \in A_{1+}} \frac{1}{n_2^{a+b}} \sum_{j=1}^{a_n} \binom{a_n}{j}^{q^n} (-1)^{j+1} n_2^{q^{n+1} j + a_n q^n - j q^n} \\
&= \frac{1}{\ell_1^a} \sum_{j=1}^{a_n} \binom{a_n}{j}^{q^n} (-1)^{j+1} \sum_{n_2 \in A_{1+}} n_2^{q^{n+1} j - j q^n - b_n q^n + 1} \\
&= \frac{1}{\ell_1^a} \sum_{j=1}^{a_n} \binom{a_n}{j}^{q^n} (-1)^{j+1} S_1(-N_j),
\end{aligned}$$

donde $N_j = jq^{n+1} - (b_n + j)q^n + 1 > 0$ ya que $b_n \leq j(q-1)$. Observe que la descomposición en base q de N_j es $N_j = 1 + (q - b_n - j)q^n + (j-1)q^{n+1}$. Puesto que $q - b_n < q - 1$, se sigue que $\ell(N_j)/(q-1) = (q-b_n)/(q-1) < 1$, donde $\ell(N_j)$ denota la suma de los dígitos de N_j en base q. Por lo tanto, y de acuerdo con [Tha04, Teorema 5.1.2], se tiene que $S_1(-N_j) = 0$.

(2) De la identidad (2.1.0.9) se sigue que $S_1(q^n - 1) = [n]/[1]^{q^n}$. Ahora, tomando $a = q^n - 1$ y $b = q^n - q + 1$ en (3.4.6.1), obtenemos

$$\begin{aligned}
\Delta(a,b) &= \sum_{n_2 \in A_{1+}} \frac{1}{n_2^{q^n-q+1}} \left(\frac{[n]}{[1]^{q^n}} - \frac{1}{n_2^{q^n-1}} \right) \\
&= \sum_{n_2 \in A_{1+}} \frac{1}{n_2^{q^n-q+1}} \frac{1}{[1]^{q^n} n_2^{q^n-1}} \left(n_2^{q^n-1}(n_2^{q^n} - n_2) - (n_2^{q^{n+1}} - n_2^{q^n}) \right) \\
&= \frac{1}{[1]^{q^n}} \sum_{n_2 \in A_{1+}} \frac{1}{n_2^{2q^n-q}} \left(n_2^{2q^n-1} - n_2^{q^{n+1}} \right) \\
&= \frac{1}{[1]^{q^n}} \sum_{n_2 \in A_{1+}} \left(n_2^{q-1} - n_2^{q^{n+1}-2q^n+q} \right) \\
&= \frac{1}{[1]^{q^n}} \left(S_1(-(q-1)) - S_1(-qN) \right)
\end{aligned}$$

donde $N = q^n - 2q^{n-1} + 1$. Por el Teorema 2.6.1 se tiene $S_1(-(q-1)) = -1$. Por otro lado, de la segunda prueba del Teorema 2.7.2 se sigue que $S_1(-N) = -1$. Luego $S_1(-qN) = -1$. Por lo tanto, $\Delta(a,b) = 0$ como se quería. $\square$

Observación 3.4.7. La evidencia numérica que hemos calculado sugiere que cuando $q = 3$, el Teorema 3.4.6 y el hecho de que (3.4.4.1) también se cumple cuando $a + b \leq q$ caracteriza completamente las $a, b \in \mathbb{Z}_+$ (suponemos sin pérdida de generalidad que $a \leq b$ y que a, b no son simultáneamente divisibles por p) tales que la Relación (3.4.4.1) se cumple.

Conjetura 3.4.8. *Sea q general. Sea $n \geq 0$. Considere los siguientes casos*

(1) $a = a_{s_a+1}q^{s_a+1} + \cdots + a_n q^n,\ b = b_{s_b+1}q^{s_b+1} + \cdots + b_n q^n$,
con $-1 \leq s_a, s_b \leq n-1$, $1 \leq a_i, b_j \leq q-1$, *y*

$$\begin{aligned}
q + j(q-1) &\leq a_n + a_{n-1} + \cdots + a_{n-j-1}, &\qquad (0 \leq j \leq n - s_a - 2),\\
q + j(q-1) &\leq b_n + b_{n-1} + \cdots + b_{n-j-1}, &\qquad (0 \leq j \leq n - s_b - 2),
\end{aligned}$$

y

$$a_n + b_n \leq \begin{cases} q & \text{si } s_a = s_b = n-1, \\ q-1 & \text{si } s_a < n-1, s_b = n-1, \\ q-1 & \text{si } s_a = n-1, s_b < n-1, \\ q-2 & \text{si } s_a, s_b < n-1. \end{cases}$$

(2) *$n \geq 1$, $1 \leq a_0, b_0 \leq q-1$, $a_0 + b_0 = q$ y*

$$a = a_0 + q^n - q, \quad b = b_0 + q^n - q.$$

Si $a, b \in \mathbb{Z}_+$ satisfacen (1) o (2), entonces

$$\zeta(a)\zeta(b) = \zeta(a+b) + \zeta(a,b) + \zeta(b,a)$$

se cumple para $\mathbb{F}_q[t]$.

Observaciones 3.4.9.

(1) Del Teorema 1 [Tha09b, p. 2324], se sigue que si $a = a_n q^n$ y $b = b_n q^n$, entonces la suma barajeada clásica se cumple siempre que $a_n + b_n \leq q$. Por lo tanto, la parte de la Conjetura 3.4.8 correspondiente a $s_a = s_b = n-1$ ya está probada.

(2) La Conjetura 3.4.8 es más general que el Teorema 3.4.6. De hecho, si en (1) de la conjetura anterior tomamos $a = a_n q^n$ y $b = (q-1) + (q-1)q + \cdots + (q-1)q^{n-1} + (b_n - 1)q^n$ (así $s_a + 1 = n$ y $s_b + 1 < n$) con $1 \leq a_n \leq q-2$ y $1 \leq b_n - 1 \leq q-1$, obtenemos el Teorema 3.4.6 (1). Análogamente, si tomamos $a_0 = 1$ y $b_0 = q-1$ en (2) de la conjetura anterior, obtenemos el Teorema 3.4.6 (2).

(3) La evidencia numérica que hemos calculado sugiere que cuando q es 3 o 5, el recíproco de la Conjetura 3.4.8 también es válido (de nuevo, suponemos que $a \leq b$ y que a y b no son simultáneamente divisibles por p).

Conjetura 3.4.10. *Sea q general, $d \geq 0$ y $n \geq 1$. Entonces*

$$S_d(a_0 + q^n - q) = \frac{\ell_{d+n-1}^{q-a_0}}{\ell_d^{q^n} \ell_{n-1}^{q-a_0}} \quad (1 \leq a_0 \leq q). \tag{3.4.10.1}$$

Observaciones 3.4.11.

(1) De la Proposición 2.7.1 sabemos que $S_1(2q^{n-1} - 1) = -[n]/[1]^{2q^{n-1}}$. Sustituyendo $d = 1$ en (3.4.10.1) obtenemos

$$S_1(a_0 + q^n - q) = (-1)^{a_0} \frac{[n]^{q-a_0}}{[1]^{q^n}} \quad (1 \leq a_0 \leq q).$$

Sean a, b como en la Conjetura 3.4.8 (2). Luego $a_0 + b_0 = q$ y $a + b = 2q^n - q$. Entonces,

$$S_1(a)S_1(b) = (-1)^{a_0+b_0} \frac{[n]^{q-a_0+q-b_0}}{[1]^{2q^n}} = -\frac{[n]^q}{[1]^{2q^n}} = S_1(a+b).$$

Por lo tanto, la Fórmula (3.4.10.1) implica la parte 2 de la Conjetura 3.4.8.

(2) Podemos deducir la Fórmula (3.4.10.1) para $n = 1$ o $a_0 = q$ de [Tha09b, 3.3] y para $a_0 = q-1$ de (2.1.0.9).

3.4.2. Aproximación 2

En la subsección anterior, consideramos como mónicos a los elementos cuyo signo era igual a un elemento fijo, pero arbitrario, de $\mathbb{F}_\infty^*$, es decir, la aproximación A1. En esta subsección usaremos la aproximación A2. Sea S un conjunto fijo de representantes de $\mathbb{F}_\infty^*/\mathbb{F}_q^*$. Ahora exploraremos si $\zeta(a)\zeta(b)$ se puede escribir como una suma de valores multizeta. De nuestros cálculos, parece que usando esta aproximación para los signos la única relación que sobrevive del caso racional es $\zeta(a)\zeta(b) = \zeta(a+b)$.

Considere la relación

$$\Delta_d(a,b) = -S_d(a,b) - S_d(b,a). \tag{3.4.11.1}$$

Teorema 3.4.12. *Sea q general. Si $a, b \in \mathbb{Z}_+$ son tales que la Relación* (3.4.11.1) *es válida para $\mathbb{F}_q[t]$ y $d = 1$, entonces, la Relación* (3.4.11.1) *es válida para toda $d \geq 0$ y para cualquier A con ∞ de cualquier grado. En este caso, tenemos la identidad*

$$\zeta(a)\zeta(b) = \zeta(a+b). \tag{3.4.12.1}$$

Bosquejo de la prueba. Sea A arbitraria. Sean $n, n' \in A_{d+}$ y $m, m' \in A_{<d+}$ tales que $\operatorname{sgn}(n) = \operatorname{sgn}(n')$ y $\operatorname{sgn}(m) = \operatorname{sgn}(m')$. Definamos

$$\begin{aligned} S_{n,m} &:= \{(n+\theta m, n+\mu m) \colon \theta, \mu \in \mathbb{F}_q, \theta \neq \mu\} \\ S'_{n,m} &:= \{(n+\theta m, m) \colon \theta \in \mathbb{F}_q\}, \\ n \sim_m n' &\leftrightarrow n' = n + \theta m, \text{ para algún } \theta \in \mathbb{F}_q. \end{aligned}$$

Ya que $\deg m < d$ y $\deg n = d$, se tiene que $\operatorname{sgn}(n+\theta m) = \operatorname{sgn}(n)$. Se sigue que los conjuntos $S_{n,m}$ y $S_{n',m'}$, los cuales son iguales o disjuntos, son las clases de equivalencia de $\sim_m$ y particionan al conjunto $\{(n_1, n_2) \colon n_i \in A_{d+}, n_1 \neq n_2, \operatorname{sgn}(n_1) = \operatorname{sgn}(n_2)\}$. Por otro lado, los conjuntos $S'_{n,m}$ particionan al conjunto $\{(n_1, m_1) \colon n_1 \in A_{d+}, m_1 \in A_{<d+}\}$.

Para cualquier $d \geq 0$ se tiene que $\Delta_d(a,b) = \mathcal{S}_1 + \mathcal{S}_2$, donde

$$\mathcal{S}_1 = \sum_{\substack{n_1 \neq n_2, n_i \in A_{d+} \\ \operatorname{sgn}(n_1) \neq \operatorname{sgn}(n_2)}} \frac{1}{n_1^a n_2^b}, \qquad \mathcal{S}_2 = \sum_{\substack{n_1 \neq n_2, n_i \in A_{d+} \\ \operatorname{sgn}(n_1) = \operatorname{sgn}(n_2)}} \frac{1}{n_1^a n_2^b}.$$

Se puede probar que $\mathcal{S}_1 = 0$ [Tha12].

Sea $d > 0$ divisible por d_∞. Haciendo $t = n/m$, se tiene

$$\begin{aligned} \sum_{(n_1,n_2) \in S_{n,m}} \frac{1}{n_1^a n_2^b} &= \sum_{\theta \neq \mu \in \mathbb{F}_q} \frac{1}{(n+\theta m)^a (n+\mu m)^b} \\ &= \frac{1}{m^{a+b}} \sum_{\theta \neq \mu \in \mathbb{F}_q} \frac{1}{(t+\theta)^a (t+\mu)^b} \\ &= \frac{1}{m^{a+b}} \left(-\sum_{\theta \in \mathbb{F}_q} \frac{1}{(t+\theta)^a} - \sum_{\theta \in \mathbb{F}_q} \frac{1}{(t+\theta)^b} \right) \\ &= -\sum_{\theta \in \mathbb{F}_q} \frac{1}{(n+\theta m)^a m^b} - \sum_{\theta \in \mathbb{F}_q} \frac{1}{(n+\theta m)^b m^a} \\ &= -\sum_{(x,y) \in S'_{n,m}} \frac{1}{x^a y^b} - \sum_{(x,y) \in S'_{n,m}} \frac{1}{x^b y^a}. \end{aligned}$$

La tercera igualdad se sigue de la hipótesis. Sumando sobre la partición obtenemos que $\mathcal{S}_2 = -S_d(a,b) - S_d(b,a)$. Dado que $\Delta_d(a,b) = 0$ y $S_d(a,b) = S_d(b,a) = 0$ para las d's que no dividen a d_∞, el teorema queda probado. □

Observaciones 3.4.13.

(1) La evidencia numérica calculada sugiere que aparte de la Relación (3.4.12.1) no existe otra relación con coeficientes en $\mathbb{F}_p$.

(2) Es deseable tener una caracterización de aquellos $a, b \in \mathbb{Z}_+$ tales que la Relación (3.4.11.1) se cumple. Una condición necesaria es que tanto a como b sean "pares" (Teorema 2.2.1 o Corolario 2.4.13).

(3) Ya que $S_1(k) = S_{<2}(k) - 1$, un cálculo directo muestra que

$$\Delta(a,b) = -S_1(a) - S_1(b) \Leftrightarrow S_{<2}(a+b) = S_{<2}(a)S_{<2}(b). \tag{3.4.13.1}$$

Teorema 3.4.14. *Sea $q = 2$. Sean $n \geq 0$ y $0 \leq \alpha \leq \beta$. Sean $a = 2^n(2^{\beta+1} - 2^\alpha) = 2^n(2^\alpha + \cdots + 2^\beta)$ y $b = 2^n(2^{\beta+1} - 1)$. Entonces,* (3.4.11.1) *es válida para $\mathbb{F}_2[t]$, y por lo tanto*

$$\zeta(a)\zeta(b) = \zeta(a+b).$$

Demostración. Es suficiente probar que

$$\Delta_1(a,b) = S_1(a,b) + S_1(b,a) = S_1(a) + S_1(b),$$

para $\mathbb{F}_2[t]$ cuando $a = 2^{\beta+1} - 2^\alpha$ y $b = 2^{\beta+1} - 1$. Aplicaremos el Teorema 2.4.17. Se tiene

$$\begin{aligned} a - 1 &= 2^\alpha - 1 + 2^{\alpha+1} + \cdots + 2^\beta \\ &= 1 + 2 + \cdots + 2^{\alpha-1} + 0 \cdot 2^\alpha + 2^{\alpha+1} + \cdots + 2^\beta. \end{aligned}$$

Dado que $2^{\beta+2} - b = 1 + 2^{\beta+1}$ y $2^{\beta+2} - a = 2^\alpha + 2^{\beta+1}$, del Teorema de Lucas concluimos que $\binom{2^{\beta+2}-b}{i}$ y $\binom{2^{\beta+2}-a}{j}$ son distintos de cero para $i = 0, 1$ y $j = 0, 2^\alpha$. Luego,

$$\Delta_1(a,b) = S_1(a) + S_1(a-1) + S_1(b) + S_1(b - 2^\alpha).$$

Ya que $a - 1 = b - 2^\alpha$, el teorema queda probado. □

Observación 3.4.15. La evidencia numérica sugiere que para el caso $\mathbb{F}_2[t]$, la relación (3.4.11.1) es válida si y solamente si a y b son de la forma dada en el Teorema 3.4.14.

Tenemos la siguiente generalización.

Teorema 3.4.16. *Sea q general. Sean $n \geq 0$ y $0 \leq \alpha \leq \beta$. Sean $a = p^n(q^{\beta+1} - q^\alpha) = p^n(q-1)(q^\alpha + \cdots + q^\beta)$ y $b = p^n(q^{\beta+1} - 1)$. Entonces, la Relación* (3.4.11.1) *es válida para $\mathbb{F}_q[t]$, y, por lo tanto,*

$$\zeta(a)\zeta(b) = \zeta(a+b).$$

La condición es suficiente pero no necesaria.

Demostración. De acuerdo con el Teorema 1.4.2, es suficiente probar que $\Delta(a,b) = -S_1(a) - S_1(b)$, donde $a = q^{\beta+1} - q^{\alpha}$ y $b = q^{\beta+1} - 1$. Del Teorema 2.4.19 se obtiene

$$\Delta(a,b) = \sum_{i=0}^{b-1} f_i S_1(b-i) + \sum_{j=0}^{b-1} g_j S_1(b-j), \tag{3.4.16.1}$$

donde $H_{a,b}(t) = (1/t^a)(P_a(t) \text{ mód } t^{a+b})$,

$$P_a(t) = -\frac{[1]^{p^m-a}}{t^{p^m-a}} \sum_{\theta\in\mathbb{F}_q^*} \frac{[1]^a}{(t+\theta)^a}, \tag{3.4.16.2}$$

y m es el entero más pequeño tal que $a+b \le p^m$.

Sea $q = p^s$ con $s \ge 1$. Tenemos $q^{\beta+1} < a+b \le 2q^{\beta+1} \le pq^{\beta+1}$, así que $m = \lceil \log_p(a+b) \rceil = s(\beta+1)+1$. De (2.1.0.9), se tiene

$$S_1(q^{\beta+1} - q^{\alpha}) = S_1(q^{\beta-\alpha+1} - 1)^{q^{\alpha}} = \frac{[\beta-\alpha+1]^{q^{\alpha}}}{[1]^{q^{\beta+1}}}.$$

Ahora,

$$\begin{aligned}
\sum_{\theta\in\mathbb{F}_q^*} \frac{[1]^a}{(t+\theta)^a} &= [1]^a \left(S_1(a) - \frac{1}{t^a} \right) \\
&= \frac{[1]^a}{t^a[1]^{q^{\beta+1}}} \left(t^a(t^{q^{\beta+1}} - t^{q^{\alpha}}) - (t^{q^{\beta+2}} - t^{q^{\beta+1}}) \right) \\
&= \frac{1}{t^a[1]^{q^{\alpha}}} \left(t^a t^{q^{\alpha}} (t^{q^{\beta+1}-q^{\alpha}} - 1) - t^a t^{q^{\alpha}} (t^{q^{\beta+2}-q^{\beta+1}} - 1) \right) \\
&= \frac{t^a - t^{(q-1)q^{\beta+1}}}{(t^{q-1}-1)^{q^{\alpha}}} \\
&= -t^a \frac{t^{(q-2)q^{\beta+1}+q^{\alpha}} - 1}{t^{(q-1)q^{\alpha}} - 1}.
\end{aligned}$$

Ya que $(q-1)q^{\beta+1}$ y $a = q^{\beta+1} - q^{\alpha}$ son ambos divisibles por $q-1$ y q^{α}, se sigue que $(q-1)q^{\alpha}$ divide $(q-2)q^{\beta+1} + q^{\alpha}$, y por tanto $\sum_{\theta\in\mathbb{F}_q^*}[1]^a/(t+\theta)^a$ es un polinomio cuyos coeficientes son todos iguales a -1. Como $(q-2)q^{\beta+1} + q^{\alpha} - (q-1)q^{\alpha} = (q-2)a$, tenemos

$$\sum_{\theta\in\mathbb{F}_q^*} \frac{[1]^a}{(t+\theta)^a} = -t^a(1 + t^{(q-1)q^{\alpha}} + \cdots + t^{(q-2)a}) = -(t^a + t^{a+(q-1)q^{\alpha}} \cdots + t^{(q-1)a}).$$

Por otro lado, la descomposición en base p de a es $(p-1)(p^{s\alpha} + p^{s\alpha+1} + \cdots + p^{s(\beta+1)-1})$. Puesto que $p^m - a = (p-1)q^{\beta+1} + q^{\alpha}$, se sigue que $\binom{p^m-a}{j} \ne 0$ para $j = j_{s\alpha}p^{s\alpha} + j_{s(\beta+1)}p^{s(\beta+1)}$, $0 \le j_{s\alpha} \le 1$ y $0 \le j_{s(\beta+1)} \le p-1$. Ya que $b < q^{\beta+1} \le (q-1)q^{\beta+1}$, se tiene

$$a + b \le a + (q-1)q^{\beta+1} \le a + l(q-1)q^{\alpha} + j(q-1), \quad 0 \le l,\ j \ne 0, q^{\alpha}.$$

Entonces,

$$\begin{aligned} P_a(t) \text{ mód } t^{a+b} &= -(t^a + \cdots + t^{(q-1)a}) - t^{(q-1)q^\alpha}(t^a + \cdots + t^{(q-1)a}) \quad \text{mód } t^{a+b} \\ &= (-t^a + t^{(q-1)q^{\beta+1}}) \text{ mód } t^{a+b}. \end{aligned}$$

Supongamos que $q > 2$. Así $P_a(t)$ mód $t^{a+b} = -t^a$. De manera semejante, $P_b(t) = -t^b$. Luego $H_{a,b}(t) = -1 = H_{b,a}(t)$, y $\Delta(a,b) = -S_1(b) - S_1(a)$.

Si $q = 2$, entonces $H_{a,b}(t) = -1 + t^{2^\alpha}$ y $H_{b,a}(t) = -1 + t$, así que $\Delta(a,b) = S_1(b) + S_1(b - 2^\alpha) + S_1(a) + S_1(a-1) = S_1(b) + S_1(a)$ porque $b - 2^\alpha = a - 1$.

La condición no es necesaria porque para $\mathbb{F}_3[t]$, $a = 2$ y $b = 4$, la Relación (3.4.11.1) se cumple para toda $d \geq 0$. □

Teorema 3.4.17. *Sean $\beta > 0$ y $1 \leq l_1, l_2 \leq q - 1$. Si $a = l_1(q^\beta - 1)$ y $b = l_2(q^\beta - 1)$, con $l_1 + l_2 \leq q$, entonces la Relación* (3.4.11.1) *se cumple para $\mathbb{F}_q[t]$, y por lo tanto*

$$\zeta(a)\zeta(b) = \zeta(a+b).$$

Demostración. De acuerdo con el Teorema 1.4.2, es suficiente probar que $\Delta(a,b) = -S_1(a) - S_1(b)$, o equivalentemente, que $S_{<2}(a+b) = S_{<2}(a)S_{<2}(b)$. Sustituyendo $d = 2$ en la siguiente fórmula

$$S_{<d}(l(q^\beta - 1)) = \frac{\ell_{d+\beta-1}^l}{\ell_{d-1}^{lq^\beta}\ell_\beta^l} \quad (1 \leq l \leq q),$$

obtenemos

$$S_{<2}(l(q^\beta - 1)) = \frac{[\beta+1]^l}{[1]^{lq^\beta}}. \tag{3.4.17.1}$$

Un cálculo directo muestra que $S_{<2}(a+b) = S_{<2}(a)S_{<2}(b)$. □

El siguiente teorema es una generalización de los Teoremas 3.4.14, 3.4.16 y 3.4.17.

Teorema 3.4.18. *Sea q general. Sean $a = l_1(q^{\beta+1} - q^{\alpha_1})$ y $b = l_2(q^{\beta+1} - q^{\alpha_2})$, donde $0 \leq \alpha_1, \alpha_2 \leq \beta$, $1 \leq l_1, l_2 \leq q-1$ y $l_1 + l_2 \leq q$. Entonces*

$$\zeta(a)\zeta(b) = \zeta(a+b)$$

es válida en $\mathbb{F}_q[t]$.

Demostración. De acuerdo con el Teorema 1.4.2, es suficiente probar que $\Delta(a,b) = -S_1(a) - S_1(b)$. Debido a la Proposición 2.4.14, en el Teorema 2.4.19, podemos usar cualquier m tal que $a + b \leq p^m$, en lugar de $m = \lceil \log_p(a+b) \rceil$. Aquí tomaremos $m = (\beta+2)\log_p q$. Entonces $a + b < p^m = q^{\beta+2}$. Dado que $(l_1 + l_2)q^{\beta+1} \leq q^{\beta+2}$ y $q^{\alpha_1} \leq l_1 q^{\alpha_1} < l_1 q^{\alpha_1} + l_2 q^{\alpha_2}$, se sigue que $a + b \leq q^{\beta+2} - q^{\alpha_1}$ y también $a + b < q^{\beta+2} \leq (q-1)q^{\beta+2}$.

Por otro lado,

$$\begin{aligned} -\left(t^{q-1}-1\right)^{p^m-l_1q^{\beta+1}} &= -\left(t^{(q-1)q^{\beta+1}}-1\right)^{q-l_1} \\ &= \sum_{j=0}^{q-l_1}\binom{q-l_1}{j}(-1)^{q-l_1-j+1}t^{j(q-1)q^{\beta+1}}. \end{aligned}$$

Ya que $l_1+l_2 \leq q \leq 2q-2$, tenemos $(l_1+l_2)q^{\beta+1} \leq 2(q-1)q^{\beta+1} < 2(q-1)q^{\beta+1} + l_1q^{\alpha_1}+l_2q^{\alpha_2}$. Así $a+b < j(q-1)q^{\beta+1}$ para $j \geq 2$.

De (3.4.17.1) tenemos

$$S_1(a) = \frac{[\beta-\alpha_1+2]^{l_1q^{\alpha_1}}}{[1]^{l_1q^{\beta+1}}} - 1.$$

De (3.4.16.2) se tiene

$$\begin{aligned} P_a(t) &= -\frac{[1]^{p^m-a}}{t^{p^m-a}}[1]^a\left(S_1(a)-\frac{1}{t^a}\right) \\ &= -\frac{[1]^{p^m}t^a}{t^{p^m}}\left(\frac{[\beta-\alpha_1+2]^{l_1q^{\alpha_1}}}{[1]^{l_1q^{\beta+1}}} - \frac{t^a+1}{t^a}\right) \\ &= -\frac{[1]^{p^m}}{t^{p^m}}\frac{t^{l_1q^{\beta+1}}}{t^{l_1q^{\alpha_1}}}\frac{[\beta-\alpha_1+2]^{l_1q^{\alpha_1}}}{[1]^{l_1q^{\beta+1}}} + \frac{[1]^{p^m}}{t^{p^m}}(t^a+1) \\ &= -\frac{[1]^{p^m}}{t^{p^m}}\frac{t^{l_1q^{\beta+1}}}{[1]^{l_1q^{\beta+1}}}\frac{[\beta-\alpha_1+2]^{l_1q^{\alpha_1}}}{t^{l_1q^{\alpha_1}}} + \frac{[1]^{p^m}}{t^{p^m}}(t^a+1) \\ &= -\left(t^{q-1}-1\right)^{p^m-l_1q^{\beta+1}}\left(t^{q^{\beta-\alpha_1+2}-1}-1\right)^{l_1q^{\alpha_1}} + (t^{(q-1)p^m}-1)(t^a+1). \end{aligned}$$

Por lo tanto,

$$\begin{aligned} P_a(t) \text{ mód } t^{a+b} &= \left(((-1)^{l_1}+(-1)^{l_1}l_1t^{(q-1)q^{\beta+1}})(-1)^{l_1} - t^a - 1\right) \text{ mód } t^{a+b} \\ &= (-t^a + l_1t^{(q-1)q^{\beta+1}}) \text{ mód } t^{a+b} \end{aligned}$$

Análogamente,

$$P_b(t) \text{ mód } t^{a+b} = (-t^b + l_2t^{(q-1)q^{\beta+1}}) \text{ mód } t^{a+b}.$$

Supongamos que $(q-1)q^{\beta+1} \leq a+b$. Entonces $(q-1-l_1-l_2)q^{\beta+1} \leq -l_1q^{\alpha_1}-l_2q^{\alpha_2} < 0$ y así $q-1 < l_1+l_2$. Ya que $l_1+l_2 \leq q$, se sigue que $l_1+l_2 = q$. Recíprocamente, si $l_1+l_2 = q$, entonces $l_1q^{\alpha_1}+l_2q^{\alpha_2} \leq l_1q^{\beta}+l_2q^{\beta} = q^{\beta+1}$. Por lo tanto $q^{\beta+2}-q^{\beta+1} \leq q^{\beta+2}-l_1q^{\alpha_1}-l_2q^{\alpha_2} = a+b$. Luego, $(q-1)q^{\beta+1} \leq a+b$ si y sólo si $l_1+l_2 = q$.

Si $a+b \geq (q-1)q^{\beta+1}$, entonces $H_{a,b}(t) = -1+l_1t^{(q-1)q^{\beta+1}-a}$, $H_{b,a}(t) = -1+l_2t^{(q-1)q^{\beta+1}-b}$. Así, por (3.4.16.1)

$$\begin{aligned} \Delta(a,b) &= -S_1(b) + l_1S_1(b-(q-1)q^{\beta+1}+a) - S_1(a) + l_2S_1(a-(q-1)q^{\beta+1}+b) \\ &= -S_1(a) - S_1(b), \end{aligned}$$

porque $l_1+l_2 = q$. Si $a+b < (q-1)q^{\beta+1}$, entonces $P_a(t)$ mód $t^{a+b} = -t^a$ y $P_b(t)$ mód $t^{a+b} = -t^b$. Luego $H_{a,b}(t) = -1$ y $H_{b,a}(t) = -1$ y por lo tanto, $\Delta(a,b) = -S_1(a) - S_1(b)$. $\square$

Corolario 3.4.19. *Sea q general. Entonces,*

$$S_{<2}(l_1(q^{\beta+1}-q^{\alpha_1})+l_2(q^{\beta+1}-q^{\alpha_2}))=\frac{[\beta-\alpha_1+2]^{l_1q^{\alpha_1}}[\beta-\alpha_2+2]^{l_2q^{\alpha_2}}}{[1]^{(l_1+l_2)q^{\beta+1}}},$$

donde $0\leq\alpha_1,\alpha_2\leq\beta$, $1\leq l_1,l_2\leq q-1$ y $l_1+l_2\leq q$.

Demostración. Se sigue del Teorema 3.4.18 y la Equivalencia (3.4.13.1). □

La siguiente conjetura es más general.

Conjetura 3.4.20. *Sea q general.*

(1) *Sea $\beta\geq 0$. Definamos*

$$a=(q-1)(a_0+a_1q+\cdots+a_\beta q^\beta),$$
$$b=(q-1)(b_0+b_1q+\cdots+b_\beta q^\beta),$$

tales que

$$a_0\leq a_1\leq\cdots\leq a_\beta\leq q-1,$$
$$b_0\leq b_1\leq\cdots\leq b_\beta\leq q-1,$$
$$a_\beta+b_\beta\leq q$$

(2) *Sean α,β tales que $0\leq\alpha\leq\beta-2$. Definamos*

$$a=a_0(q^{\alpha+1}-1)+q^{\alpha+2}(q^{\beta-\alpha-1}-1),$$
$$b=b_0(q^{\alpha+1}-1)+q^{\alpha+2}(q^{\beta-\alpha-1}-1),$$

donde $1\leq a_0,b_0\leq q-1$ y $a_0+b_0=q$.

Si $a,b\in\mathbb{Z}_+$ satisfacen (1) o (2), entonces la Relación (3.4.11.1) *es válida para $\mathbb{F}_q[t]$, y por lo tanto*

$$\zeta(a)\zeta(b)=\zeta(a+b).$$

Observaciones 3.4.21.

(1) La Conjetura 3.4.20 (1) es más general que el Teorema 3.4.18 ya que a y b en el teorema pueden ser escritos como

$$a=(q-1)(l_1q^{\alpha_1}+l_1q^{\alpha_1+1}+\cdots+l_1q^\beta),$$
$$b=(q-1)(l_1q^{\alpha_2}+l_1q^{\alpha_2+1}+\cdots+l_1q^\beta).$$

(2) Cuando q es 3 o 5, la evidencia numérica sugiere que la Conjetura 3.4.20 caracteriza a los $a,b\in\mathbb{Z}_+$ tales que la Relación (3.4.11.1) es válida.

En general, la relación $\Delta_d(a,b) = c_1 S_d(a,b) + c_2 S_d(b,a)$ no implica que $c_1 = c_2 = 0$ o $c_1 = c_2 = -1$. Por ejemplo, para $\mathbb{F}_5[t]$ se tiene

$$\begin{aligned}
\Delta_d(1,1) &= S_d(1,1) - S_d(1,1) = 2S_d(1,1) - 2S_d(1,1),\\
\Delta_d(4,4) &= S_d(4,4) + 2S_d(4,4) = -S_d(4,4) - S_d(4,4),\\
\Delta_d(2,4) &= S_d(2,4) + 0S_d(4,2).
\end{aligned}$$

La siguiente conjetura fue verificada numéricamente para varios valores de q, a y b.

Conjetura 3.4.22. *Sea q general y $A = \mathbb{F}_q[t]$. Si $\Delta(a,b) = c_1 S_1(a) + c_2 S_1(b)$ con $a \neq b$, $c_1, c_2 \in \mathbb{F}_p$ y $c_1 c_2 \neq 0$, entonces $c_1 = c_2 = -1$.*

Observación 3.4.23. Si q es par, entonces evidentemente $c_1 = c_2 = 1$. Así que si fuera necesario podríamos suponer que q es impar.

Una posible forma de probar la conjetura se muestra a continuación. Suponiendo que $a < b$ se prueba como sigue que $c_2 = -1$. De acuerdo con el Teorema 2.4.19 se tiene

$$\Delta(a,b) = \sum_{i=0}^{b-a-1} f_i S_1(b-i) + \sum_{i=b-a}^{b-1} (f_i + g_{i-(b-a)}) S_1(b-i), \tag{3.4.23.1}$$

donde $f(t) = H_{a,b}(t) = f_0 + f_1 t + \cdots + f_{b-1} t^{b-1}$, $g(t) = H_{b,a}(t) = g_0 + g_1 t + \cdots + g_{a-1} t^{a-1}$, y $H_{a,b}(t)$ está dado por (2.4.19.1). Como $c_1 c_2 \neq 0$, se sigue ya sea del Teorema 2.2.1 o del Corolario 2.4.13 que a y b deben ser ambos "pares". Ahora bien, $k = (a, 0, \ldots, 0)$ es la única $(q-1)$-ada de enteros no negativos tales que $k_1 + \cdots + k_{q-1} = a$ y $\sigma(k) = k_1 + 2k_2 + \cdots + (q-1)k_{q-1} = a$ es "par". Así que los términos constantes de los polinomios $H_{a,b}(t)$ y $H_{b,a}(t)$ son ambos iguales a -1. Comparando (3.4.23.1) con la hipótesis, se sigue que $c_2 = -1$, $c_1 = f_{b-a} - 1$ y $f_i = 0$ $(1 \leq i \leq b-a-1)$, $f_{b-a+i} + g_i = 0$, $(1 \leq i \leq a-1)$.

Para probar que $c_1 = -1$ se debe probar que $f_{b-a} = 0$. Esto se sigue de la siguiente afirmación de la cual todavía no se tiene la prueba.

Afirmación. El número de coeficientes distintos de cero de $H_{a,b}(t)$ y de $H_{b,a}(t)$ es el mismo (en general esto no siempre es cierto, e.g., $q = 2$, $a = 1$ y $b = 2$).

Dado que $f_{b-a+i} \neq 0$ si y sólo si $g_i \neq 0$, $(1 \leq i \leq a-1)$, si f_{b-a} fuera diferente de cero, entonces el número de coeficientes distintos de cero de $H_{a,b}(t)$ sería mayor que el número de coeficientes distintos de cero de $H_{b,a}(t)$. Por lo tanto, $f_{b-a} = 0$ y $c_1 = -1$.

3.5. Profundidad superior

En la secciones previas, nos enfocamos solamente en el producto de dos valores zeta, pero en general, podemos multiplicar cualesquiera dos valores multizeta. De hecho en el caso racional, el producto de dos valores multizeta se puede expresar como una suma de valores multizeta. Tal expresión preserva el peso total y mantiene la filtración de profundidad, de tal manera que el $\mathbb{F}_p$-espacio lineal de todos los valores multizeta es una álgebra [Tha10, Teorema 3]. La prueba sigue un proceso inductivo. Por otro lado, para una A arbitraria con lugar al infinito no racional, la evidencia numérica parece señalar que el $\mathbb{F}_p$-espacio de todos los valores multizeta no es una álgebra.

Tabla 3.5.1: Los elementos del producto mezclado de (a_1, a_2) y (b) están en la tercera columna.

(a_1, a_2)	$(b, 0)$	$(a_1 + b, a_2)$
(a_1, a_2)	$(0, b)$	$(a_1, a_2 + b)$
$(a_1, a_2, 0)$	$(0, 0, b)$	(a_1, a_2, b)
$(a_1, 0, a_2)$	$(0, b, 0)$	(a_1, b, a_2)
$(0, a_1, a_2)$	$(b, 0, 0)$	(b, a_1, a_2)

Tabla 3.5.2: Los elementos del producto mezclado de (a_1, a_2) y (b_1, b_2) están en la tercera columna.

(a_1, a_2)	(b_1, b_2)	$(a_1 + b_1, a_2 + b_2)$
$(0, a_1, a_2)$	$(b_1, 0, b_2)$	$(b_1, a_1, a_2 + b_2)$
$(0, a_1, a_2)$	$(b_1, b_2, 0)$	$(b_1, a_1 + b_2, a_2)$
$(a_1, 0, a_2)$	$(0, b_1, b_2)$	$(a_1, b_1, a_2 + b_2)$
$(a_1, 0, a_2)$	$(b_1, b_2, 0)$	$(a_1 + b_1, b_2, a_2)$
$(a_1, a_2, 0)$	$(0, b_1, b_2)$	$(a_1, a_2 + b_1, b_2)$
$(a_1, a_2, 0)$	$(b_1, 0, b_2)$	$(a_1 + b_1, a_2, b_2)$
$(0, 0, a_1, a_2)$	$(b_1, b_2, 0, 0)$	(b_1, b_2, a_1, a_2)
$(0, a_1, 0, a_2)$	$(b_1, 0, b_2, 0)$	(b_1, a_1, b_2, a_2)
$(0, a_1, a_2, 0)$	$(b_1, 0, 0, b_2)$	(b_1, a_1, a_2, b_2)
$(a_1, 0, 0, a_2)$	$(0, b_1, b_2, 0)$	(a_1, b_1, b_2, a_2)
$(a_1, 0, a_2, 0)$	$(0, b_1, 0, b_2)$	(a_1, b_1, a_2, b_2)
$(a_1, a_2, 0, 0)$	$(0, 0, b_1, b_2)$	(a_1, a_2, b_1, b_2)

3.5.1. Aproximación 1

El *producto mezclado* de los vectores $\underline{a} = (a_1, \ldots, a_{r_1})$ y $\underline{b} = (b_1, \ldots, b_{r_2})$ de enteros positivos, denotado por $\mathrm{pm}(\underline{a}, \underline{b})$, es la unión de todos los vectores $\underline{c} = (c_1, \ldots, c_r)$ obtenidos al insertar ceros, en cualquier posición que se requiera (los ceros se pueden insertar tanto antes del primer término como después del último) tanto en $(a_1, \ldots, a_{r_1})$ como en $(b_1, \ldots, b_{r_2})$ de tal manera que los dos nuevos vectores tengan la misma longitud r, con $\max\{r_1, r_2\} \leq r \leq r_1 + r_2$ y sumar los dos vectores resultantes término a término. Los ceros se deben insertar de tal manera que ninguna c_i sea cero [Wal00].

Por ejemplo, los elementos del producto mezclado de (a_1, a_2) y (b) se listan en la tercera columna de la Tabla 3.5.1. De manera similar, los elementos del producto mezclado de (a_1, a_2) y (b_1, b_2) se muestran en la tercera columna de la Tabla 3.5.2.

El producto mezclado nos será de utilidad para escribir de forma más compacta el producto de valores multizeta.

Calculemos primero el producto $\zeta(a_1,a_2)\zeta(b)$ para $\mathbb{F}_q[t]$ suponiendo que $\Delta(a_1,b)=0$ y $\Delta(a_2,b)=0$, i.e., $S_1(a_1)S_1(b)=S_1(a_1+b)$ y $S_1(a_2)S_1(b)=S_1(a_2+b)$. Del Teorema 1.4.2 se sigue que $S_d(a_i)S_d(b)=S_d(a_i+b)$ $(i=1,2)$ para toda $d\geq 0$.

Ahora

$$\zeta(a_1,a_2)\zeta(b)=\sum_{d_1>d_2} S_{d_1}(a_1)S_{d_2}(a_2)\sum_{d_3} S_{d_3}(b)=\mathcal{S}_1+\mathcal{S}_2+\mathcal{S}_3+\mathcal{S}_4+\mathcal{S}_5$$

donde

$$\begin{aligned}
\mathcal{S}_1&=\sum_{d_1>d_2>d_3} S_{d_1}(a_1)S_{d_2}(a_2)S_{d_3}(b),\\
\mathcal{S}_2&=\sum_{d_1>d_3>d_2} S_{d_1}(a_1)S_{d_2}(a_2)S_{d_3}(b),\\
\mathcal{S}_3&=\sum_{d_3>d_1>d_2} S_{d_1}(a_1)S_{d_2}(a_2)S_{d_3}(b),\\
\mathcal{S}_4&=\sum_{d_1=d_3>d_2} S_{d_1}(a_1)S_{d_2}(a_2)S_{d_3}(b)=\sum_{d_1>d_2} S_{d_1}(a_1+b)S_{d_2}(a_2),\\
\mathcal{S}_5&=\sum_{d_1>d_2=d_3} S_{d_1}(a_1)S_{d_2}(a_2)S_{d_3}(b)=\sum_{d_1>d_2} S_{d_1}(a_1)S_{d_2}(a_2+b).
\end{aligned}$$

La cuarta y quinta igualdades se siguen usando el hecho que $S_{d_1}(a_1)S_{d_1}(b)=S_{d_1}(a_1+b)$ y $S_{d_2}(a_2)S_{d_2}(b)=S_{d_2}(a_2+b)$. Por lo tanto,

$$\begin{aligned}
\zeta(a_1,a_2)\zeta(b)&=\zeta(a_1,a_2,b)+\zeta(a_1,b,a_2)+\zeta(b,a_1,a_2)+\zeta(a_1+b,a_2)+\zeta(a_1,a_2+b)\\
&=\sum_{\underline{c}\in\mathrm{pm}(\underline{a},\underline{b})}\zeta(\underline{c}),
\end{aligned}$$

donde $\underline{a}=(a_1,a_2)$ y $\underline{b}=(b)$.

Análogamente, si $\Delta(a_i,b_j)=0$ para $1\leq i,j\leq 2$, entonces

$$\begin{aligned}
\zeta(a_1,a_2)\zeta(b_1,b_2)&=\zeta(a_1,a_2,b_1,b_2)+\zeta(a_1,b_1,a_2,b_2)+\zeta(b_1,a_1,a_2,b_2)\\
&\quad+\zeta(a_1,b_1,b_2,a_2)+\zeta(b_1,a_1,b_2,a_2)+\zeta(b_1,b_2,a_1,a_2)\\
&\quad+\zeta(a_1,a_2+b_1,a_2)+\zeta(a_1+b_1,a_2,b_2)+\zeta(a_1,b_1,a_2+b_2)\\
&\quad+\zeta(b_1,a_1,a_2+b_2)+\zeta(a_1+b_1,b_2,a_2)+\zeta(b_1,a_1+b_2,a_2)\\
&\quad+\zeta(a_1+b_1,a_2+b_2)\\
&=\sum_{\underline{c}\in\mathrm{pm}(\underline{a},\underline{b})}\zeta(\underline{c}),
\end{aligned}$$

donde $\underline{a}=(a_1,a_2)$ y $\underline{b}=(b_1,b_2)$.

Tenemos el siguiente

Teorema 3.5.1. *Sean q general, $\underline{a}=(a_1,\ldots,a_{r_1})\in\mathbb{Z}_+^{r_1}$ y $\underline{b}=(b_1,\ldots,b_{r_2})\in\mathbb{Z}_+^{r_2}$ tales que $\Delta(a_i,b_j)=0$, $(1\leq i\leq r_1,\ 1\leq j\leq r_2)$ en $\mathbb{F}_q[t]$, entonces para cualquier A con el lugar al infinito de cualquier grado y usando la convención A1 para los signos se tiene*

$$\zeta(\underline{a})\zeta(\underline{b})=\sum_{c\in\mathrm{pm}(\underline{a},\underline{b})}\zeta(\underline{c}).$$

Demostración. Se sigue del Teorema 3.4.4 y cálculos rutinarios. □

3.5.2. Aproximación 2

Sean $a_1, a_2, b \in \mathbb{Z}_+$ tales que $\Delta(a_1, a_2) = -S_1(a_1) - S_1(a_2)$ y $\Delta(a_1, b) = -S_1(a_1) - S_1(b)$ son válidos en $\mathbb{F}_q[t]$. Como antes,

$$\begin{aligned}\zeta(a_1, a_2)\zeta(b) &= \sum_{d_1>d_2} S_{d_1}(a_1)S_{d_2}(a_2)\sum_{d_3} S_{d_3}(b)\\ &= \zeta(a_1, a_2, b) + \zeta(a_1, b, a_2) + \zeta(b, a_1, a_2) + \mathcal{S}_4 + \mathcal{S}_5\end{aligned}$$

donde

$$\begin{aligned}\mathcal{S}_4 &= \sum_{d_1=d_3>d_2} S_{d_1}(a_1)S_{d_2}(a_2)S_{d_3}(b),\\ \mathcal{S}_5 &= \sum_{d_1>d_2=d_3} S_{d_1}(a_1)S_{d_2}(a_2)S_{d_3}(b)\end{aligned}$$

De la hipótesis se sigue que $S_{d_1}(a_1)S_{d_1}(b) = S_{d_1}(a_1+b) - S_{d_1}(a_1, b) - S_{d_1}(b, a_1)$. Entonces,

$$\mathcal{S}_4 = \sum_{d_1>d_2} (S_{d_1}(a_1 + b) - S_{d_1}(a_1, b) - S_{d_1}(b, a_1))S_{d_2}(a_2) = \zeta(a_1 + b, a_2) - \mathcal{S}'_4 - \mathcal{S}''_4,$$

donde

$$\begin{aligned}\mathcal{S}'_4 &= \sum_{d_1>d_2} S_{d_1}(a_1, b)S_{d_2}(a_2),\\ \mathcal{S}''_4 &= \sum_{d_1>d_2} S_{d_1}(b, a_1)S_{d_2}(a_2).\end{aligned}$$

Ahora bien,

$$\mathcal{S}'_4 = \sum_{d_1>d_2}\sum_{d_1>d_3} S_{d_1}(a_1)S_{d_2}(a_2)S_{d_3}(b) = \zeta(a_1, a_2, b) + \zeta(a_1, b, a_2) + \mathcal{S}_5.$$

Por otro lado,

$$\mathcal{S}''_4 = \sum_{d_1>d_2}\sum_{d_1>d_3} S_{d_1}(b)S_{d_3}(a_1)S_{d_2}(a_2) = \zeta(b, a_2, a_1) + \zeta(b, a_1, a_2) + \mathcal{S}'''_4,$$

donde

$$\begin{aligned}\mathcal{S}'''_4 &= \sum_{d_1>d_2=d_3} S_{d_1}(b)S_{d_3}(a_1)S_{d_2}(a_2)\\ &= \sum_{d_1>d_2=d_3} S_{d_1}(b)(S_{d_2}(a_1 + a_2) - S_{d_2}(a_1, a_2) - S_{d_2}(a_2, a_1))\\ &= \zeta(b, a_1 + a_2) - \sum_{d_1>d_2} S_{d_1}(b)S_{d_2}(a_1, a_2) - \sum_{d_1>d_2} S_{d_1}(b)S_{d_2}(a_2, a_1)\\ &= \zeta(b, a_1 + a_2) - \zeta(b, a_1, a_2) - \zeta(b, a_2, a_1).\end{aligned}$$

La segunda igualdad se sigue usando que $S_{d_2}(a_1)S_{d_2}(a_2) = S_{d_2}(a_1 + a_2) - S_{d_2}(a_1, a_2) - S_{d_2}(a_2, a_1)$. Poniendo todo junto y simplificando obtenemos

$$\zeta(a_1, a_2)\zeta(b) = \zeta(b, a_1, a_2) + \zeta(a_1 + b, a_2) - \zeta(b, a_1 + a_2).$$

De esta manera hemos probado el siguiente teorema.

Teorema 3.5.2. *Sean q general, $a_1, a_2, b \in \mathbb{Z}_+$ tales que $\Delta(a_1, a_2) = -S_1(a_1) - S_1(a_2)$ y $\Delta(a_1, b) = -S_1(a_1) - S_1(b)$ son válidas para $\mathbb{F}_q[t]$. Entonces para cualquier A con el lugar al infinito de cualquier grado y usando la convención A2 para los signos se tiene*

$$\zeta(a_1, a_2)\zeta(b) = \zeta(b, a_1, a_2) + \zeta(a_1 + b, a_2) - \zeta(b, a_1 + a_2).$$

CAPÍTULO 4

Acerca de von Staudt para los números de Bernoulli-Carlitz

4.1. Introducción

En 1935, L. Carlitz introdujo y estudió los análogos a los números de Bernoulli en característica positiva [Car35], para los cuales fue capaz de probar un teorema análogo al Teorema de von Staudt-Clausen [Car37, Car40]. Para una exposición auto-contenida y en un lenguaje moderno vea [Gos78]; para algunas identidades entre estos análogos a los números de Bernoulli vea [Gek89]. En los libros [Gos96, Tha04], el lector interesado encontrará teoremas relacionados con los números de Bernoulli desde la perspectiva de los campos de funciones.

Recordemos primero la situación clásica. Los números de Bernoulli $\mathcal{B}_m$ y sus asociados $\mathcal{B}_m/m$ son importantes en varias ramas de las matemáticas. Vea por ejemplo, [MS74, Leh88] y [Tha04, 4.16]. El Teorema de von Staudt-Clausen determina la parte fraccional de los números de Bernoulli. Más precisamente, si $m > 0$ es un número par, $\mathcal{B}_m - \sum 1/p$ es un entero racional, donde la suma se toma sobre los primos p tales que $p-1$ divide a m. De aquí que el denominador de $\mathcal{B}_m$ es el producto de todos los primos p tales que $p-1$ divide a m. El Teorema de Lipschitz-Sylvester dice que $a^m(a^m-1)\mathcal{B}_m/m$ es un entero para cualquier número entero a. Combinando estos dos resultados, se sigue fácilmente que los primos que dividen a los denominadores de $\mathcal{B}_m$ y de $\mathcal{B}_m/m$ son exactamente los mismos (escoja a que sea una raíz primitiva módulo p que divida a m).

Para cualquier entero positivo, los números de Bernoulli-Carlitz B_m son elementos de $\mathbb{F}_q(t)$, pero sólo estamos interesados en las m's que son múltiplos de $q-1$, es decir en las m's “pares” ya que $B_m = 0$ si m no es “par”. Carlitz fue capaz de probar, sobre el campo de funciones racionales $K = \mathbb{F}_q(t)$, un análogo al Teorema de von Staudt-Clausen (Teorema 4.2.5). El caso $q = 2$ hay que tratarlo con cuidado, como fue notado por Carlitz en [Car41]. Ahí, él da una corrección cuando $q = 2$ de su teorema análogo al Teorema de von Staudt-Clausen, ya que como originalmente fue establecido en [Car37, Car40] era incorrecto.

Notemos que B_m/m no tiene sentido para los números de Bernoulli-Carlitz B_m ya que m puede ser cero en característica positiva. Por otro lado, D. Thakur prueba que un buen análogo para $\mathcal{B}_m/m$ en el caso de campos de funciones es $B_m(m-1)!_C/m!_C$, donde $m!_C$ denota el factorial de Carlitz. En [Tha04, Teorema 4.16.5], Thakur da un teorema que compara la descomposición en factores primos de los denominadores de B_m y $B_m(m-1)!_C/m!_C$. El caso $q>2$ está resuelto y el caso $q=2$ está resuelto excepto por algunas posibles excepciones. El propósito de este capítulo es completar ese caso.

4.2. Números de Bernoulli-Carlitz

Aquí, nos enfocamos en el caso $A=\mathbb{F}_q[t]$, con $q=p^n$, y p un número primo. Para la definición de D_k, L_k y $[k]$ vea la Sección 2.1.

La función factorial para A fue definida por Carlitz [Car37] como sigue:

Definición 4.2.1. Sea $m\in\mathbb{Z}_+$ y sea $m=\sum m_i q^i$ su expansión q-ádica. Entonces, el factorial de Carlitz de m está definido por

$$m!_C := \prod_i D_i^{m_i}.$$

El factorial de Carlitz tiene propiedades de divisibilidad análogas a las propiedades del factorial clásico [Tha04, Capítulo 4].

Ejemplos 4.2.2.

(1) Con esta definición, tenemos que $q^l!_C = D_l$.

(2) Para cualquier entero positivo m, $(qm-1)!_C=(q(m-1))!_C$. De hecho, si $m-1=\sum_{i=0}^{\nu} n_i q^i$ es la expansión q-ádica de $m-1$, entonces, $qm-1=q-1+\sum_{i=0}^{\nu} n_i q^{i+1}$ es la expansión q-ádica de $qm-1$.

Ahora, usamos el factorial de Carlitz para definir los análogos a los números de Bernoulli. Para cada entero positivo m, los números de Bernoulli-Carlitz $B_m\in\mathbb{F}_q(t)$ se definen por medio de la función generadora

$$\frac{z}{e_C(z)}=\sum_{m=0}^{\infty}\frac{B_m}{m!_C}z^m,$$

donde e_C la exponencial de Carlitz

$$e_C(z)=\sum_{j=0}^{\infty}\frac{z^{q^j}}{D_j}.$$

Observaciones 4.2.3.

(1) Note que la suma que define a los números de Bernoulli-Carlitz B_m contiene únicamente términos “pares”.

(2) Aquí, B_m difiere de los correspondientes B_m en los artículos de Carlitz por $(-1)^m$.

(3) Para cualquier l, tenemos [Tha04]

$$\frac{B_{p^l m}}{(p^l m)!_C} = \left(\frac{B_m}{m!_C}\right)^{p^l}.$$

Podemos ver esto tomando la p-ésima potencia de la función generadora y comparando al sustituir z por z^p.

Definamos $A_m^{(k)}$ por medio de

$$e_C(z)^{q^k-1} = \sum_{m=q^k-1}^{\infty} \frac{A_m^{(k)}}{m!_C} z^m. \tag{4.2.3.1}$$

Carlitz [Car37] probó que

$$B_m = \sum_{q^k \leq m+1} \frac{A_m^{(k)}}{L_k}, \tag{4.2.3.2}$$

donde $A_m^{(k)}$ es entero y múltiplo de $(q^k-1)!_C$. Sea $C_m^{(k)} \in A$ tal que $A_m^{(k)} = C_m^{(k)}(q^k-1)!_C$. Entonces,

$$\frac{A_m^{(k)}}{L_k} = \frac{C_m^{(k)}(q^k-1)!_C}{L_{k-1}} \frac{1}{[k]} = C_m^{(k)} \frac{(D_1 \cdots D_{k-1})^{q-1}}{L_{k-1}} \frac{1}{[k]}. \tag{4.2.3.3}$$

Ahora, L_{k-1} divide a $(D_1 \cdots D_{k-1})^{q-1}$ y, excepto cuando $q = 2 = k$, los primos en $[k]$ de grado menor que k dividen al cociente resultante. Más aún, excepto para el caso $q = 2 = k$, los factores irreducibles del denominador de $(q^k-1)!_C/L_k$ son todos de grado k.

Sea $m = \sum m_i p^i$ la expansión p-ádica de m. Consideremos las condiciones

$$h = \frac{\sum m_i}{n(p-1)} \in \mathbb{Z}_+, \quad q^h - 1 \mid m. \tag{4.2.3.4}$$

Observación 4.2.4. Carlitz demostró [Car37, p. 514], [Car40, p. 63] que si P es un primo de grado k, y k no satisface las condiciones (4.2.3.4), entonces $A_m^{(k)} \equiv 0 \text{ mód } P$.

Tanto los números de Bernoulli clásicos $\mathcal{B}_m$ como sus asociados $\mathcal{B}_m/m$ son importantes ya que aparecen en muchas áreas: sumas de potencias, medidas y valores especiales de las funciones zeta y de las L-funciones, y también en topología, sólo por mencionar algunas áreas. Vea por ejemplo el Apéndice B del libro de Milnor [MS74] para las aplicaciones a topología. Von Staudt probó que los primos que dividen los denominadores de $\mathcal{B}_m$ y $\mathcal{B}_m/m$ son exactamente los mismos.

Los números $B_m(m-1)!_C/m!_C$ se pueden pensar [Tha04, 4.16] como los análogos a $\mathcal{B}_m/m$, aunque los primeros parece que no satisfacen congruencias tipo Kummer. Para los números de Bernoulli-Carlitz, Thakur probó un análogo al Teorema de Lipschitz-Sylvester [Tha04, Teorema 4.16.3] (vea también algunas variantes más débiles en [Car37, Teorema 5] y en [Car41, Teorema 3]). Pero, también notó que ello no implica que los primos que dividen a los denominadores en la situación análoga son los mismos. De aquí que los siguientes dos teoremas que describen los denominadores por separado pueden ser considerados como análogos al Teorema de von Staudt-Clausen.

Denotemos con P_k al producto de todos los polinomios primos mónicos de grado k. A continuación presentamos el Teorema de Carlitz análogo al Teorema de von Staudt-Clausen para los números de Bernoulli-Carlitz.

Teorema 4.2.5 (Carlitz [Car37, Car40, Car41])**.** *Sea $A = \mathbb{F}_q[t]$. Sean $m \in \mathbb{Z}_+$ "par" y $m = \sum m_i p^i$ su expansión p-ádica. Denotemos por $d(m)$ al denominador mónico de B_m. Sea h como en* (4.2.3.4)*. Entonces,*

1. *Sea $q > 2$. Si h es entero y $q^h - 1$ divide a m, entonces $d(m) = P_h$, en otro caso $d(m) = 1$.*

2. *Sea $q = 2$, $h \neq 2$. Si $q^h - 1$ divide a m, entonces $d(m) = P_h$, en otro caso $d(m) = 1$. Sea $h = 2$. Si $q^h - 1 = 3$ divide a m, entonces $d(m) = P_2$ cuando m es un múltiplo de 2 y $d(m) = [2] = P_1 P_2$ en otro caso. Si $q^h - 1$ no divide a m, entonces cuando m no es un múltiplo de 2, $d(m) = P_1$ y en otro caso $d(m) = 1$.*

Observación 4.2.6. Para $q = 2$, el resultado como fue originalmente establecido en [Car37], [Car40] y [Gos78] no es correcto. Una versión corregida de este resultado se encuentra en [Car41].

Teorema 4.2.7. (1) *Sea $q > 2$. Entonces, los primos que dividen al denominador de B_m o de $B_m(m-1)!_C/m!_C$ son los mismos. De hecho, si q^k es la máxima potencia de q que divide a m, y si el denominador de B_m es P_h, entonces el denominador de $B_m(m-1)!_C/m!_C$ es $P_h^{\lfloor k/h \rfloor + 1}$.*

(2) *Sea $q = 2$. Entonces, los primos que dividen al denominador de B_m o de $B_m(m-1)!_C/m!_C$ son los mismos, a menos que m sea de la forma $2 + 2^\alpha$ con $\alpha > 1$. Si 2^k es la máxima potencia de 2 que divide a m, y si el denominador de B_m es $\mathcal{D}$, entonces el denominador de $B_m(m-1)!_C/m!_C$ es $\mathcal{D}^{\lfloor k/h \rfloor + 1}$.*

(3) *Sea $q = 2$, $m = 2 + 2^\alpha$, $\alpha > 1$.*

a) Si $m \equiv 0 \bmod 3$, entonces el denominador de $B_m(m-1)!_C/m!_C$ es $P_1 P_2 = t(t+1)(t^2+t+1)$.

b) Si $m \equiv 1 \bmod 3$, entonces el denominador de $B_m(m-1)!_C/m!_C$ es $P_1 = t(t+1)$.

Demostración. (1) Vea [Tha04, Teorema 4.16.5].

Por razones de tipo práctico, probaremos (3) antes que (2).

(3) Note que para cualquier q,

$$\frac{(m-1)!_C}{m!_C} = \frac{1}{L_k} \tag{4.2.7.1}$$

donde q^k es la máxima potencia de q que divide a m.

Escribamos $B_m = N_m/d(m)$ con N_m y $d(m)$ primos relativos.

Si $m \equiv 0$ mód 3, se sigue que $m = 2 + 2^{2i}$, ($i \geq 1$). Entonces $h = 2$, $q^h - 1 = 3$ divide a m y m es par. Así, $d(m) = P_2 = t^2 + t + 1$. Como $(m-1)!_C/m!_C = 1/L_1$, tenemos

$$B_m = \frac{N_m}{P_2}, \quad B_m \frac{(m-1)!_C}{m!_C} = \frac{N_m}{P_2} \frac{1}{P_1}.$$

Si $m = 2+2^{2i+1}$, entonces $h = 2$, $q^h - 1 = 3$ no divide a m, y m es par. Así $d(m) = 1$. Por lo tanto,

$$B_m = N_m, \quad B_m \frac{(m-1)!_C}{m!_C} = \frac{N_m}{1} \frac{1}{P_1}.$$

Resta probar que P_1 no divide a N_m. Dado que m no es una potencia de 2, de (4.2.3.1) se sigue que $A_m^{(1)} = 0$. Sea $k > 2$ tal que $2^k - 1 \leq m$. Claramente, k no satisface (4.2.3.4). Ahora, si P es un primo de grado k, de la Observación 4.2.4 se sigue que P_k divide a $C_m^{(k)}$ así que $A_m^{(k)}/L_k$ pertenece a A. También, de (4.2.3.3), se sigue que P_1 divide a $A_m^{(k)}/L_k$. Por lo tanto,

$$B_m = G_m + \frac{A_m^{(2)}}{L_2}, \tag{4.2.7.2}$$

donde $G_m \in \mathbb{F}_q[t]$ es divisible por P_1 y

$$G_m = \sum_{q^k - 1 \leq m, k \neq 2} \frac{A_m^{(k)}}{L_k}. \tag{4.2.7.3}$$

Supongamos primero que $m = 2 + 2^{2i}$. Entonces

$$\frac{A_m^{(2)}}{L_2} = \frac{t^2 + t^{2^{2i}}}{[1][2]} = \frac{[2i-1]^2}{P_1^2 P_2} = \frac{N}{P_2},$$

donde $N = [2i-1]^2/P_1^2 \in A$ y N es primo relativo a P_2. Del Algoritmo Euclidiano, sabemos que existen $Q(t)$ y $R(t)$ en A, únicos, tales que $N = P_2 Q(t) + R(t)$, donde R es distinto de cero y $\deg R < 2$. Ya que N y P_2 son invariantes respecto de los automorfismos $t \to t+1$ de A, se sigue que $R(t) = R(t+1)$, así que R no es t ni $t+1$. De aquí que $R = 1$. Ahora, dado que N es primo relativo a P_1^2, entonces $N \equiv 1$ mód P_1^2. Luego, $Q(t)P_2 \equiv 0$ mód P_1^2. Puesto que P_2 y P_1^2 son primos relativos, se sigue que $Q \equiv 0$ mód P_1^2. Tenemos que

$$B_m = \frac{1}{P_2}\left(G_m + Q + 1\right),$$

donde P_1 divide a $G_m + Q$. Por lo tanto, el numerador de B_m no es divisible por P_1.

Ahora, sea $m = 2 + 2^{2i+1}$, ($i \geq 1$). Entonces

$$\frac{A_m^{(2)}}{L_2} = \frac{t^2 + t^{2^{2i+1}}}{[1][2]} = \frac{[2i]^2}{P_1^2 P_2}.$$

Así $A_m^{(2)}/L_2$ está en A y no es divisible por P_1. Dado que $B_m = G_m + A_m^{(2)}/L_2$, donde G_m es divisible por P_1, se sigue que el numerador de B_m no es divisible por P_1.

(2) Ahora, tratemos el caso cuando m es un entero que no es de la forma $2 + 2^\alpha$, con $\alpha > 1$. Si $k = 0$, i.e., si m es impar, de (4.2.7.1) tenemos que $B_m = B_m(m-1)!_C/m!_C$. De hecho, si $h \neq 2$, por la parte que ya está probada por Thakur [Tha04, Teorema 4.16.5], tenemos que los primos que dividen al denominador de B_m y los que dividen al denominador de $B_m(m-1)!_C/m!_C$ son exactamente los mismos.

Si $m = 4 + 2^\alpha$, con $\alpha > 2$, escribamos $m = 2m'$, donde $m' = 2 + 2^{\alpha-1}$. Entonces,

$$\begin{aligned}\frac{(2m'-1)!_C B_{2m'}}{(2m')!_C} &= \frac{(2m'-1)!_C}{(2(m'-1))!_C}\frac{(2(m'-1))!_C}{(m'-1)!_C^2}\left(\frac{(m'-1)!_C B_{m'}}{m'!_C}\right)^2 \\ &= [1][\alpha]\left(\frac{(m'-1)!_C B_{m'}}{m'!_C}\right)^2.\end{aligned}$$

De la parte (3), tenemos

$$\frac{(2m'-1)!_C B_{2m'}}{(2m')!_C} = \begin{cases} \frac{[1][\alpha]N_{m'}^2}{P_1^2} & \text{si } \alpha \text{ es par,} \\ \frac{[1][\alpha]N_m^2}{P_1^2P_2^2} & \text{si } \alpha \text{ es impar.}\end{cases}$$

Entonces, el denominador de $B_m(m-1)!_C/m!_C$ es 1 o P_2^2, dependiendo de que α sea par o no.

A continuación aplicamos inducción sobre $k > 2$. Como,

$$\frac{(2m-1)!_C B_{2m}}{(2m)!_C} = [1][2]\cdots[k][\alpha+1]\left(\frac{(m-1)!_C B_m}{m!_C}\right)^2,$$

vemos que si un primo P divide al denominador de $B_{2m}(2m-1)!_C/(2m)!_C$, entonces divide al denominador de $B_m(m-1)!_C/m!_C$, lo cual por la hipótesis de inducción implica que P divide al denominador B_m. La comparación de las condiciones del Teorema 4.2.5 para m y para qm implica que P divide al denominador de B_{2m}.

Note que $[i]$ es el producto de todos los primos mónicos en A cuyo grado divide a i. Entonces $P_h^{\lfloor k/h \rfloor}$ es la máxima potencia de P_h que divide a L_k. Se sigue que el denominador de $B_m(m-1)!_C/m!_C$ es como se afirmó. $\square$

Observación 4.2.8. David Goss observó que nuestros resultados encajan en el marco de su trabajo [Gos11]. De hecho, veremos a continuación que el grupo $S_{(q)}$ (definido a continuación) se puede ver como simetrías de nuestro teorema tipo von Staudt-Clausen.

Sea q una potencia de p y sea $x \in \mathbb{Z}_p$. Escribamos x q-ádicamente como

$$x = \sum_{i=0}^{\infty} c_i q^i$$

donde $0 \leq c_i < q$ para toda i. Sea ρ una permutación del conjunto $\{0, 1, 2, \ldots\}$. D. Goss define [Gos11] $\rho_*(x)$, $x \in \mathbb{Z}_p$, por

$$\rho_*(x) := \sum_{i=0}^{\infty} c_i q^{\rho(i)}.$$

Sea $S_{(q)}$ el subgrupo de las permutaciones de $\mathbb{Z}_p$ obtenida al variar ρ sobre todas las permutaciones de $\{0, 1, 2, \ldots\}$.

Denotemos con $\partial(m)$ al denominador de $B_m(m-1)!_C/m!_C$ para A. El siguiente corolario prueba que la condición de que un primo divida a $\partial(m)$ satisface las simetrías dadas por los Corolarios 5 y 6 en [Gos11].

Corolario 4.2.9. *Sea q una potencia de p y $\mathfrak{P}$ un primo de grado h. Si $q = 2$ y $h = 1$, entonces la condición $v_{\mathfrak{P}}(\partial(m)) > 0$ es un invariante del subgrupo $\tilde{S}_4$ de $S_{(4)}$ que surge de las permutaciones de $\{0, 1, 2, \ldots\}$ que fijan a 0. De otra manera, la condición $v_{\mathfrak{P}}(\partial(m)) > 0$ es un invariante de la acción de $S_{(q^h)}$ sobre los enteros positivos divisibles por $q - 1$.* $\square$

APÉNDICE A

Lista de conjeturas probadas

En este apéndice presentamos la relación de conjeturas que fueron probadas en este trabajo. Algunas de estas conjeturas fueron formuladas por Thakur y otras por el autor en su tesis de maestría.

Tabla A.0.1: Conjeturas formuladas por Thakur en [Tha09b].

Lugar donde aparece la conjetura	Probada en
4.1.2 Índices grandes especiales, pág. 1338	Teorema 2.3.14, Ejemplos 2.3.17
4.1.3 Ambos índices grandes, fórmulas 1, 2 y 5, pág. 1338	Ejemplo 2.4.9 Corolario 2.4.8
4.1.3 Ambos índices grandes, fórmulas 3 y 4, pág. 1338	Ejemplo 2.4.7
4.1.4 Paso 2 de la conjetura recursiva para $q = 2$, pág. 1339	Teorema 2.5.2
4.3.1 Una conjetura general para q, pág. 2342	Teorema 2.6.2
5.3 La restricción "par", pág. 2344	Teorema 2.2.1, Corolario 2.4.13
4.1.4 Paso 3 de la conjetura recursiva para $q = 2$, pág. 2340	Todavía no ha sido probada

El paso 1 de la conjetura recursiva para $q = 2$ fue probado por Thakur en [Tha10].

Tabla A.0.2: Conjeturas formuladas por el autor.

Conjetura(s)	Probada en
1.4.7 excepto el apartado 4	Teorema 2.3.14, Corolario 2.3.19 y Observación 2.3.21
1.5.1	Teoremas 2.6.5 y 2.6.6
1.5.2	Teorema 2.6.7
1.5.5	Teorema 2.6.6
1.5.3	Probada parcialmente en la Proposición 2.6.9
1.5.7.1	Teorema 2.7.2
1.5.3, 1.5.4, 1.5.6, 1.5.7 excepto 1.5.7.1, 1.5.9	Todavía no han sido probadas

La Conjetura 1.5.9 ya fue probada por el autor, pero la prueba no fue incluida en este trabajo.

APÉNDICE B

Artículos publicados

Lista de artículos publicados.

A.1 José Alejandro Lara Rodríguez. Relations between multizeta values in characteristic p. *J. Number Theory*, 131(4):2081–2099, 2011.

A.2 José Alejandro Lara Rodríguez. Special relations between function field multizeta values and parity results. *Journal of the Ramanujan Mathematical Society*, 27(3):275–293, 2012.

A.3 José Alejandro Lara Rodríguez. On von Staudt for Bernoulli-Carlitz numbers. *J. Number Theory*, 132(4):495-501, 2012.

B.1. Relations between multizeta values in characteristic p

Journal of Number Theory 131 (2011) 2081–2099

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Relations between multizeta values in characteristic p

José Alejandro Lara Rodríguez

Departamento de Control Automático, Centro de Investigación y de Estudios Avanzados del IPN, Av. Instituto Politécnico Nacional 2508, San Pedro Zacatenco, 07360 México, D.F., Mexico

ARTICLE INFO

Article history:
Received 28 December 2010
Revised 20 April 2011
Accepted 10 May 2011
Available online xxxx
Communicated by David Goss

Keywords:
Multizeta
Function fields
Product of zeta values
Periods
Drinfeld modules

ABSTRACT

We study relations between the multizeta values for function fields introduced by D. Thakur. The product $\zeta(a)\zeta(b)$ is a linear combination of multizeta values. For $q = 2$, a full conjectural description of how the product of two zeta values can be described as the sum of multizetas was given by Thakur. The recursion part of this recipe was generalized by the author. In this paper, the main conjecture formulated by the author, as well as some conjectures of Thakur are proved. Moreover, for general q, we prove closed formulas as well as a recursive recipe to express $\zeta(a)\zeta(b)$ as a sum of multizeta values.

1. Introduction

We refer to [Wal05], and the references in there, for a survey of many exciting recent developments related to the multizeta values introduced by Euler. We refer to [Gos96,Tha04] for discussion of Goss zeta functions in connection with the function field arithmetic.

Dinesh Thakur [Tha04, Section 5.10] introduced two types of multizeta values for function fields over finite fields of characteristic p, one complex valued (generalizing the Artin–Weil zeta function) and the other with values in Laurent series over finite fields (generalizing the Carlitz–Goss zeta function). In this paper, we only focus on the latter. For its properties, connections with Drinfeld modules and Anderson t-motives, we refer the reader to [AT09,Tha04,Tha09,Tha10].

Thakur proves the existence of "shuffle" relations for the multizeta values (for a general A with a rational place at infinity) [Tha10]. In particular, he shows that the product of multizeta values can also be expressed as a sum of some multizeta values, so that the $\mathbb{F}_p$-span of all multizeta values is an algebra. In the function field case, the identities are much more complicated than the classical shuffle identities. In fact there are two types of identities, one with $\mathbb{F}_p(t)$ coefficients and the other with $\mathbb{F}_p$

E-mail addresses: lrodri@uady.mx, jlara@ctrl.cinvestav.mx.

0022-314X/$ – see front matter © 2011 Published by Elsevier Inc.
doi:10.1016/j.jnt.2011.05.007

coefficients. (Note that although for many purposes a good analog of $\mathbb{Q}$ is $\mathbb{F}_q(t)$, the prime field in characteristic p (0 respectively) is $\mathbb{F}_p$ ($\mathbb{Q}$ respectively).) We concentrate only on the latter type.

The results in [Tha10], although effective, are not explicit and bypass the explicit conjectures formulated in [Tha09,Lar09,Lar10]. In this paper, we use the ideas of the process in [Tha10] to prove the main conjecture formulated in [Lar09,Lar10] and to give a closed formula for the expression of the product of zeta values as the sum of multizeta values (Theorems 6.3 and 7.1). More precisely, for general q, we prove that the expression of $\zeta(a)\zeta(b)$ as a sum of multizeta values is obtained by a recursive process; we effectively determine the recursion length, the terms and the number of terms to be added at each step of the recursion (Theorem 5.13). Also, when $q=2$, we give formulas to compute the initial values (Theorem 6.1 and Corollary 7.2) and, using one of these formulas, some conjectures in [Tha09] are proved.

2. Frequently used notation

$\mathbb{Z}$	{integers}
$\mathbb{Z}_+$	{positive integers}
q	a power of a prime p, $q=p^s$
$\mathbb{F}_q$	a finite field of q elements
t	an independent variable
A	the polynomial ring $\mathbb{F}_q[t]$
A_+	monics in A
K	the function field $\mathbb{F}_q(t)$
K_∞	$=\mathbb{F}_q((1/t))=$ the completion of K at ∞
A_d	{elements of A of degree d}
A_{d+}	$A_d\cap A_+$
$[n]$	$=t^{q^n}-t$
'even'	multiple of $q-1$
deg	function assigning to $a\in A$ its degree in t
$\ell(k)$	sum of the digits of the base q expansion of k
$\lfloor x\rfloor$	the largest integer not greater than x
$\lceil x\rceil$	the smallest integer not less than x.

3. Thakur multizeta values

For $s\in\mathbb{Z}_+$, the *Carlitz zeta values* [Gos96,Tha04] are defined as

$$\zeta_A(s):=\sum_{a\in A_+}\frac{1}{a^s}\in K_\infty.$$

For $s\in\mathbb{Z}$ and $d\geqslant 0$, write

$$S_d(s):=\sum_{a\in A_{d+}}\frac{1}{a^s}\in K.$$

Given integers $s_i\in\mathbb{Z}_+$ and $d\geqslant 0$ put

$$S_d(s_1,\dots,s_r)=S_d(s_1)\sum_{d>d_2>\cdots>d_r\geqslant 0}S_{d_2}(s_2)\cdots S_{d_r}(s_r)\in K.$$

For $s_i\in\mathbb{Z}_+$, Thakur defined the *multizeta values* [Tha04,Tha09] by:

$$\zeta(s_1,\ldots,s_r) := \sum_{d_1>\cdots>d_r\geqslant 0} S_{d_1}(s_1)\cdots S_{d_r}(s_r) = \sum \frac{1}{a_1^{s_1}\cdots a_r^{s_r}} \in K_\infty,$$

where the second sum is over all $a_i \in A_+$ of degree d_i such that $d_1 > \cdots > d_r \geqslant 0$. We say that this multizeta value has depth r and weight $\sum s_i$.

4. Relations between multizeta values

Recall that Euler's multizeta values ζ (only in this paragraph, the Greek letter ζ will be used to denote the classical multizeta values) are defined by $\zeta(s_1,\ldots,s_r) = \sum (n_1^{s_1}\cdots n_r^{s_r})^{-1}$, where the sum is over positive integers $n_1 > n_2 > \cdots > n_r$ and s_i are positive integers, with $s_1 > 1$ (this condition is required for convergence). Since $n_1 = n_2$, $n_1 > n_2$ or $n_2 > n_1$, we have the "sum shuffle relation"

$$\begin{aligned}\zeta(a)\zeta(b) &= \sum_{n_1=1}^{\infty}\frac{1}{n_1^a}\sum_{n_2=1}^{\infty}\frac{1}{n_2^b} = \sum_{n_1=n_2}\frac{1}{n_1^{a+b}} + \sum_{n_1>n_2}\frac{1}{n_1^a n_2^b} + \sum_{n_2>n_1}\frac{1}{n_2^b n_1^a}\\ &= \zeta(a+b) + \zeta(a,b) + \zeta(b,a).\end{aligned}$$

In the function field case, this sum shuffle relation fails because there are many polynomials of a given degree. In contrast to the classical sum shuffle, in the function field case the identities we get are much more involved.

For $s_1, s_2 \in \mathbb{Z}_+$ put

$$S_d(s_1,s_2) = \sum_{\substack{d=d_1>d_2\\ a_i\in A_+}} \frac{1}{a_1^{s_1}a_2^{s_2}}$$

where $d_i = \deg(a_i)$. For $a, b \in \mathbb{Z}_+$, we define

$$\Delta_d(a,b) = S_d(a)S_d(b) - S_d(a+b).$$

We write $\Delta(a,b)$ for $\Delta_1(a,b)$. The definition implies $\Delta_d(a,b) = \Delta_d(b,a)$.

The next two theorems (the second theorem in the reference has implications to higher genus function fields, but we state only a special case relevant to us) are due to Thakur [Tha10, Theorems 1, 2].

Theorem 4.1. *Given $a, b \in \mathbb{Z}_+$, there are $f_i \in \mathbb{F}_p$ and $a_i \in \mathbb{Z}_+$, so that*

$$\Delta_d(a,b) = \sum f_i S_d(a_i, a+b-a_i) \tag{4.1.1}$$

holds for $d = 1$.

Theorem 4.2. *Fix A. If (4.1.1) holds for some $f_i \in \mathbb{F}_p^\times$ and distinct $a_i \in \mathbb{Z}_+$ for $d = 1$, then (4.1.1) holds for all $d \geqslant 0$. In this case, we have the shuffle relation*

$$\zeta(a)\zeta(b) - \zeta(a+b) - \zeta(a,b) - \zeta(b,a) = \sum f_i \zeta(a_i, a+b-a_i).$$

5. Main results

In this section we shall prove the recursion part of the main conjecture formulated by Lara [Lar10, Lar09], except the items concerning the initial values.

Let us start with a definition.

Definition 5.1. Let $a \in \mathbb{Z}_+$.

(1) We set

$$r_a = (q-1)p^m,$$

where m is the smallest integer such that $a \leqslant p^m$.

(2) Put

$$\phi(j) := r_a - a - j(q-1).$$

(3) We define

$$j_{a,\max} = \left\lfloor \frac{r_a - a}{q-1} \right\rfloor.$$

(4) Let q be prime. For $0 \leqslant j \leqslant j_{a,\max}$, let $c_{a,j} \in \mathbb{F}_p$ be defined by:

$$c_{a,j} = \begin{cases} 1 & \text{if } j = 0, \\ \lceil \frac{j(q-1)}{j_{a,\max}} \rceil^{-1} \binom{r_a - a}{j(q-1)} & 0 < j \leqslant j_{a,\max}. \end{cases}$$

(5) For each j, $0 \leqslant j \leqslant p-1$, let μ_j be the number of j's in the p expansion of $a-1$. Set

$$t_a = \prod_{j=0}^{p-2} (p-j)^{\mu_j}.$$

Remark 5.2. For q prime and $0 < j \leqslant j_{a,\max}$, $\lceil j(q-1)/j_{a,\max} \rceil$ is not zero in $\mathbb{F}_p$ because $0 < j(q-1)/j_{a,\max} \leqslant q-1 < p$. Therefore, $c_{a,j}$ in Definition 5.1 (4) makes sense. For q non-prime, $c_{a,j}$ is not always defined (e.g., $q=4$, $a=5$, $j=3$).

Let $a, b \in \mathbb{Z}_+$. Let $j \in 0, 1, \ldots, p^m - a$. Since p^m and $q-1$ are coprime, p^m is a unit in $\mathbb{Z}/(q-1)\mathbb{Z}$; so, the equation $j \equiv -ip^m \bmod (q-1)$ has always a solution. There exists exactly one solution in the range $0 \leqslant i < q-1$.

Definition 5.3. Let i_j be the unique integer $0 \leqslant i_j < q-1$ such that $j + i_j p^m \equiv 0 \bmod (q-1)$. Let l_j be the non-negative integer defined by

$$l_j = \frac{j + i_j p^m}{q-1}.$$

In general, the correspondence $j \mapsto i_j$ between $\{0, 1, \ldots, p^m - a\}$ and $0, 1, \ldots, q-2$ is neither injective (e.g., $q=3$, $a=4$) nor surjective (e.g., $q=4$, $a=3$).

J.A. Lara Rodríguez / Journal of Number Theory 131 (2011) 2081–2099 2085

Proposition 5.4. *The map*

$$\begin{aligned}\{0, 1, \ldots, p^m - a\} &\to \{l(q-1) \mid 0 \leqslant l \leqslant j_{a,\max}\},\\ j &\mapsto j + i_j p^m\end{aligned}$$

is injective.

Proof. Since $0 \leqslant j \leqslant p^m - a$ and $0 \leqslant i_j \leqslant q-2$, it follows that $0 \leqslant j + i_j p^m \leqslant p^m - a + p^m(q-2) = r_a - a$. This shows that the map is well defined. If $a = p^m$, then the map is clearly injective. Assume $a < p^m$. If $j_1 + i_{j_1} p^m = j_2 + i_{j_2} p^m$, then $p^m \mid j_1 - j_2$. Since $0 \leqslant j_1, j_2 \leqslant p^m - a < p^m$, we conclude that $j_1 = j_2$. □

When $q = 2$, the map of the above proposition is a bijection, but in general the map is not surjective. For instance, consider $q = 3$ and $a = 2$.

Proposition 5.5. *The following statements hold in* $\mathbb{F}_p$:

a) *If* $0 \leqslant i \leqslant q-1$, *then*

$$\binom{q-1}{i} = (-1)^i. \tag{5.5.1}$$

b) *If* $0 \leqslant i \leqslant p-2$, *then*

$$\binom{p-2}{i} = (-1)^i(i+1).$$

c) *The number of* j*'s,* $0 \leqslant j \leqslant p^m - a$, *such that* $\binom{p^m-a}{j}$ *is not zero modulo* p *is* t_a.

Proof. a) First consider the case $0 \leqslant i \leqslant p-1$. Then, $(p-1)!$, $i!$, and $(p-1-i)!$ are non-zero modulo p; therefore, in $\mathbb{F}_p$, we have

$$\binom{p-1}{i} = \frac{(p-1)(p-2)\cdots(p-i)}{i!} = \frac{(-1)(-2)\cdots(-i)}{i!} = (-1)^i.$$

Thus, (5.5.1) holds in this special case.

For general i, let $i = \sum_{l=0}^{s-1} i_l p^l$ be the base p expansion of i. The base p expansion of $q-1$ is $\sum_{l=0}^{s-1}(p-1)p^l$. Note that $(-1)^{a_l} = (-1)^{a_l p^l}$. By the Lucas theorem, we conclude

$$\binom{q-1}{i} = \prod_{l=0}^{s-1}\binom{p-1}{i_l} = \prod_{l=0}^{s-1}(-1)^{i_l p^l} = (-1)^i.$$

Thus, (5.5.1) holds in the general case.

b) For the second part, we have

$$\binom{p-2}{i} = \frac{(p-2)\cdots(p-2-(i-1))}{i!} = \frac{(-2)\cdots(-(i+1))}{i!} = (-1)^i(i+1).$$

c) Let t'_a be the number of j's in $0, 1, \dots, p^m - a$ such that $\binom{p^m-a}{j} \not\equiv 0 \bmod p$. Let us prove that $t'_a = t_a$. Since $a \leqslant p^m$, then $a - 1 \leqslant p^m - 1 = \sum_{l=0}^{m-1}(p-1)p^l$. Let $a - 1 = \sum_{l=0}^{m-1} a_l p^l$ and $j = \sum_{l=0}^{m-1} b_l p^l$ be the base p expansions of $a-1$ and j, respectively. Since $p^m - 1 - (a-1) = p^m - a$, the base p expansion of $p^m - a$ is $\sum_{l=0}^{m-1}(p-1-a_l)p^l$. By the Lucas theorem,

$$\binom{p^m - a}{j} \equiv \prod_{l=0}^{m-1} \binom{p - 1 - a_l}{b_l} \mod p.$$

Since $\binom{\alpha}{\beta}$ vanishes modulo p if $\beta > \alpha$, by choosing b_l in the set $\{0, 1, \dots, p-1-a_l\}$, we guarantee that $\binom{p^m-a}{j}$ does not vanish modulo p. Therefore,

$$t'_a = \prod_{l=0}^{m-1}(p - a_l) = \prod_{k=0}^{p-2}(p-k)^{\mu_k} = t_a. \qquad \square$$

Proposition 5.6. *Let $q = 2$. Then, $j_{a,\max} = 0$ if and only if $a = p^m$. If $q > 2$, then $j_{a,\max} = 0$ if and only if $a = 1$.*

Proof. This follows by a straight calculation from the definitions. $\square$

Definition 5.7. For each j, $0 \leqslant j \leqslant p^m - a$, let $f_{a,j} \in \mathbb{F}_p$ be defined by

$$f_{a,j} = \binom{p^m - a}{j}(-1)^j.$$

Proposition 5.8. *The number of j's such that $f_{a,j} \neq 0$ is t_a.*

Proof. It follows immediately from Proposition 5.5(c). $\square$

When q is prime, we have another description for $f_{a,j}$ which is consistent with the part 3 of the main conjecture in [Lar10] (see Remark 5.19(1)).

Proposition 5.9. *If q is prime (so that $q = p$), then for $j \in \{1, 2, \dots, p^m - a\}$*

$$f_{a,j} = \left\lceil \frac{j + i_j p^m}{j_{a,\max}} \right\rceil^{-1} \binom{r_a - a}{j + i_j p^m} = c_{a,l_j},$$

where c_{a,l_j} is as defined in Definitions 5.1 and 5.3.

Proof. We claim that (A) $i_j + 1 = \lceil \frac{j + i_j p^m}{j_{a,\max}} \rceil$, which is equivalent to showing

$$i_j j_{a,\max} \leqslant i_j p^m < j + i_j p^m \leqslant (i_j + 1) j_{a,\max}.$$

It is enough to prove the rightmost inequality. To do so, we first compute i_j for $j > 0$, as follows. Write $j = l(q-1) + r$, $0 \leqslant r < q - 1$. If $r > 0$, then

$$j + (q - 1 - r)p^m = \bigl(l + p^m\bigr)(q-1) + r\bigl(1 - p^m\bigr) \equiv 0 \mod (q-1),$$

and $0 < q-1-r < q-1$. If $r=0$, then $j \equiv 0 \bmod (q-1)$. By definition, it follows that $i_j = q-1-r$ if $r>0$ and $i_j = 0$, otherwise. Note $0 \leqslant i_j \leqslant q-2$, so that i_j+1 is non-zero in $\mathbb{F}_p$. Write $a = l'(q-1)+a'$, $0 \leqslant a' < q-1$. Then $j_{a,\max} = p^m - l' - y$, where $y=0$ if $a'=0$ and $y=1$ otherwise. Let us consider first the case $j \not\equiv 1 \bmod (q-1)$. Thus $i_j \neq q-2$. Let $j_0 \in \{2,\dots,p^m-a\} \cap \{2,\dots,q-1\}$ such that $i_j = i_{j_0}$. Then $j_0 = q-u$ for some u, $1 \leqslant u \leqslant q-2$ and $i_{j_0} = u-1$, $0 \leqslant i_{j_0} < q-2$. Then

$$\begin{aligned} j + i_j p^m &\leqslant j_0 + i_{j_0} p^m + (q-1)\left\lfloor \frac{p^m - a + i_j p^m - (j_0 + i_{j_0} p^m)}{q-1} \right\rfloor \\ &= q - u + (u-1)p^m + (q-1)\left\lfloor \frac{p^m - a - j_0}{q-1} \right\rfloor \\ &= q - u + (u-1)p^m + p^m - 1 - l'(q-1) - z(q-1), \end{aligned}$$

where $z=1$ if $0 < (a'+j_0-1)/(q-1) \leqslant 1$ and $z=2$ if $1 < (a'+j_0-1)/(q-1) < 1 + (q-2)/(q-1)$. Since $u \leqslant q-1$, then $l'u \leqslant l'(q-1) \leqslant l'(q-1) + (z-1)(q-1)$. Therefore

$$j + i_j p^m = up^m - u - l'(q-1) - (z-1)(q-1) \leqslant up^m - l'u - yu = (i_j+1) j_{a,\max}.$$

On the other hand, if $j \equiv 1 \bmod (q-1)$, then $i_j + 1 = q-1$. Since $j \leqslant p^m - a$, then $j + i_j p^m \leqslant r_a - a$. Now,

$$\frac{j + i_j p^m}{i_j + 1} = \frac{j + i_j p^m}{q-1} \leqslant \frac{r_a - a}{q-1}.$$

The claim now follows as the left side is an integer.

Let $j = b_0 + b_1 p + \dots + b_{m-1} p^{m-1}$ and $a - 1 = a_0 + a_1 p + \dots + a_{m-1} p^{m-1}$ be the base p expansions of j and $a-1$, respectively. The base p expansion of $p^m(p-1) - 1$ is $\sum_{l=0}^{m-1} (p-1)p^l + (p-2)p^m$. Consequently, the base p expansion of $r_a - a = r_a - 1 - (a-1)$ is $\sum_{l=0}^{m-1} (p-1-a_l)p^l + (p-2)p^m$. Finally, the base p expansion of $j + i_j p^m$ is $\sum_{l=0}^{m-1} b_l p^l + i_j p^m$.

Note $j + i_j \equiv j + i_j p^m \equiv 0 \bmod (q-1)$, so, (B) $(-1)^{i_j} = (-1)^j$. By the Lucas theorem, b) of Proposition 5.5, and (A), (B) respectively, we have

$$\begin{aligned} \binom{r_a - a}{j + i_j p^m} &= \binom{p-1-a_0}{b_0} \cdots \binom{p-1-a_{m-1}}{b_{m-1}} \binom{p-2}{i_j} \\ &= \binom{p^m - a}{j} (-1)^{i_j} (i_j + 1) \\ &= f_{a,j} \left\lceil \frac{j + i_j p^m}{j_{a,\max}} \right\rceil. \qquad \square \end{aligned}$$

Proposition 5.10. *Let q be arbitrary and $a \in \mathbb{Z}_+$. For each $n \in A_{1^+}$, let g_n be defined by*

$$g_n = -\frac{[1]^{p^m - a}}{n^{p^m - a}} [1]^a S_1(a).$$

Then,

$$g_n = 1 + \sum_{j=1}^{p^m - a} f_{a,j} n^{r_a - (j + i_j p^m)}$$

where $f_{a,j}$ is as in Definition 5.7 and i_j is the unique integer, $0 \leqslant i_j < q-1$, such that $j + i_j p^m \equiv 0 \bmod (q-1)$.

Proof. Note

$$-\frac{[1]^{p^m-a}}{n^{p^m-a}} = -\left(n^{q-1}-1\right)^{p^m-a} = \sum_{j_1=0}^{p^m-a}\binom{p^m-a}{j_1}(-1)^{p^m-a-j_1+1}n^{j_1(q-1)}.$$

On the other hand, by specializing [Tha09, 3.3] to $d=1$ we see that

$$S_1(k+1) = \frac{(-1)^{k+1}}{[1]^{k+1}}\left(1+\sum_{k_1=1}^{\lfloor k/q\rfloor}\binom{k-k_1(q-1)}{k_1}(-1)^{k_1}[1]^{k_1(q-1)}\right).$$

Hence,

$$[1]^a S_1(a) = (-1)^a + \sum_{j_2=1}^{n_a}\binom{a-1-j_2(q-1)}{j_2}(-1)^{a+j_2}n^{j_2(q-1)}\left(n^{q-1}-1\right)^{j_2(q-1)},$$

where $n_a = \lfloor (a-1)/q\rfloor$. Since

$$n^{j_1(q-1)}n^{j_2(q-1)}\left(n^{q-1}-1\right)^{j_2(q-1)} = \sum_{j_3=0}^{j_2(q-1)}\binom{j_2(q-1)}{j_3}(-1)^{j_2(q-1)-j_3}n^{(j_1+j_2+j_3)(q-1)},$$

we see that $g_n = -(n^{q-1}-1)^{p^m-a}[1]^a S_1(a) \in \mathbb{F}_p[n]$. Note that all powers of n involved are 'even'. If $n = t-\theta$ for some $\theta \in \mathbb{F}_q$, then $g_n(t+\theta) = g_t$. If $g_n = \sum_j c_{n,j}n^{j(q-1)}$, it follows that $c_{n,j} = c_{t,j}$ for all j. Now it suffices to compute $c_{t,j}$. To do so let us put $h_\theta = (t-\theta)^{p^m-a}((t-\theta)^{q-1}-1)^{p^m}$, $\theta \in \mathbb{F}_q^*$. Then,

$$\begin{aligned}
h_\theta &= \sum_{j=0}^{p^m-a}\binom{p^m-a}{j}t^{p^m-a-j}\theta^j(-1)^j\left(\sum_{i=0}^{q-1}\binom{q-1}{i}^{p^m}t^{p^m(q-1-i)}\theta^{ip^m}(-1)^i - 1\right)\\
&= \sum_{j=0}^{p^m-a} f_{a,j}t^{p^m-a-j}\left(\sum_{i=0}^{q-1}t^{p^m(q-1-i)}\theta^{j+ip^m} - \theta^j\right).
\end{aligned}$$

Hence,

$$\begin{aligned}
\sum_{\theta\in\mathbb{F}_q^*} h_\theta &= \sum_{j=0}^{p^m-a} f_{a,j}t^{p^m-a-j}\left(\sum_{i=0}^{q-1}t^{p^m(q-1-i)}\sum_{\theta\in\mathbb{F}_q^*}\theta^{j+ip^m} - \sum_{\theta\in\mathbb{F}_q^*}\theta^j\right)\\
&= \sum_{j=0}^{p^m-a} f_{a,j}t^{p^m-a-j}\left(\sum_{i=0}^{q-2}t^{p^m(q-1-i)}\sum_{\theta\in\mathbb{F}_q^*}\theta^{j+ip^m}\right)\\
&= \sum_{j=0}^{p^m-a} f_{a,j}t^{p^m-a-j}\left(t^{p^m(q-1-i_j)}(-1)\right)\\
&= -\sum_{j=0}^{p^m-a} f_{a,j}t^{r_a-a-(j+i_jp^m)+p^m}.
\end{aligned}$$

Here, we used that $\sum_{\theta\in\mathbb{F}_q^*}\theta^l$ is 0 if $q-1$ does not divide l, and -1 if $l\geqslant 0$ is divisible by $q-1$. Now,

$$[1]^{p^m}S_1(a)=\sum_{n\in A_{1+}}\frac{[1]^{p^m}}{n^a}=\sum_{n\in A_{1+}}n^{p^m-a}\big(n^{q-1}-1\big)^{p^m}=t^{p^m-a}\big(t^{r_a}-1\big)+\sum_{\theta\in\mathbb{F}_q^*}h_\theta.$$

It follows that

$$g_t=-t^{r_a}+1+\sum_{j=0}^{p^m-a}f_{a,j}t^{r_a-(j+i_jp^m)}=1+\sum_{j=1}^{p^m-a}f_{a,j}t^{r_a-(j+i_jp^m)}. \qquad \square$$

Example 5.11. Let $q=9$ and $a=17$. Then, $m=3$ and $r_a=27(8)=216$. Since $a-1=1+2p+p^2$, $t_a=3^02^2=4$. The j's for which $f_{a,j}\neq 0$ are 0, 1, 9, and 10. Using that $0\mapsto 0$, $1\mapsto 5$, $9\mapsto 5$, and $10\mapsto 2$, we have

$$g_t=1+f_{a,1}t^{216-136}+f_{a,9}t^{216-144}+f_{a,10}t^{216-64}=1+2t^{80}+2t^{72}+t^{152}.$$

Definition 5.12. Let q be arbitrary. For $a,b\in\mathbb{Z}_+$, let $S(a,b)$ denote the pairs (f_i,a_i) such (4.1.1) holds for $d=1$.

The following theorem proves parts 1 and 7 of the main Conjecture 1.5 in [Lar10], and is more precise in that it gives a complete recipe for general q.

Theorem 5.13. *Let $a,b\in\mathbb{Z}_+$. Let r_a, i_j, $f_{a,j}$ be as in Definitions* 5.1, 5.3, 5.7. *Then*

$$\Delta(a,b+r_a)-\Delta(a,b)=\sum_{j=0}^{p^m-a}f_{a,j}S_1\big(a+b+\big(j+i_jp^m\big)\big).$$

In particular, the sets $S(a,b)$ can be found recursively with recursion length r_a, by

$$S(a,b+r_a)=S(a,b)\cup T(a,b+r_a),$$

where

$$T(a,b+r_a)=\big\{\big(f_{a,j},a+b+\big(j+i_jp^m\big)\big)\;\big|\;0\leqslant j\leqslant p^m-a,\ f_{a,j}\neq 0\big\},$$

or equivalently,

$$T(a,b+r_a)=\big\{\big(f_{a,j},b+r_a-\phi(l_j)\big)\;\big|\;0\leqslant j\leqslant p^m-a,\ f_{a,j}\neq 0\big\},$$

where $\phi(l_j)=r_a-a-l_j(q-1)$.

The set $T(a,b+r_a)$ is a set of size t_a.

Proof. By definition of $\Delta(a,b+r_a)$, it follows that

$$\Delta(a,b+r_a)=\sum_{\substack{n_1\neq n_2\\ n_1,n_2\in A_{1+}}}\frac{1}{n_1^an_2^{b+r_a}}=\sum_{n_2\in A_{1+}}\frac{1}{n_2^{b+r_a}}\left(S_1(a)-\frac{1}{n_2^a}\right).$$

By Proposition 5.10, for any $n \in A_{1^+}$, we have $g_n = 1 + \sum_{j=1}^{p^m-a} f_{a,j} n^{r_a-(j+i_j p^m)}$. Let $\Sigma = \sum_{j=1}^{p^m-a} f_{a,j} \times S_1(b + r_a - \phi(l_j))$. Then,

$$\Sigma = \sum_{n_2 \in A_{1+}} \sum_{j=1}^{p^m-a} \frac{f_{a,j}}{n_2^{b+r_a-(r_a-a+(j+i_j p^m))}} = \sum_{n_2 \in A_{1+}} \frac{1}{n_2^{b+r_a}} \frac{1}{n_2^a} \sum_{j=1}^{p^m-a} f_{a,j} n_2^{r_a-(j+i_j p^m)}.$$

Using this leads to

$$\begin{aligned}
\Delta(a, b + r_a) - \Sigma &= \sum_{n_2 \in A_{1+}} \frac{S_1(a)}{n_2^{b+r_a}} \left(1 - \frac{1}{S_1(a) n_2^a} \left(1 + \sum_{j=1}^{p^m-a} f_{a,j} n_2^{r_a-(j+i_j p^m)}\right)\right) \\
&= \sum_{n_2 \in A_{1+}} \frac{S_1(a)}{n_2^{b+r_a}} \left(1 - \frac{1}{S_1(a) n_2^a} g_{n_2}\right) \\
&= \sum_{n_2 \in A_{1+}} \frac{S_1(a)}{n_2^{b+r_a}} \left(1 + \frac{[1]}{n_2}\right)^{p^m} \\
&= \sum_{n_2 \in A_{1+}} \frac{S_1(a)}{n_2^{b+r_a}} \left(n_2^{q-1}\right)^{p^m} \\
&= S_1(a) S_1(b).
\end{aligned}$$

Therefore, $\Delta(a, b + r_a) - S_1(a) S_1(b) = \Sigma$. From this, we get

$$\begin{aligned}
\Delta(a, b + r_a) - \Delta(a, b) &= \Sigma + S_1(a + b) \\
&= \sum_{j=1}^{p^m-a} f_{a,j} S_1\big(b + r_a - \phi(l_j)\big) + S_1\big(b + r_a - \phi(0)\big) \\
&= \sum_{j=0}^{p^m-a} f_{a,j} S_1\big(b + r_a - \phi(l_j)\big).
\end{aligned}$$

This shows that $T(a, b+r_a)$ is exactly as claimed. By Proposition 5.8 it follows that the size of $T(a, b+r_a)$ is precisely t_a. □

Remark 5.14.

(1) The set T_a of pairs $(f_{a,j}, \phi(l_j))$ with $f_{a,j} \neq 0$ clearly is independent of b as predicted in Conjecture 1.5(1c) in [Lar10], which did not have precise description for it as above.
(2) The number of terms t_a to be added at each step of the recursion depends on q only through p.

Examples 5.15 *(Special large indices).* (See [Tha09, p. 2338].) Let $q = 2$.

(1) Let $a = 2^n - 1$. Then, $m = n$ and $a - 1 = 2 + \cdots + 2^{n-1}$. There is only one zero in the base 2 expansion of $a - 1$. Thus, $t_a = (2 - 0)^1 = 2$. At each step of recursion, two terms must be added. Furthermore, $T_a = \{(1, r_a - a), (1, r_a - a - 1)\}$ because in this case $l_j = j$ for $j = 0, 1$.

(2) For $a = 2^n + 1$, 2^n top terms are added. Then, $m = n + 1$. The base 2 expansion of $a - 1$ has n zeros and so $t_a = 2^n$. As before, for any j, $0 \leqslant j \leqslant 2^n - 1$, $i_j = 0$, and $l_j = j$. Thus, $T_a = \{(1, r_a - a - j) \mid 0 \leqslant j \leqslant 2^n - 1\}$.

Example 5.16. (See Example in [Tha09, p. 2337].) Let $q = 2$ and $a = 19$. Then, $m = 5$, $t_{19} = 8$, and $r_{19} = 32$. In this case, $i_j = 0$, and $l_j = j$ for all j. The j's for which $f_{19,j} \neq 0$ are 0, 1, 4, 5, 8, 9, 12, and 13. The polynomial g_t is $g_t = 1 + t^{31} + t^{28} + t^{27} + t^{24} + t^{23} + t^{20} + t^{19}$. Therefore,

$$\begin{aligned}
\Delta(19, b + 32) - \Delta(19, b) &= \sum_{j=0}^{13} f_{19,j} S_1(19 + b + j) \\
&= S_1(b + 19) + S_1(b + 20) + S_1(b + 23) + S_1(b + 24) \\
&\quad + S_1(b + 27) + S_1(b + 28) + S_1(b + 31) + S_1(b + 32).
\end{aligned}$$

The following corollary proves parts 2, 5, and 6 of the main conjecture in [Lar10].

Corollary 5.17. *Let notations be the same as before.*

a) $(1, \phi(0)) = (1, r_a - a) \in T_a$.
b) $T_a = \{(1, \phi(0))\}$ *if and only if* $a = p^m$.
c) *If* $a' = p^{m'} a$, *then*

$$T_{a'} = \{(f_{a,j}, p^{m'} \phi(l_j)) \mid 0 \leqslant j \leqslant p^m - a,\ f_{a,j} \neq 0\}.$$

d) *If* q *is prime,*

$$T_a = \{(c_{a,l_j}, \phi(l_j)) \mid 0 \leqslant j \leqslant p^m - a,\ f_{a,j} \neq 0\}.$$

Proof. To prove a), just note that $f_{a,0} = 1$.

b) When $a = p^m$, then $g_n = 1$ and, thus, $T_a = \{(1, r_a - a)\}$. Conversely, since $t_a = 1$, by definition of t_a, it follows that $a - 1 = \sum_{i=0}^{m-1} (p-1)p^i = p^m - 1$.

c) Let $a' = p^{m'} a$ for some integer $m' \in \mathbb{Z}_+$. Then, $m + m'$ is the smallest integer such that $a' \leqslant p^{m+m'}$. We have

$$\begin{aligned}
-\frac{[1]^{p^{m+m'}}}{n^{p^{m+m'}-a'}} S_1(a') &= \left(-\frac{[1]^{p^m}}{n^{p^m-a}} S_1(a)\right)^{p^{m'}} \\
&= (g_n)^{p^{m'}} \\
&= \left(1 + \sum_{j=1}^{p^m-a} f_{a,j} n^{r_a-(j+i_j p^m)}\right)^{p^{m'}} \\
&= 1 + \sum_{j=1} f_{a,j}^{p^{m'}} n^{p^{m'}(r_a-(j+i_j p^m))} \\
&= 1 + \sum_{j=1} f_{a,j} n^{p^{m'}(r_a-(j+i_j p^m))}.
\end{aligned}$$

d) If q is prime, by Proposition 5.9 $f_{a,j} = c_{a,l_j}$ follows. $\square$

Proposition 5.18. *If $\binom{r_a-a}{l(q-1)} \neq 0$ in $\mathbb{F}_p$ for some l, $0 \leqslant l \leqslant j_{a,\max}$, then there exists j, $0 \leqslant j \leqslant p^m - a$, such that $l(q-1) = j + i_j p^m$ and $\binom{p^m-a}{j} \neq 0$.*

Proof. Writing the base p expansion of $a-1$ as $\sum a_k p^k$ as before, we have

$$r_a - a = p^m - a + p^m(q-2) = \sum_{k=0}^{m-1}(p-1-a_k)p^k + (p-2)p^m + \sum_{k=m+1}^{m+s-1}(p-1)p^k.$$

Let $l(q-1) = \sum_{k=0}^{m+s-1} b_k p^k$ be the base p expansion of $l(q-1)$. Since $\binom{r_a-a}{l(q-1)} \neq 0$, by the Lucas theorem, we have $\binom{p-1-a_k}{b_k} \neq 0$ for $k = 0, 1, \ldots, m-1$ and $\binom{p-2}{b_m} \neq 0$. Therefore, $b_k \leqslant p-1-a_k$ for $k = 0, 1, \ldots, m-1$ and $b_m \leqslant p-2$. Let $j = \sum_{k=0}^{m-1} b_k p^k$ and $i = \sum_{k=0}^{s-1} b_{m+k} p^k$. Thus, $0 \leqslant j \leqslant p^m - a$ and $0 \leqslant i \leqslant q-2$. Since $j + ip^m = l(q-1) \equiv 0 \bmod (q-1)$, we have $i = i_j$. It follows that $\binom{p^m-a}{j} \neq 0$. $\square$

Remark 5.19.

(1) This proposition proves part 3 of the main conjecture in [Lar10]: If there is no carry over base p in the sum of $l(q-1)$ and $\phi(l)$, then $\binom{r_a-a}{l(q-1)} \neq 0$ and, so, by Proposition 5.18 and Theorem 5.13, $(f_{a,j}, \phi(l_j))$ belongs to T_a.

(2) By Proposition 5.9, if q is prime, $f_{a,j} \neq 0$ if and only if $\binom{r_a-a}{l_j(q-1)} \neq 0$. If q is not prime, we could have $\binom{p^m-a}{j} \neq 0$ and $\binom{r_a-a}{l_j(q-1)} = 0$ (e.g., $q = 4$, $a = 5$, $j = 1$).

Example 5.20. (See [Tha09, Theorems 3 and 7].) We give another proof of Theorems 3 and 7 in [Tha09] using Theorem 5.13. Let $q = 2$.

a) Let $a = 1$. Then $m = 0$, $r_1 = 1$, $g_t = 1$, and $t_1 = 1$. By Theorem 5.13, we have $\Delta(1, b+1) - \Delta(1, b) = S_1(1+b)$. Then, $\Delta(1,2) = \Delta(1,1) + S_1(2) = S_1(2)$. By repeating this process, we get $\Delta(1,3) = \Delta(1,2) + S_1(3) = S_1(2) + S_1(3)$. It follows that $\Delta(1,b) = \sum_{i=2}^{b} S_1(i)$. Therefore, we get

$$\zeta(1)\zeta(b) = \zeta(1+b) + \sum_{i=1}^{b-1} \zeta(i, b+1-i).$$

b) Now let $a = 2$. Then $r_2 = 2$, $g_t = 1$, and $t_2 = 1$. Since $\Delta(2,1) = S_1(2)$ and $\Delta(2,2) = 0$, proceeding as in part a), it follows that

$$\Delta(2,b) = \begin{cases} \sum_{i=1}^{(b-1)/2} S_1(2i+1) + S_1(2) & \text{if } b \text{ is odd,} \\ \sum_{i=2}^{b/2} S_1(2i) & \text{if } b \text{ is even.} \end{cases}$$

6. Closed formulas

Let $a, b \in \mathbb{Z}_+$. By Theorem 4.1, there are $f_i \in \mathbb{F}_p$ and $a_i \in \mathbb{Z}_+$ so that $\Delta(a,b) = \sum_{i=0}^{\delta} f_i S_1(a_i)$. From this, we get the partial fraction decomposition of $\Delta(a,b)$:

$$\Delta(a,b) = \sum_{\mu \in \mathbb{F}_q} \frac{h_\mu(t)}{(t-\mu)^n}, \tag{6.0.1}$$

where $h_\mu(t) = f_0 + f_1(t-\mu)^{a_0-a_1} + \cdots + f_{a_\delta}(t-\mu)^{a_0-a_\delta}$ (we assume that $n = a_0 > a_1 > \cdots > a_\delta$). Uniqueness of the partial fraction decomposition guarantees uniqueness of f_i's.

Conversely, since the denominator of $\Delta(a,b)$ is a power of [1], its partial fraction decomposition is of the form (6.0.1), where $h_\mu(t) \in \mathbb{F}_q[t]$ is relatively prime to $t-\mu$; also, $\deg h_\mu < n$. Now, $\Delta(a,b)$ is invariant with respect to the automorphisms $t \to t+\theta$, $\theta \in \mathbb{F}_q$ of A. By the uniqueness of the partial fraction decomposition, we have $h_0(t) = h_\theta(t+\theta)$ for any $\theta \in \mathbb{F}_q$. Let $h_0(t) = f_0 + f_1 t + \cdots + f_{n-1}t^{n-1}$. Then,

$$\Delta(a,b) = \sum_{\mu\in\mathbb{F}_q} \frac{h_0(t-\mu)}{(t-\mu)^n} = \sum_{i=0}^{n-1} f_i \sum_{\mu\in\mathbb{F}_q} \frac{1}{(t-\mu)^i} = \sum_{i=0}^{n-1} f_i S_1(n-i).$$

By the uniqueness of f_i's and by Theorem 4.1, it follows that $f_i \in \mathbb{F}_p$.

We proceed as follows to find $h_0(t)$. Since $[1]^n/t^n$ is a unit modulo t^n, it follows from (6.0.1) that modulo t^n, we have $[1]^n\Delta(a,b) = \frac{[1]^n}{t^n}h_0(t)$, so that $h_0(t) \bmod t^n = ([1]^n\Delta(a,b) \bmod t^n)(\frac{[1]^n}{t^n} \bmod t^n)^{-1}$. To finish, we pick the unique representative of $h_0(t) \bmod t^n$ of degree less than n.

We first explain the case $q=2$, when we can simplify a lot to get a nice expression, before giving the general case. When $a=b$, we know that $\Delta(a,b)=0$ [Tha09a, Theorem 8]. Since $S(a,b)=S(b,a)$, we can assume, without loss of generality, that $a>b$.

Theorem 6.1. *Let $q=2$. If $a>b\geqslant 1$, then*

$$\Delta(a,b) = \sum_{k=0}^{a-1} f_k S_1(a-k) \quad \textit{where } f_k = \sum_{\substack{i+j=k \\ i\leqslant 2^m-a \\ j\leqslant a-b-1}} \binom{2^m-a}{i}\binom{a-b}{j}.$$

In particular,

$$S(a,b) = \bigl\{(f_k, a-k) \bigm| f_k \neq 0,\ 0\leqslant k\leqslant a-1\bigr\}.$$

Proof. Since $a>b$,

$$\Delta(a,b) = \frac{1}{t^a(t+1)^b} + \frac{1}{(t+1)^a t^b} = \frac{(t+1)^{a-b}+t^{a-b}}{t^a(t+1)^a} = \frac{S_1(b-a)}{[1]^a}.$$

The degree of the numerator of $\Delta(a,b)$ is less than $a-b$ and, thus, less than the degree of the denominator. Next, we apply the method explained above to write $\Delta(a,b)$ as a sum $\frac{h_0(t)}{t^a} + \frac{h_0(t-1)}{(t-1)^a}$. Since $(t+1)^{2^m-a}(t+1)^a \equiv 1 \bmod t^a$ we have that $(t+1)^{2^m-a} \bmod t^a$ is the inverse of $(t+1)^a \bmod t^a$. Then, $h_0(t) \bmod t^a = (t+1)^{2^m-a}S_1(b-a) \bmod t^a$. The only representative of degree less than a of $(t+1)^{2^m-a} \bmod t^a$ is $(t+1)^{2^m-a}$ because $a > 2^{m-1}$. The only representative of degree less than a of $S_1(b-a) \bmod t^a$ is $S_1(b-a)$. Now,

$$(t+1)^{2^m-a} = \sum_{i=0}^{2^m-a} \binom{2^m-a}{i} t^i,$$

$$S_1(b-a) = t^{a-b} + (t+1)^{a-b} = \sum_{j=0}^{a-b-1} \binom{a-b}{j} t^j.$$

The degree of $(t+1)^{2^m-a}S_1(b-a)$ is at most 2^m-b-1. By taking as $h_0(t)$ the remainder of $(t+1)^{2^m-a}S_1(b-a)$ when divided by t^a the theorem follows. $\square$

Remark 6.2.

(1) If $b \geqslant 2^m - a$, then $2^m - b - 1 < a$ and, therefore, it is not necessary to divide by t^a.
(2) If $k = 0$, then $i = j = 0$ and $f_0 = \binom{2^m-a}{0}\binom{a-b}{0} = 1$.

Now we make the recipe in Theorem 4.1 explicit by giving a closed formula for f_i there.

Theorem 6.3. *Let q be arbitrary. Let $a, b \in \mathbb{Z}_+$ such that $a \geqslant b \geqslant 1$; let m the smallest integer such that $a \leqslant p^m$. Then*

$$\Delta(a,b) = \sum_{i=0}^{a-1} f_i S_1(a-i), \tag{6.3.1}$$

where $f(t) := f_0 + \cdots + f_{a-1}t^{a-1} \in \mathbb{F}_p[t]$ is given by

$$-\left(t^{q-1}-1\right)^{p^m-a} \sum_{\theta\in\mathbb{F}_q} \sum_{\mu\in\mathbb{F}_q^*} \left(\sum_{j=1}^{q-1} \mu^{q-1-j}(t+\theta)^{j-1}\right)^a (t+\theta-\mu)^{a-b} \mod t^a.$$

Equivalently, $f(t)$ is given by

$$\begin{aligned} &\sum_{i_3=0}^{p^m-a} \sum_k \sum_{i_1=0}^{a-b} \sum_{i_2=0}^{\sigma(k)+i_1-1} \binom{p^m-a}{i_3} \binom{a}{k_1,\ldots,k_{q-1}} \binom{a-b}{i_1} \\ &\quad \times \binom{\sigma(k)+i_1}{i_2} (-1)^{b+i_1+i_3} t^{i_2+i_3(q-1)}, \end{aligned} \tag{6.3.2}$$

where the second sum extends over all $(q-1)$-tuples $k = (k_1, \ldots, k_{q-1})$ of non-negative integers such that $k_1 + \cdots + k_{q-1} = a$; $\sigma(k) := \sum_{j=2}^{q-1}(j-1)k_j$; $\tau(k) := \sum_{j=1}^{q-2}(q-1-j)k_j$; and i_1, i_2, i_3 are subjected to $\sigma(k) + i_1 - i_2$, $\tau(k) + a - b - i_1$ being both 'even', and $i_2 + i_3(q-1) < a$.

Proof. The proof method is the same as the one of Theorem 6.1, but with more combinatorial complications as we deal with any q. We now sketch the steps, omitting the routine calculations. First, the inverse modulo t^a of $[1]^a/t^a$ is $-(t^{q-1}-1)^{p^m-a}$ responsible for the first binomial coefficient. Let $\theta, \mu \in \mathbb{F}_q$, with $\mu \neq 0$. Then raising

$$\begin{aligned} \frac{[1]}{(t+\theta)(t+\theta-\mu)} = \frac{(t+\theta-\mu)^{q-1}-1}{t+\theta} &= \sum_{j=1}^{q-1} \binom{q-1}{j} (t+\theta)^{j-1}(-\mu)^{q-1-j} \\ &= \sum_{j=1}^{q-1} \mu^{q-1-j}(t+\theta)^{j-1}, \end{aligned}$$

to the a-th power by the multinomial theorem brings in $\tau(k), \sigma(k)$, the multinomial coefficient; whereas the multiplication by $(t+\theta-\mu)^{a-b}$ the next binomial coefficient, and also $(t+\theta)^{\sigma(k)+i_1}$ bringing in the last binomial coefficient. Finally, we sum over θ and μ and use the fact that $\sum_{\xi\in\mathbb{F}_q^*} \xi^\ell$ is -1 or 0 as ℓ is 'even' or not, accounting for the conditions. $\square$

Corollary 6.4. *The i's in Eq. (6.3.1) are such that $b + i$ is 'even'.*

Proof. Each i is of the form $i_2 + i_3(q-1)$. Since both $\sum_{j=1}^{q-1}(j-1)k_j + i_1 - i_2$ and $\sum_{j=1}^{q-1}(q-1-j)k_j + a - b - i_1$ are 'even', and $\sum_{j=1}^{q-1}(j-1)k_j + \sum_{j=1}^{q-1}(q-1-j)k_j + a = a(q-1)$, it follows that $a(q-1) - (b+i_2)$ is 'even'. Then, $b + i_2$ is 'even', too. Therefore, $b + i = b + i_2 + i_3(q-1)$ is 'even'. $\square$

Remark 6.5.

(1) Corollary 6.4 proves the parity conjecture of Thakur [Tha09, 5.3]. We have already proved the parity conjecture by a different method [Lar].
(2) When $q = 2$, in Eq. (6.3.2) instead of fours sums and four multinomial coefficients, we have two sums and two binomial coefficients and we reduce to formula for $q = 2$.
(3) By the Lucas theorem the multinomial coefficient or the binomial coefficients in (6.3.2) are zero if there is carry over base p in the corresponding sum. So only terms where there is no carry over base p (in the corresponding sums) need to be considered. Similarly, the other conditions and vanishings of binomial coefficients reduce the number of terms in the sum a lot.

Example 6.6. (See [Tha09, Both indices large, p. 2338].) We use Theorem 6.1 to prove two conjectures due to Thakur. Let $q = 2$.

a) Let $a = 2^n + 1$ and $b = 2^n - 1$. Then,

$$\Delta_d(a,b) = \sum_{k=2}^{2^n+1} S_d\bigl(k, 2^n + 1 - k\bigr).$$

b) Let $a = 2^n + 1$ and $b = 2^{n-1}$. Then,

$$\Delta_d(a,b) = S_d(a,b) + \sum_{i=k}^{2^{n-1}+1} S_d\bigl(k, 3 \cdot 2^{n-1} + 1 - k\bigr).$$

Proof. It is enough to prove the case $d = 1$ as it is established in Theorem 4.1.

a) In this case, $m = n + 1$, $p^m - a = 2^n - 1$, and $a - b - 1 = 1$. Then, $f_k = 1$ for $k = 1, \ldots, 2^n - 1$ and $f_{a-1} = 0$ for $k = a - 1 = 2^n$. By Theorem 6.1,

$$\Delta\bigl(2^n + 1, 2^n - 1\bigr) = \sum_{k=0}^{2^n-1} S_1\bigl(2^n + 1 - k\bigr).$$

b) Now, $m = n + 1$, $p^m - a = 2^n - 1$, and $a - b = 2^{n-1} + 1$. Looking at the base 2 expansions of j and $2^{n-1} + 1$ and using the Lucas theorem, we see that the values of j, $0 \leqslant j \leqslant 2^{n-1}$, such that $\binom{2^{n-1}+1}{j} \neq 0$ are $j = 0, 1, 2^{n-1}$. On the other hand, $\binom{2^n-1}{i} \neq 0$ for $i = 0, 1, \ldots, 2^n - 1$. We already know that $f_0 = 1$. For $1 \leqslant k \leqslant 2^n - 1$, we have

$$f_k = \binom{2^n-1}{k}\binom{2^{n-1}+1}{0} + \binom{2^n-1}{k-1}\binom{2^{n-1}+1}{1} + \binom{2^n-1}{k-2^{n-1}}\binom{2^{n-1}+1}{2^{n-1}}.$$

Therefore, $f_k = 0$ for $1 \leqslant k < 2^{n-1}$ and $f_k = 1$ for $2^{n-1} \leqslant k \leqslant 2^n - 1$. For $k = a - 1 = 2^n$,

$$f_k = \binom{2^n-1}{k-1}\binom{2^{n-1}+1}{1} + \binom{2^n-1}{k-2^{n-1}}\binom{2^{n-1}+1}{2^{n-1}} = 0.$$

2096 J.A. Lara Rodríguez / Journal of Number Theory 131 (2011) 2081–2099

It follows that $S(a,b) = \{(f_0, a-0)\} \cup \{(f_k, a-k) \mid 2^{n-1} \leqslant k \leqslant 2^n - 1\}$. Then

$$\Delta(a,b) = S_1\bigl(2^n+1\bigr) + \sum_{k=2^{n-1}}^{2^n-1} S_1\bigl(2^n+1-k\bigr). \qquad \square$$

The following corollary gives special cases of Theorem 6.1.

Corollary 6.7. *Let $q = 2$.*

a) *If $a = 2^m$ and $b < 2^m$, then*

$$\Delta(2^m, b) = \sum_{k=0}^{2^m-b-1} \binom{2^m-b}{k} S_1(a-k).$$

$\binom{2^m-b}{k} \neq 0$ *if there is no carry over base 2 in the sum of k and $b-1$.*

b) *If $b = a-1$, then*

$$\Delta(a, a-1) = \sum_{k=0}^{2^m-a} \binom{2^m-a}{k} S_1(a-k).$$

The number of non-zero coefficients is t_a.

Proof. a) If $a = 2^m$, then $i = 0$ and $\binom{2^m-a}{0} = 1$. Thus, $f_k = \binom{2^m-b}{k}$ for $0 \leqslant k \leqslant 2^m - b - 1$. Let $b-1 = b_0 + b_1 2 + \cdots + b_{m-1}2^{m-1}$ and $k = k_0 + k_1 2 + \cdots + k_{m-1}2^{m-1}$ be the base p expansions of $b-1$ and k, respectively. Then the base 2 expansion of $2^m - b$ is $\sum (1-b_l)p^l$. If $k \leqslant 2^m - b - 1$ and there is no carry over base 2 in the sum of k and $b-1$, then $f_k \neq 0$ because of the Lucas theorem.

b) If $b = a-1$, then $a-b-1 = 0$ and, so, $j = 0$. Therefore, $f_k = \binom{2^m-a}{k}$ for $0 \leqslant k \leqslant 2^m - a$. In this special case, the number of $f_k \neq 0$ is t_a because of Proposition 5.5(c). $\square$

Example 6.8. We use the corollary to prove the following conjectures for $q = 2$ [Tha09, Section 4.1.3]:

$$\Delta_d\bigl(2^n, 2^n-1\bigr) = S_d\bigl(2^n, 2^n-1\bigr) \tag{6.8.1}$$

$$\Delta_d\bigl(2^n+1, 2^n\bigr) = \sum_{i=2}^{2^n+1} S_d\bigl(i, 2^{n+1}+1-i\bigr). \tag{6.8.2}$$

When $l < n-1$,

$$\Delta_d\bigl(2^n-2^l, 2^n-2^l-1\bigr) = S_d\bigl(2^n-2^l, 2^n-2^l-1\bigr) + S_d\bigl(2^n-2^{l+1}, 2^n-1\bigr). \tag{6.8.3}$$

In all cases, it is enough to prove for $d = 1$. Conjecture (6.8.1) follows immediately either from a) or b) of Corollary 6.7, taking $a = 2^n$ and $b = a-1$. For Conjecture (6.8.2), take $a = 2^n+1$ and $b = 2^n$. Then $m = n+1$. By Proposition 5.9(b), we have $\binom{2^n-1}{k} = 1$ for $k = 0, 1, \ldots, 2^n-1$; so,

$$\Delta\bigl(2^n+1, 2^n\bigr) = \sum_{k=0}^{2^n-1} S_1\bigl(2^n+1-k\bigr) = \sum_{k=2}^{2^n+1} S_1(k).$$

Finally, for Conjecture (6.8.3), let $a = 2^n - 2^l$ and $b = a - 1$. Then, $m = n$, $p^m - a = 2^l$ and, thus,

$$\begin{aligned}\Delta(a,b) &= \sum_{k=0}^{2^l} \binom{2^l}{k} S_1(a-k)\\ &= S_1\big(2^n - 2^l\big) + S_1\big(2^n - 2^l - 2^l\big) + \sum_{k=1}^{2^l-1} \binom{2^l}{k} S_1(a-k).\end{aligned}$$

The 2-adic valuation of $\binom{2^l}{k}$ is $\ell(k) + \ell(2^l - k) - \ell(2^l)$, where $\ell(k)$ is the sum of the digits of k base $q = 2$. Since $k \neq 0$ and $2^l - k \neq 0$, we have that $\ell(k) + \ell(2^l - k) - \ell(2^l) \geqslant 1 + 1 - 1 = 1$ and $\binom{2^l}{k} = 0$ for $k = 1, \dots, 2^l - 1$ and the result follows.

Example 6.9. (See [Lar10, Conjecture 2.8.1].) Now we prove that

$$\Delta_d\big(q^n, q^n - 1\big) = -S_d\big(q^n\big), \tag{6.9.1}$$

for any q, which is a generalization of (6.8.1). In [Lar], we have already proved (6.9.1). Here, we prove it again, as a corollary of Theorem 6.3. By Theorem 4.2, it is enough to prove the case $d = 1$. Let $a = q^n$, $b = a - 1$, and $N = 1 + (q-2)q^n$. Then, $p^m - a = 0$, and the polynomial $f(t)$ of Theorem 6.3 becomes

$$\sum_{\theta\in\mathbb{F}_q} (t+\theta)^N = -1 - \sum_{0<l<\frac{N}{q-1}} \binom{N}{l(q-1)} t^{N-l(q-1)}\theta^l.$$

Taking a as $q^n - 1$ in Proposition 5.18, it follows that $\binom{N}{l(q-1)} = 0$ for $0 < l < N/(q-1)$. Also, it is easy to see that the result follows from the comparison of the coefficients of x^j in the identity $(1+x)^N = (1+x)(1+x^{q^n})^{q-2}$, which is valid over $\mathbb{F}_q$ (the author thanks the referee for pointing this out).

Example 6.10. We continue with Example 5.16. Let us evaluate $S(19,20)$. Let $a = 20$ and $b = 19$. Then $m = 5$ and $a - b - 1 = 0$. Therefore, $f_k = \binom{12}{k}$ for $k = 0, 1, \dots, 12$. The k's for which $f_k \neq 0$ are $0, 4, 8$ and 12. Then $S(19,20) = S(20,19) = \{(1,20), (1,16), (1,12), (1,8)\}$. The size of $S(19,20)$ is $4 = t_{20}$.

7. Symmetric closed formulas

In this section we give a symmetric closed formula for the f_i in Theorem 4.1.

Theorem 7.1. *Let q be arbitrary. Let $a, b \in \mathbb{Z}_+$; let m be the smallest integer such that $a + b \leqslant p^m$. Then*

$$\Delta(a,b) = \sum_{i=0}^{b-1} f_i S_1(b-i) + \sum_{j=0}^{a-1} g_j S_1(a-j),$$

where $f(t) = H_{a,b}(t) = f_0 + f_1 t + \dots + f_{b-1}t^{b-1}$, $g(t) = H_{b,a}(t) = g_0 + g_1 t + \dots + g_{a-1}t^{a-1}$, $H_{a,b}(t)$ is given by

$$H_{a,b}(t) = \frac{1}{t^a}\left(-\big(t^{q-1}-1\big)^{p^m-a} \sum_{\theta\in\mathbb{F}_q^*} \big((t+\theta)^{q-1}-1\big)^a \bmod t^{a+b}\right),$$

and $H_{b,a}$ is obtained interchanging a and b. Equivalently,

$$H_{a,b}(t) = \sum_{j=0}^{p^m-a} \sum_{k} \binom{p^m-a}{j} \binom{a}{k_1,\dots,k_{q-1}} (-1)^{a+j+1} t^{j(q-1)+\sigma(k)-a}, \tag{7.1.1}$$

where the second sum runs over all $(q-1)$-tuples $k=(k_1,\dots,k_{q-1})$ of non-negative integers such that $k_1 + \cdots + k_{q-1} = a$ and $\sigma(k)$ is 'even', where $\sigma(k) := \sum_{j=1}^{q-1} jk_{j-1}$ and j and $\sigma(k)$ are subject to $j(q-1)+\sigma(k) < a+b$.

Proof. Following the same steps as in the proof of Theorem 6.1, it is easy to see that $\Delta(a,b) = \sum_{i=0}^{a+b-1} p_i S_1(a+b-i)$, where $P(t) = p_0 + p_1 t + \cdots + p_{a+b-1}t^{a+b-1} \in \mathbb{F}_p[t]$ is given by

$$P(t) = -\frac{[1]^{p^m-a-b}}{t^{p^m-a-b}} [1]^{a+b} \Delta(a,b) \mod t^{a+b}.$$

Let us write $P(t) = P_a(t) + P_b(t) + P_{a,b}(t)$, where $P_a(t) = -\frac{[1]^{p^m-a}}{t^{p^m-a}} \sum_{\theta\in\mathbb{F}_q^*} \frac{[1]^a}{(t+\theta)^a}$ and $P_{a,b}(t) = -\frac{[1]^{p^m-a-b}}{t^{p^m-a-b}} \sum_{\theta,\mu\in\mathbb{F}_q^*,\theta\neq\mu} \frac{[1]^a}{(t+\theta)^a} \frac{[1]^b}{(t+\mu)^b}$. Since $v_t(P_{a,b}(t)) \geqslant a+b$, where $v_t(\cdot)$ is the valuation at t, we have $P(t) \equiv P_a(t) + P_b(t)$ modulo t^{a+b}. Note that $H_{a,b}(t) = (1/t^a)(P_a(t) \bmod t^{a+b})$ (observe that $v_t(P_a(t)) \geqslant a$) and that $H_{b,a}(t)$ is obtained by interchanging a and b. Suppose for example that $\min\{a,b\} = a$. Then $P_a(t) + P_b(t)$ modulo t^{a+b} equals

$$t^a f(t) + t^b g(t) = \sum_{i=a}^{b-1} f_{i-a} t^i + \sum_{i=b}^{a+b-1} (f_{i-a} + g_{i-b}) t^i.$$

Therefore,

$$\Delta(a,b) = \sum_{i=0}^{b-1} f_i S_1(b-i) + \sum_{i=0}^{a-1} g_i S_1(a-i).$$

Now we compute $P_a(t)$. The factor $-[1]^{p^m-a}/t^{p^m-a} = -(t^{q-1}-1)^{p^m-a}$ brings in the binomial coefficient. Let $\theta \in \mathbb{F}_q^*$. Then, raising $[1]/(t+\theta) = \sum_{i=1}^{q-1} (-t)^i \theta^{q-1-i}$ to the a-th power, by the multinomial theorem, brings in $\sigma(k)$ and the multinomial coefficient. Summing over $\theta \in \mathbb{F}_q^*$ and using the fact that $\sum_{\xi\in\mathbb{F}_q^*} \xi^\ell$ is -1 or 0, depending on ℓ being 'even' or not, we get

$$P_a(t) = \sum_{j=0}^{p^m-a} \sum_{\substack{k_1+\cdots+k_{q-1}=a \\ q-1|\sigma(k)}} \binom{p^m-a}{j} \binom{a}{k_1,\dots,k_{q-1}} (-1)^{a+j+1} t^{j(q-1)+\sigma(k)}.$$

Since $H_{a,b}(t)$ is $1/t^a$ times the remainder of $P_a(t)$ when divided by t^{a+b}, we see that $H_{a,b}(t)$ is exactly as claimed. $\square$

When $q=2$, we get the following compact formula.

Corollary 7.2. *Let $q = 2$. Let $a, b \in \mathbb{Z}_+$ and let m be the smallest integer such that $a + b \leqslant 2^m$. Then*

$$\Delta(a,b) = \sum_{j=0}^{b-1} \binom{2^m - a}{j} S_1(b-j) + \sum_{i=0}^{a-1} \binom{2^m - b}{i} S_1(a-i).$$

Proof. For $q = 2$, Eq. (7.1.1) becomes $H_{a,b}(t) = \sum_{j=0}^{b-1} \binom{p^m - a}{j} t^j$. $\square$

Acknowledgments

This work has been developed under the direction of Dr. Dinesh S. Thakur at the University of Arizona and Dr. Gabriel D. Villa Salvador at the Departamento de Control Automático del Centro de Investigación y de Estudios Avanzados del IPN (Cinvestav-IPN) in México City. I thank Javier Diaz-Vargas for his suggestions and advice. I want to express my gratitude to the Universidad Autónoma de Yucatán and the Consejo Nacional de Ciencia y Tecnología for their financial support. I thank the Sage project [S+10] contributors for providing the environment to develop this research. I thank the referee for several helpful suggestions.

References

[AT09] Greg W. Anderson, Dinesh S. Thakur, Multizeta values for $\mathbb{F}\_q[t]$, their period interpretation and relations between them, Int. Math. Res. Not. IMRN 2009 (11) (May 2009) 2038–2055.

[Gos96] David Goss, Basic Structures of Function Field Arithmetic, Ergeb. Math. Grenzgeb. (3) (Results in Mathematics and Related Areas (3)), vol. 35, Springer-Verlag, Berlin, 1996.

[Lar] José Alejandro Lara Rodríguez, Special relations between function field multizeta values and parity results, preprint.

[Lar09] José Alejandro Lara Rodríguez, Some conjectures and results about multizeta values for $\mathbb{F}_q[t]$, Master's thesis, Autonomous University of Yucatan, Mexico, May 2009.

[Lar10] José Alejandro Lara Rodríguez, Some conjectures and results about multizeta values for $\mathbb{F}_q[t]$, J. Number Theory 130 (4) (2010) 1013–1023.

[S+10] W.A. Stein, et al., Sage mathematics software (version 4.4.4), The Sage Development Team, http://www.sagemath.org, 2010.

[Tha04] Dinesh S. Thakur, Function Field Arithmetic, World Scientific Publishing Co. Inc., River Edge, NJ, 2004.

[Tha09a] Dinesh S. Thakur, Power sums with applications to multizeta and zeta zero distribution for $\mathbb{F}_q[t]$, Finite Fields Appl. 15 (4) (2009) 534–552.

[Tha09] Dinesh S. Thakur, Relations between multizeta values for $\mathbb{F}_q[t]$, Int. Math. Res. Not. IMRN 2009 (12) (June 2009) 2318–2346.

[Tha10] Dinesh S. Thakur, Shuffle relations for function field multizeta values, Int. Math. Res. Not. IMRN 2010 (11) (2010) 1973–1980.

[Wal05] Michel Waldschmidt, Hopf algebras and transcendental numbers, in: Zeta Functions, Topology and Quantum Physics, in: Dev. Math., vol. 14, Springer, New York, 2005, pp. 197–219.

B.2. Special relations between multizeta values and parity results

J. Ramanujan Math. Soc. **27,** No.3 (2012) 275–293

Special relations between multizeta values and parity results

José Alejandro Lara Rodríguez

Departamento de Control Automático, Centro de Investigación y de Estudios Avanzados del IPN, Av. Instituto Politécnico Nacional 2508, San Pedro Zacatenco, 07360, México, D.F.
and
Facultad de Matemáticas de la Universidad Autónoma de Yucatán Anillo Periférico Norte, Tablaje Cat. 13615, Colonia Chuburná Hidalgo Inn, Mérida Yucatán, México
e-mail: lrodri@uady.mx; jlara@ctrl.cinvestav.mx

Communicated by: Dipendra Prasad

Received: January 10, 2011

Abstract. We study relations between multizeta values for function fields introduced by Thakur in [25,24]. The $\mathbb{F}_p$-span of Thakur's multizeta values is an algebra [26]. In particular, the product $\zeta(a)\zeta(b)$ is a linear combination of multizeta values. In this paper, several of the conjectures formulated in [16,25] for small values or for special families of a about how to write $\zeta(a)\zeta(b)$ as an $\mathbb{F}_p$-linear combination of multizeta values, are proved. Also, the parity conjecture formulated in [25] is proved.

1. Introduction

There are various interesting analogies [13,24,27,21] between function fields over finite fields and number fields. These analogies have been used to guess and prove results in one setting from the other. We start, at a very basic level, with the simplest analogies. The field $K = \mathbb{F}_q(t)$ of rational functions over $\mathbb{F}_q$ is a good analogue of the field $\mathbb{Q}$ of rational numbers. The polynomial ring $A = \mathbb{F}_q[t]$ is the analogue of the ring of integers $\mathbb{Z}$. Similarly, we have analogies $K_\infty \leftrightarrow \mathbb{R}$ and $\mathbb{C}_\infty \leftrightarrow \mathbb{C}$, where the notation is defined below. These analogies have helped the development of number theory.

Recall that the Riemann zeta function is defined as $\zeta_{\mathbb{Z}}(s) = \sum_{n=1}^{\infty} n^{-s}$, where $s \in \mathbb{C}$ and $\Re s > 1$. There is a rich *special values* theory associated to $\zeta_{\mathbb{Z}}(s)$, which is intimately connected to Bernoulli numbers, B_n. If $n \geq 0$, we have $\zeta_{\mathbb{Z}}(-n) = -B_{n+1}/(n+1)$. Consequently, if $n \geq 1$, $\zeta_{\mathbb{Z}}(-2n) = 0$. Such zeros are called trivial zeros and they are simple zeros. With respect to the non-trivial zeros, the well known Riemann hypothesis says that the non-trivial zeros of $\zeta_{\mathbb{Z}}(s)$ lie on the line $\Re s = 1/2$. It is still unknown whether the Riemann hypothesis holds. For $m = 2k$, $k > 0$ an integer, we have Euler's Theorem

$$\zeta_{\mathbb{Z}}(m) = -\frac{B_m(2\pi i)^m}{2(m!)}.$$

There is no simple formula for $\zeta_{\mathbb{Z}}(2k+1)$ analogous to the previous one. It is not known even whether $\zeta_{\mathbb{Z}}(2k+1)$ is rational or irrational, except for $k = 1$ when it is irrational by well-known result of Apéry [1].

For function field analogy, the Artin-Weil zeta function is defined by $\zeta_A(s) = \sum \mathrm{Norm}(I)^{-s}$, where the sum is over nonzero ideals and s is a complex variable, with $\Re s > 1$. The Riemann hypothesis in this case is known by Weil's theorem, but it is only a rational function of q^{-s}. So, for example there cannot be an analogue of Euler's Theorem connecting $\zeta_A(2k)$ to $(2\pi i)^{2k}$.

A more suitable analogue of transcendental special values of the Riemann zeta are the Carlitz zeta values defined by $\zeta_A(s) = \sum_{a \in A_+} a^{-s}$, where $s \in \mathbb{Z}_+$ and A_+ denotes the monic polynomials in $A = \mathbb{F}_q[t]$. Here the requirement monic is playing the role of "positive" in the classical Riemann zeta function $\zeta_{\mathbb{Z}}(s)$. In other words, instead of the norm which just depends on the degree of the polynomial, Carlitz used the whole polynomial, paying the price of considering a smaller domain for s, since we do not know how to raise a polynomial to a complex power. More justification lies in the following result [6,7], [24, Theorem 5.2.1]. If m is 'even' (that is, a multiple of $q-1$) and positive,

$$\zeta_A(m) = -B_m \widetilde{\pi}^m/(q-1)\Pi(m).$$

Here, $B_m \in K$ is a Bernoulli analogue, $\Pi(m) \in A$ is a factorial analogue, and

$$\widetilde{\pi} = (t - t^q)^{\frac{1}{q-1}} \prod_{n=1}^{\infty} \left(1 - \frac{t^{q^n} - t}{t^{q^{n+1}} - t}\right) \in \mathbb{C}_\infty,$$

plays the role of $2\pi i$ and is known to be transcendental over K [28]. There is no functional equation known. But in fact, much is known about the nature of the special values at positive integers in contrast to the classical case. We have the following result due to Anderson, Thakur, and Yu [2,31]: For m positive, $\zeta_A(m)$ is transcendental over K, and $\zeta_A(m)/\widetilde{\pi}^m$ is also transcendental if m is not 'even'.

In this case, the analogue of the Riemann hypothesis is known ([30,9,14,23,24,5]). Orders of vanishing of zeta at negative integers are not yet fully understood (but see [24,14,10,4]). For the details of the analytic continuation due to Goss, the theory of special values, its links with cyclotomic theory, periods of t-motives, etc., we refer to [14,24].

Now we turn to multizeta values. We refer to [29], and references in there, for a survey of many exciting recent developments related to the multizeta values introduced by Euler and their connections with theory of algebraic number fields. We will be concerned with an analogous theory of function fields.

Dinesh Thakur [24, Section 5.10] introduced two types of multizeta values for function fields over finite fields of characteristic p, one complex valued (generalizing the Artin-Weil zeta function) and the other with values in Laurent series over finite fields (generalizing the Carlitz-Goss zeta function). In this paper, we only focus on the latter. For its properties, connections with Drinfeld modules and Anderson t-motives, we refer the reader to [3,24–26].

Thakur proves the existence of "shuffle" relations for the multizeta values (for a general A with a rational place at infinity) [26]. In particular, he shows that the product of multizeta values can also be expressed as a sum of some multizeta values, so that the $\mathbb{F}_p$-span of all multizeta values is an algebra. In the function field case, the identities are much more complicated than the classical shuffle identities. In fact there are two types of identities, one with $\mathbb{F}_p(t)$ coefficients and the other with $\mathbb{F}_p$ coefficients. Note that although for many purposes a good analogue of $\mathbb{Q}$ is $\mathbb{F}_q(t)$, the prime field in characteristic p is $\mathbb{F}_p$ as $\mathbb{Q}$ is the prime field in characteristic 0. We concentrate only on the latter type.

The results in [26], although effective, are not explicit and bypass the explicit conjectures formulated in [25,15,16]. In this paper, we use the ideas of the process in [26] to prove the main conjecture formulated in [15,16]. In this paper, several conjectures for small values of a (Theorems 7.3, 7.6, 7.7, and 7.9), and a conjecture for special large values of a and b (Theorem 6.3) are proved. Also, the parity conjecture (Theorem 5.1) formulated in [25] is proved.

2. Notation

$\mathbb{Z}$	Ring of integers,
$\mathbb{Z}_+$	positive integers,
q	a power of a prime p, $q = p^s$,
$\mathbb{F}_q$	a finite field of q elements,
t	an independent variable,
A	the polynomial ring $\mathbb{F}_q[t]$,
A_+	monic polynomials in A,
K	the function field $\mathbb{F}_q(t)$,
K_∞	$\mathbb{F}_q((1/t))$, the completion of K at ∞,
$\mathbb{C}_\infty$	completion of an algebraic clousure of K_∞,
A_d	elements in A of degree d,
A_{d+}	$A_d \cap A_+$,

$[n]$	$= t^{q^n} - t$,
ℓ_n	$= \prod_{i=1}^{n}(t - t^{q^i}) = (-1)^n[n][n-1]\cdots[1]$,
'even'	multiple of $q-1$,
deg	function assigning to $a \in A$ its degree in t,
$\operatorname{Int}(x)$	$= \begin{cases} 0 & \text{if } x \text{ is not integer} \\ 1 & \text{if } x \text{ is integer} \end{cases}$
$\lfloor x \rfloor$	the largest integer not greater than x.

3. Thakur's multizeta values

For $s \in \mathbb{Z}_+$, the *Carlitz zeta values* [14,24] are defined as

$$\zeta(s) = \zeta_A(s) := \sum_{a \in A_+} \frac{1}{a^s} \in K_\infty.$$

For $s \in \mathbb{Z}$ and $d \geq 0$, we write

$$S_d(s) := \sum_{a \in A_{d+}} \frac{1}{a^s} \in K.$$

Given integers $s_i \in \mathbb{Z}_+$ and $d \geq 0$ put

$$S_d(s_1, \ldots, s_r) = S_d(s_1) \sum_{d > d_2 > \cdots > d_r \geq 0} S_{d_2}(s_2) \cdots S_{d_r}(s_r) \in K.$$

For $s_i \in \mathbb{Z}_+$, Thakur's *multizeta values* [24,25] are defined by:

$$\zeta(s_1, \ldots, s_r) := \sum_{d_1 > \cdots > d_r \geq 0} S_{d_1}(s_1) \cdots S_{d_r}(s_r) = \sum \frac{1}{a_1^{s_1} \cdots a_r^{s_r}} \in K_\infty,$$

where the second sum is over all $a_i \in A_+$ of degree d_i such that $d_1 > \cdots > d_r \geq 0$. We say that this multizeta value has depth r and weight $\sum s_i$.

4. Relations between multizeta values

Recall that Euler's multizeta values ζ (only in this paragraph, the greek letter ζ will be used to denote the classical multizeta values) are defined by $\zeta(s_1, \ldots, s_r) = \sum (n_1^{s_1} \cdots n_r^{s_r})^{-1}$, where the sum is over positive integers $n_1 > n_2 > \cdots > n_r$ and s_i are positive integers, with $s_1 > 1$ (this condition is required for convergence). Since $n_1 = n_2$, $n_1 > n_2$ or $n_2 > n_1$, we have the "sum shuffle relation"

$$\begin{aligned}\zeta(a)\zeta(b) = \sum_{n_1=1}^{\infty} \frac{1}{n_1^a} \sum_{n_2=1}^{\infty} \frac{1}{n_2^b} &= \sum_{n_1=n_2} \frac{1}{n_1^{a+b}} + \sum_{n_1>n_2} \frac{1}{n_1^a n_2^b} + \sum_{n_2>n_1} \frac{1}{n_2^b n_1^a} \\ &= \zeta(a+b) + \zeta(a,b) + \zeta(b,a).\end{aligned}$$

In the function field case, this sum shuffle relation fails because there are many polynomials of a given degree. In contrast to the classical sum shuffle, in the function field case, the identities we get are much more involved.

For $s_1, s_2 \in \mathbb{Z}_+$, put

$$S_d(s_1, s_2) = \sum_{\substack{d=d_1>d_2\\ a_i\in A_+}} \frac{1}{a_1^{s_1} a_2^{s_2}}$$

where $d_i = \deg(a_i)$. For $a, b \in \mathbb{Z}_+$, we define

$$\Delta_d(a, b) = S_d(a)S_d(b) - S_d(a+b).$$

We write $\Delta(a, b)$ for $\Delta_1(a, b)$. The definition implies that $\Delta_d(a, b) = \Delta_d(b, a)$.

The next two theorems (the second theorem in the reference has implications to higher genus function fields, but we state only a special case relevant to us) are due to Thakur [26, Theorems 1, 2].

Theorem 4.1. *Given $a, b \in \mathbb{Z}_+$, there are $f_i \in \mathbb{F}_p$ and $a_i \in \mathbb{Z}_+$, so that*

$$\Delta_d(a, b) = \sum f_i S_d(a_i, a+b-a_i) \tag{4.1.1}$$

holds for $d = 1$.

Theorem 4.2. *Fix A. If* (4.1.1) *holds for some $f_i \in \mathbb{F}_p^\times$ and distinct $a_i \in \mathbb{Z}_+$ for $d = 1$, then* (4.1.1) *holds for all $d \geq 0$. In this case, we have the shuffle relation*

$$\zeta(a)\zeta(b) - \zeta(a+b) - \zeta(a,b) - \zeta(b,a) = \sum f_i \zeta(a_i, a+b-a_i).$$

Remark 4.3. For each $a, b \in \mathbb{Z}_+$ the set $S(a, b)$ of pairs (f_i, a_i) is independent of d. Notice that $S(a, b) = S(b, a)$.

5. The 'even' restriction

In [25], Thakur conjectures that in the multizeta value identities all the iterated indices are 'even' and gives some heuristics reason for it. The following theorem proves the parity conjecture of Thakur. A different proof is given in [17], but it is much more involved.

Theorem 5.1. *Let $A = \mathbb{F}_q[t]$. Given $a, b \in \mathbb{Z}_+$, there are $f_i \in \mathbb{F}_p$ and $a_i \in \mathbb{Z}_+$, so that*

$$S_1(a)S_1(b) - S_1(a+b) = \sum f_i S_1(a_i). \tag{5.1.1}$$

Moreover, the a_i's are such that $a+b-a_i$ are 'even'.

Proof. The first part is proved in [26]. Here, we shall prove the second part following the proof in there. By specializing [25, 3.3] to $d = 1$ we see that

(5.1.2)
$$S_1(k+1) = \frac{(-1)^{k+1}}{[1]^{k+1}}\left(1 + \sum_{k_1=1}^{\lfloor k/q \rfloor}\binom{k - k_1(q-1)}{k_1}(-1)^{k_1}[1]^{k_1(q-1)}\right).$$

To simplify a little bit the notation, let us make the change $U \longleftrightarrow \frac{1}{[1]}$. Equation (5.1.2) becomes

$$S_1(a) = (-1)^a U^a\left(1 + \sum_{i=1}^{n_a}\binom{a-1-i(q-1)}{i}(-1)^i U^{-i(q-1)}\right)$$
$$= \alpha_{a,0}U^{\varphi_a(0)} + \alpha_{a,1}U^{\varphi_a(1)} + \cdots + \alpha_{a,n_a}U^{\varphi_a(n_a)},$$

where $\varphi_a(i) = a - i(q-1)$, $0 \le i \le n_a = \lfloor (a-1)/q \rfloor$, and

$$\alpha_{a,i} = \begin{cases} (-1)^a & \text{if } i = 0, \\ \binom{\varphi_{a-1}(i)}{i}(-1)^{a+i} & \text{for } i = 1, \ldots, n_a. \end{cases}$$

Thus, $S_1(a)$ is a $\mathbb{F}_p$-linear combination of powers of U and, therefore, so is $\Delta(a, b)$. More precisely, since $\varphi_a(i) + \varphi_b(j) = \varphi_{a+b}(i+j)$, and $\alpha_{a,0}\alpha_{b,0} = \alpha_{a+b,0} = (-1)^{a+b}$, we have

$$\begin{aligned}
&S_1(a)S_1(b) - S_1(a+b) \\
&= \left(\sum_{i=0}^{n_a}\alpha_{a,i}U^{\varphi_a(i)}\right)\left(\sum_{j=0}^{n_b}\alpha_{b,j}U^{\varphi_b(j)}\right) - \sum_{l=0}^{n_{a+b}}\alpha_{a+b,l}U^{\varphi_{a+b}(l)} \\
&= \sum_{k=0}^{n_a+n_b}\beta_k U^{\varphi_{a+b}(k)} - \sum_{l=0}^{n_{a+b}}\alpha_{a+b,l}U^{\varphi_{a+b}(l)} \\
&= \sum_{k=1}^{n_a+n_b}\beta_k U^{\varphi_{a+b}(k)} - \sum_{k=1}^{n_{a+b}}\alpha_{a+b,k}U^{\varphi_{a+b}(k)},
\end{aligned}$$

where $\beta_k = \sum_{i+j=k}\alpha_{a,i}\alpha_{b,j}$. Notice that

$$a + b - \varphi_{a+b}(k) = (a+b) - (a+b) + k(q-1) = k(q-1).$$

Therefore, $S_1(a)S_1(b) - S_1(a+b)$ is a polynomial in U with coefficients in $\mathbb{F}_p$ of degree less than $a+b$, such that $a+b-i$ is 'even' for every power i of U. Write

$$S_1(a)S_1(b) - S_1(a+b) = \theta_n U^n + \cdots + \theta_0 U^0,$$

where $\theta_n \neq 0$, $n < a+b$. Let $f_1 = (-1)^n\theta_n$ and $a_1 = n$. Each power of U in $S_1(a_1)$ is of the form $\varphi_{a_1}(i) = a_1 - i(q-1)$. Since $q-1$ divides $a+b-a_1$, it divides $a+b-a_1+i(q-1) = a+b-\varphi_{a_1}(i)$. Then, $S_1(a)S_1(b) - S_1(a+b) - f_1 S_1(a_1)$ is again a polynomial in U with coefficients in $\mathbb{F}_p$ of degree less than n, and each power of U satisfies the 'even' condition. We continue in this way, inductively, untill the sum is vacuous. $\square$

Theorem 5.2. *Fix q. Let K be a function field of one variable with field of constants $\mathbb{F}_q$; let ∞ be a place of K of degree one, and let A be the ring of elements of K with no poles outside ∞. Given $a, b \in \mathbb{Z}_+$, there are $f_i \in \mathbb{F}_p$ and $a_i \in \mathbb{Z}_+$ such that*

$$\zeta(a)\zeta(b) - \zeta(a+b) - \zeta(a,b) - \zeta(b,a) = \sum f_i \zeta(a_i, a+b-a_i),$$

with $a+b-a_i$ 'even'.

Proof. By the above theorem, there are $f_i \in \mathbb{F}_p$ and $a_i \in \mathbb{Z}_+$ such that (5.1.1) holds, and $a+b-a_i$ are 'even'. By Theorem 4.2, or rather by its more general version in [26] we have for general A as above that

$$S_d(a)S_d(b) - S_d(a+b) = \sum f_i S_d(a_i, a+b-a_i)$$

holds for all $d \geq 0$. $\square$

6. A relation for large indices

In this section we shall prove the Conjecture 2.8.1 formulated in [15,16] in two different ways. In [17], there is a third proof of this result.

Lucas Theorem [19,20,11] gives a method to determine the value of the binomial coefficient $\binom{m}{n}$ modulo a prime number p:

$$\binom{m}{n} \equiv \binom{m_0}{n_0} \cdots \binom{m_k}{n_k} \bmod p,$$

where $m = m_0 + m_1 p + \cdots + m_k$ and $n = n_0 + n_1 p + \cdots + n_k$ are the base p expansions of m and n, respectively. Since $\binom{a}{b} = 0$ if $b > a$, Lucas Theorem implies that the binomial coefficient $\binom{m}{n}$ does not vanish modulo p if and only if there is no carry over in base p in the sum of n and $m-n$.

Proposition 6.1. *For general q, we have*

$$S_1(2q^n - 1) = -\frac{[n+1]}{[1]^{2q^n}}. \tag{6.1.1}$$

Proof. We shall prove that for any k_1, $0 \le k_1 \le 2q^{n-1} - 1$,

$$\binom{2q^n - 2 - k_1(q-1)}{k_1}(-1)^{k_1} = \begin{cases} 1 & \text{if } k_1 \in \{0, 1, 1+q, \dots, 1+q+\cdots+q^{n-1}\}, \\ 0 & \text{otherwise.} \end{cases}$$

By Lucas Theorem, only the terms where there is no carry over in base p in the sum of k_1 and $2q^n - 2 - k_1 q$ need to be considered. The base p expansion of $2q^{n-1} - 1$ is

$$2q^{n-1} - 1 = (p-1) + (p-1)p + \cdots + (p-1)p^{s(n-1)-1} + p^{s(n-1)}.$$

Let $k_1 = a_0 + a_1 p + \cdots + a_{s(n-1)-1} p^{s(n-1)-1} + a_{s(n-1)} p^{s(n-1)}$ be the base p expansion of $0 \le k_1 \le 2q^{n-1} - 1$, where $a_{s(n-1)} \in \{0, 1\}$. Therefore, the base p expansion of $k_1 q$ is $a_0 p^s + a_1 p^{s+1} + \cdots + a_{s(n-1)-1} p^{sn-1} + a_{s(n-1)} p^{sn}$. Finally $2q^n - 2 = (p-2) + (p-1)p + \cdots + (p-1)p^{sn-1} + p^{sn}$ is the base p expansion of $2q^n - 2$. Let b_i denote the digits of $2q^n - 2 - k_1 q$. Since the first s digits of $2q^n - 2$ are $p-2, p-1, \dots, p-1$, the first s digits of $k_1 q$ are zero, and $k_1 q + (2q^n - 2 - k_1 q) = 2q^n - 2$, it follows that the first s digits of $2q^n - 2 - k_1 q$ are $b_0 = p-2$ and $b_i = p-1$, $1 \le i \le s-1$. Next we determine the remaining b_i's assuming that there is no carry over in the sum of $2q^n - 2 - k_1 q$ and k_1. By this assumption, it follows immediately that $a_i = 0$ for $1 \le i \le s-1$. Thus, $b_{s+1} = \cdots = b_{2s-1} = p-1$. Using again that there is no carry over in the sum of k_1 and $2q^n - 2 - k_1 q$, we get $a_{s2-1} = \cdots = a_{3s-1} = 0$ and, therefore, $b_{2s+1} = \cdots = b_{3s-1} = p-1$. By continuing this way we obtain that $k_1 = a_0 + a_s p^s + a_{2s} p^{2s} + \cdots + a_{s(n-1)} p^{s(n-1)}$. Now, since $a_k + b_k \le p-1$, $a_k + b_{k+s} = p-1$ and $b_0 = p-2$, we conclude that $a_{si} = 0$ or $a_{si} = 1$. It follows that if $a_{si} = 0$ for some i, then $a_{sj} = 0$ for $j > i$.

Now, if $k_1 = 0$, clearly $\binom{2q^n - 2 - k_1(q-1)}{k_1}(-1)^{k_1} = 0$. Let us assume that $k_1 = 1 + q + \cdots + q^i$ for some $0 \le i \le n-1$. Then, $q^{i+1} - 1 = (1 + q + \cdots + q^i)(q-1)$. Therefore, $2q^n - 2 - k_1(q-1) = q^n - 1 + q^{i+1}(q^{n-i-1} - 1)$. The digits c_j of $2q^n - 2 - k_1(q-1)$ are $c_{s(i+1)} = p-2$, $c_{sn} = 1$, and $c_j = p-1$, otherwise. The digits of k_1 are $a_j = 1$ for $j = 0, s, \dots, si$ and 0 otherwise. By Lucas Theorem, in $\mathbb{F}_p$ we have

$$\binom{2q^n - 2 - k_1(q-1)}{k_1} = \prod_{j=0}^{sn} \binom{c_j}{a_j} = (p-1)^{i+1} = (-1)^{i+1}.$$

Then $\binom{2q^n - 2 - k_1 q}{k_1}(-1)^{k_1} = (-1)^{i+1+k_1} = 1$ because $i+1$ and k_1 have the same parity. Since $(-1)^{2q^n - 1} = -1$ for any q, $\left\lfloor \frac{2q^n - 2}{q} \right\rfloor = 2q^{n-1} - 1$, and

$\sum_{i=0}^{n}[1]^{q^i} = [n+1]$, by (5.1.2) we have

$$\begin{aligned}
&S_1(2q^n-1)\\
&\quad = -\frac{1}{[1]^{2q^n-1}}\left(1+\sum_{k_1=1}^{2q^{n-1}-1}\binom{2q^n-2-k_1(q-1)}{k_1}(-1)^{k_1}[1]^{k_1(q-1)}\right)\\
&\quad = -\frac{1}{[1]^{2q^n-1}}\left(1+[1]^{q-1}+[1]^{q^2-1}+\cdots+[1]^{q^n-1}\right)\\
&\quad = -\frac{[n+1]}{[1]^{2q^n}}. \qquad \square
\end{aligned}$$

Remark 6.2. The Proposition 6.1 proves the Conjecture 2.10 in [16] for the case $m=2$ and $d=1$.

Next we prove the Conjecture 2.8.1 formulated in [16]. For general q we have the following theorem.

Theorem 6.3. *Let q be arbitrary. Then*

$$\zeta(q^n)\zeta(q^n-1) = \zeta(2q^n-1) + \zeta(q^n-1, q^n).$$

Proof 1. By Theorem 4.2 it is enough to prove

$$S_1(q^n)S_1(q^n-1) = S_1(2q^n-1) - S_1(q^n). \tag{6.3.1}$$

From [25, 3.3], we know that

$$S_d(ap^n) = 1/\ell_d^{ap^n}, \quad \text{if } a \le q, \tag{6.3.2}$$

$$S_d(q^i-1) = \frac{\ell_{d+i-1}}{\ell_{i-1}\ell_d^{q^i}} = \frac{[d+i-1]\cdots[d+1]}{[i-1]\cdots[1]\ell_d^{q^i-1}}. \tag{6.3.3}$$

Equation (6.3.1) follows from formulas (6.1.1), (6.3.2), (6.3.3), and from the fact $[n+1]-[n] = [1]^{q^n}$. $\square$

Proof 2. By definition of $\Delta(a,b)$, it follows that

$$\Delta(a,b) = \sum_{\substack{n_1\neq n_2\\ n_1,n_2\in A_{1+}}}\frac{1}{n_1^a n_2^b} = \sum_{n_2\in A_{1+}}\frac{1}{n_2^b}\left(S_1(a)-\frac{1}{n_2^a}\right). \tag{6.3.4}$$

For any $a \in A_{1+}$, we have $[1]/a = a^{q-1}-1$. By (6.3.2), we also have $[1]^{q^n}S_1(q^n) = -1$. Taking $b = q^n-1$ in (6.3.4), we have

$$\begin{aligned}\Delta(q^n, q^n - 1) &= S_1(q^n) \sum_{a \in A_{1+}} \frac{1}{a^{q^n - 1}} \left(1 + \frac{[1]^{q^n}}{a^{q^n}}\right) \\ &= S_1(q^n) \sum_{a \in A_{1+}} \frac{1}{a^{q^n - 1}} a^{(q-1)q^n} \\ &= S_1(q^n) S_1(-N),\end{aligned}$$

where $N = q^{n+1} - 2q^n + 1$. To finish, we prove that $S_1(-N) = -1$. Now

$$\begin{aligned}S_1(-N) &= \sum_{\theta \in \mathbb{F}_q} (t + \theta)^N \\ &= t^N + \sum_{\theta \in \mathbb{F}_q^*} (t + \theta)^N = t^N + \sum_{l=0}^{N} \binom{N}{l} t^{N-l} \sum_{\theta \in \mathbb{F}_q^*} \theta^l.\end{aligned}$$

Since the sum $\sum_{\theta \in \mathbb{F}_q^*} \theta^l$ is 0 if $q - 1$ does not divide l, and -1 if $l \geq 0$ is divisible by $q - 1$, and $N \equiv 0 \bmod (q - 1)$, we get

$$S_1(-N) = -1 - \sum_{0 < l < \frac{N}{q-1}} \binom{N}{l(q-1)} t^{N - l(q-1)}.$$

Let $m = sn$. The base p expansion of N is $N = 1 + (p - 2)p^m + (p - 1)p^{m+1} + \cdots + (p - 1)p^{m+s-1}$. Let $l(q - 1) = \sum_{k=0}^{m+s-1} b_k p^k$ be the base p expansion of $l(q - 1)$. By Lucas Theorem, the following equality holds in $\mathbb{F}_p$

$$\binom{N}{l(q-1)} = \binom{1}{b_0}\binom{0}{b_1} \cdots \binom{0}{b_{m-1}}\binom{p-2}{b_m}\binom{p-1}{b_{m+1}} \cdots \binom{p-1}{b_{m+s-1}}.$$

Therefore, $\binom{N}{l(q-1)} \neq 0$ if and only if $b_0 \leq 1$, $b_k = 0$ for $k = 1, \ldots, m - 1$, and $b_m \leq p - 2$.

Since p^m and $q-1$ are coprime, p^m is a unit in $\mathbb{Z}/(q-1)\mathbb{Z}$. Therefore, the equation $j \equiv -\imath p^m \bmod (q - 1)$ has always a solution. Furthermore, there is exactly one solution in the range $0 \leq \imath < q - 1$. For $j = 0$, the solution is 0, and for $j = 1$ the solution is $q - 2$ because $N = 1 + (q - 2)p^m \equiv 0 \bmod (q - 1)$.

If $\binom{N}{l(q-1)} \neq 0$, then $l(q - 1) = j + ip^m$, $0 \leq j \leq 1$, $0 \leq i \leq q - 2$, where $i = \sum_{k=0}^{m+s-1} b_{m+k} p^k$. Then, $l(q - 1) \in \{0, N\}$. Thus, $\binom{N}{l(q-1)} = 0$ for $1 \leq l < N/(q - 1)$. Therefore, $S_1(-N) = -1$. □

7. Relations for small values of *a*

In this section we prove that for $1 \leq a \leq p$, the sets $S(a, b)$ can be found recursively; we also prove some of the conjectures for low values of a given in [25,16].

The following results will be used in this section.

Theorem 7.1. *Let k be a positive integer. Let $\ell(k)$ be the sum of digits of k in base q.*

a) *If $d > \ell(k)/(q-1)$, then $S_d(-k) = 0$ ([24, Theorem 5.1.2]; see also [18, Lemma 7.1] and [12, Corollary 2.12]).*
b) *$S_d(-(q^{k+d}-1)) = (-1)^d D_{d+k}/L_d D_k^{q^d}$, where $D_n = [n][n-1]^q \cdots [1]^{q^{n-1}}$ and $L_n = [n][n-1]\cdots[1]$ for $n > 0$, $D_0 = 1$, and $L_0 = 1$ ([8]; see also [12, Theorem 4.1]).*

In particular, when $d = 1$, we have $S_1(-(q-1)) = -1$.

Definition 7.2. *Let $a \in \mathbb{Z}_+$.*

(1) *We set*

$$r_a := (q-1)p^m,$$

where m is the smallest integer such that $a \leq p^m$.

(2) *For i, j, put*

$$\phi(i, j) := r_a - a - j(q-1) + i r_a,$$
$$\phi(j) := \phi(0, j).$$

(3) *We define*

$$j_{a,\max} = \left\lfloor \frac{r_a - a}{q-1} \right\rfloor,$$

where $\lfloor x \rfloor$ is the largest integer not greater than x.

(4) *Let* Int (x) *be 1 if x is integer, and* 0*, otherwise.*

Theorem 7.3 (Conjecture 4.3.1, [25]). *For general q, we have,*

$$\zeta(1)\zeta(b) = \zeta(1+b) + \zeta(1, b) + \zeta(b, 1) + \sum_{i=0}^{\sigma-1} \zeta(b - \phi(i), 1 + \phi(i)),$$

where $\phi(i)$ and r_1 are as in Definition 7.2, and $b = r_1\sigma + \beta, 0 < \beta \leq r_1$.

Proof. Let $a = 1$. Then, $r_1 = q - 1$. By (6.3.3), we have $[1]S_1(1) = -1$. Proceeding as in the second proof of Theorem 6.3, we get $\Delta(1, b + r_1) = S_1(1)S_1(b)$. Therefore, $\Delta(1, b+r_1) - \Delta(1, b) = S_1(1+b)$. Now, $\Delta(1, b) = 0$ for $1 \leq b \leq q - 1$ because $1 + b \leq q$ [25, Theorem 1]. Therefore, for any $b \in \mathbb{Z}_+$, $\Delta(1, b) = \sum_{i=0}^{\sigma-1} S_1(b - \phi(i))$. Theorem follows from applying Theorem 4.2. $\square$

Remarks 7.4.

(1) Theorem 7.3 is proved for $q = 2$ and b arbitrary, and also for general q and b 'even' in [25].
(2) The proof of Theorem 7.3 shows that the sets $S(1, b)$ can be found recursively, with recursion length $r_1 = q - 1$.

Theorem 7.5. *Let $a, b \in \mathbb{Z}_+$. Let r_a be as in Definition 7.2. If $2 \leq a \leq p$, then*

$$\begin{aligned}&\Delta(a, b + r_a) - \Delta(a, b)\\ &\quad = \sum_{j=1}^{p-a} f_{a,j} S_1(a + b + (p - j)(q - 1)) + S_1(a + b),\end{aligned}$$

where $f_{a,j} = \binom{a+j-1}{j} = \binom{a+j-1}{a-1}$ is nonzero for any j. In particular, the sets $S(a, b)$, $2 \leq a \leq p$, can be found recursively with recursion length r_a, by

$$S(a, b + r_a) = S(a, b) \cup T(a, b + r_a),$$

where

$$\begin{aligned}&T(a, b + r_a)\\ &\quad = \{(1, a + b)\} \cup \left\{(f_{a,j}, a + b + (p - j)(q - 1)) \mid 1 \leq j \leq p - a\right\}.\end{aligned}$$

Proof. For each $n \in A_{1+}$, let $g_n = (-1)^{a+1}[1]^{p-a}/n^{p-a}$. Then

$$g_n = (-1)^{a+1}(n^{q-1} - 1)^{p-a} = 1 + \sum_{j=1}^{p-a} f_{a,j} n^{j(q-1)},$$

where $f_{a,j} = \binom{p-a}{j}(-1)^j$. Let $\Sigma = \sum_{j=1}^{p-a} f_{a,j} S_1(b + r_a - \phi(p - j))$. Then,

$$\begin{aligned}\Sigma &= \sum_{n_2 \in A_{1+}} \sum_{j=1}^{p-a} \frac{f_{a,j}}{n_2^{b+r_a-(r_a-a-(p-j)(q-1))}}\\ &= \sum_{n_2 \in A_{1+}} \frac{1}{n_2^{b+r_a}} \frac{1}{n_2^{a}} \sum_{j=1}^{p-a} f_{a,j} n_2^{j(q-1)}.\end{aligned}$$

By (6.3.3), we have $[1]^a S_1(a) = (-1)^a$. For any $n \in A_{1+}$,

$$S_1(a) - \frac{g_n}{n^a} = S_1(a) + S_1(a)\frac{[1]^p}{n^p} = S_1(a)\left(1 + \frac{[1]}{n}\right)^p = S_1(a)n^{p(q-1)}.$$

Then,

$$\begin{aligned}\Delta(a, b + r_a) - \Sigma &= \sum_{n_2 \in A_{1+}} \frac{1}{n_2^{b+r_a}}\left(S_1(a) - \frac{1}{n_2^a}\left(1 + \sum_{j=1}^{p-a} f_{a,j} n_2^{j(q-1)}\right)\right)\\ &= S_1(a) \sum_{n_2 \in A_{1+}} \frac{n_2^{p(q-1)}}{n_2^{b+r_a}}\\ &= S_1(a)S_1(b).\end{aligned}$$

Therefore, $\Delta(a, b + r_a) - \Delta(a, b) = \Sigma + S_1(a + b)$. This shows that $T(a, b + r_a)$ is exactly as claimed. Note that $f_{a,j} \neq 0$ because of Lucas Theorem. Finally,

$$\begin{aligned}f_{a,j} &= \binom{p-a}{j}(-1)^j = (-1)^j \frac{1}{j!}\prod_{i=0}^{j-1}(p - a - i)\\ &= \frac{1}{j!}\prod_{i=0}^{j-1}(a + i) = \binom{a + j - 1}{j}.\end{aligned}$$

□

Next, we apply Theorem 7.5 to $a = 2$ and $p = 2$.

Theorem 7.6 (Conjecture 2.1, [16]). *Let q be a power of $p = 2$. Let r_2, $\phi(i, j)$ and* Int$(\cdot)$ *be as in Definition 7.2. Write $b = r_2\sigma + \beta$, $0 < \beta \leq r_2$. Then*

$$\begin{aligned}\zeta(2)\zeta(b) &= \zeta(2 + b) + \zeta(2, b) + \zeta(b, 2)\\ &\quad + \sum_{i=0}^{\sigma-1} \zeta(b - \phi(i, 0), 2 + \phi(i, 0)) + \mathrm{Int}\left(\frac{b}{q-1}\right)\frac{b}{q-1}\zeta(2, b).\end{aligned}$$

Proof. By Theorem 4.2, it is enough to prove $\Delta(2, b) = D(2, b)$, where

$$D(2, b) = \sum_{i=0}^{\sigma-1} S_1(b - \phi(i, 0)) + \mathrm{Int}\left(\frac{b}{q-1}\right)\frac{b}{q-1}S_1(2). \tag{7.6.1}$$

Note that $b + r_2 = r_2(\sigma + 1) + \beta$; also $b + r_2 - \phi(i, 0) = b - \phi(i - 1, 0)$. It follows that

$$D(2, b + r_2) = \sum_{i=-1}^{\sigma-1} S_1(b - \phi(i, 0)) + \mathrm{Int}\left(\frac{b + r_2}{q-1}\right)\frac{b + r_2}{q-1}S_1(2).$$

Since $q-1$ divides r_2, then $q-1$ divides b if and only if $q-1$ divides $b+r_2$; also $b-\phi(-1,0)=2+b$. Thus, $D(2,b+r_2)-D(2,b)=S_1(2+b)$. On the other hand, since $a=p$, by Theorem 7.5, we have $\Delta(2,b+r_2)-\Delta(2,b)=D(2,b+r_2)-D(2,b)$.

Let us compute $\Delta(2,b)$ for $1\le b\le r_2$. Proceeding as in the proof of Theorem 6.3, we get $\Delta(2,b)=S_1(2)S_1(-(r_2-b))$. If $b=r_2=2(q-1)$, then $S_1(0)=0$. If $b=q-1$, then, by Theorem 7.1 (b), $S_1(-(q-1))=-1$ follows. Suppose $1\le b<q-1$. Then $r_2-b=(q-2-b)+q$ is the base q expansion of r_2-b. Since $\ell(r_2-b)<q-1$, by Theorem 7.1 (a), it follows that $S_1(-(r_2-b))=0$. If now, $q-1<b<r_2$, write $b=(q-1)+\rho$, where $0<\rho<q-1$. Then $r_2-b=q-1-\rho$ is the base q expansion of r_2-b. Applying Theorem 7.1 (a) again, we have that $S_1(-(r_2-b))=0$. In summary, $\Delta(2,b)=S_1(2)$ if $b=q-1$ and 0, otherwise. Therefore, $\Delta(2,b)=D(2,b)$ for $b=1,\dots,r_2$. □

Theorem 7.7 (Conjecture 2.6, [16]). *Let p be any prime and let q be a power of p. Then*

$$\begin{aligned}\zeta(2)\zeta(b)&=\zeta(2+b)+\zeta(2,b)+\zeta(b,2)\\&\quad+\sum_{j=0}^{p-1}(j+2)\sum_{b-\phi(i,p-1-j)>2}\zeta(b-\phi(i,p-1-j),2\\&\quad+\phi(i,p-1-j))+\mathrm{Int}\left(\frac{b}{q-1}\right)\frac{b}{q-1}\zeta(2,b),\end{aligned}$$

where $\phi(i,k)$ and $\mathrm{Int}(\cdot)$ *are as in Definition 7.2.*

Proof. Let $f_b=\mathrm{Int}\left(\frac{b}{q-1}\right)\frac{b}{q-1}$. By Theorem 4.2, it is enough to prove $\Delta(2,b)=D(2,b)$, where

$$D(2,b)=\sum_{j=0}^{p-1}(j+2)\sum_{i=0}^{n(b,j)}S_1(b+2-(pi+1+j)(q-1))+f_bS_1(2). \tag{7.7.1}$$

We have $b+r_2+2-(pi+1+j)(q-1)=b+2-(p(i-1)+1+j)(q-1)$ and $n(b+r_2,j)=n(b,j)+1$. Then

$$\begin{aligned}&D(2,b+r_2)\\&\quad=\sum_{j=0}^{p-1}(j+2)\sum_{i=-1}^{n(b,j)}S_1(b+2-(pi+1+j)(q-1))+f_{b+r_2}S_1(2).\end{aligned}$$

Now, $q-1$ divides b if and only if $q-1$ divides $b+r_2$ because $q-1$ divides r_2. Therefore,

$$D(2,b+r_2)-D(2,b)=\sum_{j=1}^{p}(j+1)S_1(2+b+(p-j)(q-1))).$$

On the other hand, $f_{2,j}=\binom{j+1}{1}=j+1$ for $1\le j\le p-2$, $j+1=0$ when $j=p-1$, and $j+1=1$ when $j=p$. By Theorem 7.5, it follows that

$$\begin{aligned}\Delta(2,b+r_2)-\Delta(2,b)&=\sum_{j=1}^{p-2}f_{2,j}S_1(2+b+(p-j)(q-1))+S_1(2+b)\\&=D(2,b+r_2)-D(2,b).\end{aligned}$$

To finish, we prove that $\Delta(2,b)=D(2,b)$ for $1\le b\le r_2$. Let $1\le b\le r_2$. If $n(b,j)\ge 1$, then $r_2\ge b\ge r_2+(1+j)(q-1)+1$ which implies the contradiction $0\ge(1+j)(q-1)+1\ge 1$. Thus, $n(b,j)<1$. Now, $n(b,j)=0$ if and only if $b-1-(1+j)(q-1)\ge 0$. Thus, equation (7.7.1) becomes

$$D(2,b)=\sum_{j=0}^{\left\lfloor\frac{b-q}{q-1}\right\rfloor}(j+2)S_1(b+2-(1+j)(q-1))+f_bS_1(2). \tag{7.7.2}$$

Write $b=\lambda(q-1)+\rho$, where $0\le\rho<q-1$. If $\rho=0$, take $l=\lambda-1$; if $\rho>0$, let $l=\lambda$. Thus, l is the integer in the set $\{0,1,\ldots,p-1\}$ such that $l(q-1)+1\le b\le(l+1)(q-1)$. Then, $(l-1)(q-1)\le b-q\le l(q-1)-1<l(q-1)$. Therefore, $\left\lfloor\frac{b-q}{q-1}\right\rfloor=l-1$. Now, we rewrite equation (7.7.2) as follows:

$$\begin{aligned}D(2,b)&=\sum_{n\in A_{1+}}\sum_{j=0}^{l-1}\frac{j+2}{n^{b+2-(1+j)(q-1)}}+\sum_{n\in A_{1+}}\frac{f_b}{n^2}\\&=\sum_{n\in A_{1+}}\frac{1}{n^{b+2-(q-1)}}\left(\sum_{j=0}^{l-1}\frac{(j+2)n^{b+2-(q-1)}}{n^{b+2-(1+j)(q-1)}}+f_bn^{b-(q-1)}\right)\\&=\sum_{n\in A_{1+}}\frac{P_n}{n^{b+2-(q-1)}},\end{aligned}$$

where $P_n=\sum_{j=0}^{l-1}(j+2)n^{j(q-1)}+f_bn^{b-(q-1)}$. By (6.3.2), $S_1(2)=1/[1]^2$. Then

$$\Delta(2,b)-D(2,b)=\sum_{n\in A_{1+}}\frac{n^2-[1]^2-n^{q-1}[1]^2P_n}{n^{b+2}[1]^2}.$$

Now, we compute $(n^{q-1}-1)^2 P_n$. Firstly, note that

$$n^{2(q-1)} \sum_{j=0}^{l-1} (j+2) n^{j(q-1)} = \sum_{j=0}^{l-1} (j+2) n^{(j+2)(q-1)},$$

$$-2n^{q-1} \sum_{j=0}^{l-1} (j+2) n^{j(q-1)} = -\sum_{j=-1}^{l-1} 2(j+3) n^{(j+2)(q-1)},$$

and

$$\sum_{j=0}^{l-1} (j+2) n^{j(q-1)} = \sum_{j=-2}^{l-1} (j+4) n^{(j+2)(q-1)}.$$

Therefore, $(n^{q-1}-1)^2 P_n$ equals

$$2 - n^{q-1} - (l+2) n^{l(q-1)} + (l+1) n^{(l+1)(q-1)} + (n^{q-1}-1)^2 f_b n^{b-(q-1)}.$$

Since $n^{q-1}[1]^2 P_n = n^{q+1}(n^{q-1}-1)^2 P_n$, it follows that $n^{q-1}[1]^2 P_n$ equals

$$\begin{aligned} &2n^{q+1} - n^{2q} - (l+2) n^{(l+1)(q-1)+2} \\ &\quad + (l+1) n^{(l+2)(q-1)+2} + n^{q-1}[1]^2 f_b n^{b-(q-1)}. \end{aligned}$$

Using $n^2 - [1]^2 = -n^{2q} + 2n^{q+1}$, we get

$$\begin{aligned} n^2 - [1]^2 - n^{q-1}[1]^2 P_n &= (l+2) n^{(l+1)(q-1)+2} \\ &\quad - (l+1) n^{(l+2)(q-1)+2} - n^{q-1}[1]^2 f_b n^{b-(q-1)}. \end{aligned}$$

Dividing $n^2 - [1]^2 - n^{q-1}[1]^2 P_n$ by n^{b+2} and summing over $n \in A_{1+}$, we get

$$[1]^2(\Delta(2,b) - D(2,b)) = (l+2) S_1(-k_1) - (l+1) S_1(-k_2) - f_b.$$

where $k_1 = (l+1)(q-1) - b$ and $k_2 = (l+2)(q-1) - b$. Now, if $b \equiv 0 \mod (q-1)$, then $l = \frac{b}{q-1} - 1$; thus, $k_1 = 0$ and $k_2 = q-1$. By Theorem 7.1 (b), we have $S_1(-(q-1)) = -1$; since $S_1(0) = 0$ and $f_b = \frac{b}{q-1} = l+1$, it follows that $(\Delta(2,b) - D(2,b)) = 0$. Suppose $b \not\equiv 0 \mod (q-1)$. Then, $f_b = 0$. In this case, $b = l(q-1) + \rho$ with $0 < \rho < q-1$. Therefore, $k_1 = q-1-\rho$ and $k_2 = (q-2-\rho) + q$. Note that these are the base q expansions of k_1 and k_2 because $q-1-\rho < q-1$ and $q-2-\rho < q-1$. Then, $\ell(k_1) = \ell(k_2) = q-1-\rho$. Since $\ell(k_1) = \ell(k_2) < (q-1)$, by Theorem 7.1 (a), it follows that $S_1(-k_1) = S_1(-k_2) = 0$. Therefore, $\Delta(a,b) - D(2,b) = 0$ for $1 \leq b \leq r_2$. $\square$

Remark 7.8. Theorem 7.7 generalizes Theorem 7.6. Let q be a power of p. Let $b \in \mathbb{Z}_+$ and $0 \leq j \leq p-1$. Since $\phi(i, p-1-j) = (pi+1+j)(q-1)-2$, the condition $b - \phi(i, p-1-j) > 2$ is equivalent to $n(b, j) \geq i$, where $n(b, j) = \left\lfloor \frac{b-1-(1+j)(q-1))}{r_2} \right\rfloor$. More precisely, $b - \phi(i, p-1-j) > 2 \Longleftrightarrow \frac{b-1}{q-1} \geq pi + 1 + j$. Now, we specialize to $p = 2$ and write $b = r_2\sigma + \beta$, $0 < \beta \leq r_2$. Then, $n(b, p-1) = n(b, 1) = \sigma - 1$. Equation (7.7.1) becomes equation (7.6.1):

$$\sum_{j=0}^{1}(j+2)\sum_{i=0}^{\sigma-1} S_1(b - \phi(i, 1-j)) + \mathrm{Int}\left(\frac{b}{q-1}\right)\frac{b}{q-1}S_1(2)$$
$$= 3\sum_{i=0}^{\sigma-1} S_1(b - \phi(i, 0)) + \mathrm{Int}\left(\frac{b}{q-1}\right)\frac{b}{q-1}S_1(2).$$

Theorem 7.9 (Conjecture 2.3, [16]). *Let $q = 2$. For $b \in \mathbb{Z}_+$, we have*

$$\zeta(3)\zeta(b) = \zeta(b+3) + \zeta(3, b) + \zeta(b, 3)$$
$$+ \sum_{i=0}^{\lfloor (b-5)/4 \rfloor} \zeta(b-1-4i, 4+4i) + \sum_{i=0}^{\lfloor (b-4)/4 \rfloor} \zeta(b-4i, 3+4i)$$
$$+ \sum_{i=1}^{2} \mathrm{Int}\left(\frac{b-i}{r_3}\right)(\zeta(2, b+1) + \zeta(3, b)).$$

Proof. It is enough to prove that $\Delta(3, b) = D(3, b)$, where

$$D(3, b) = \sum_{i=0}^{\lfloor (b-5)/4 \rfloor} S_1(b-1-4i) + \sum_{i=0}^{\lfloor (b-4)/4 \rfloor} S_1(b-4i)$$
$$+ \sum_{i=1}^{2} \mathrm{Int}\left(\frac{b-i}{r_3}\right)(S_1(2) + S_1(3)).$$

Using that $\lfloor x+1 \rfloor = \lfloor x \rfloor + 1$, we get $\lfloor (b-5)/4 \rfloor = \lfloor (b-1)/4 \rfloor - 1$ and $\lfloor (b-4)/4 \rfloor = \lfloor b/4 \rfloor - 1$. Then,

$$\sum_{i=0}^{\lfloor (b-1)/4 \rfloor} S_1(b+4-1-4i) = \sum_{i=-1}^{\lfloor (b-5)/4 \rfloor} S_1(b-1-4i),$$

and

$$\sum_{i=0}^{\lfloor b/4 \rfloor} S_1(b+4-4i) = \sum_{i=-1}^{\lfloor (b-4)/4 \rfloor} S_1(b-4i).$$

Since $(b-i) \equiv 0 \bmod 4$ if and only if $(b+4-i) \equiv 0 \bmod 4$, it follows that $D(3, b+4) - D(3, b) = S_1(b+3) + S_1(b+4)$. By (5.1.2), we have

$$S_1(3) = \frac{1}{[1]^3} + \frac{1}{[1]^2} = \frac{1}{n^3(n+1)^3} + \frac{1}{n^2(n+1)^2}.$$

A straight-forward calculation shows that $S_1(3) - \frac{1}{n^3} - n^4 S_1(3) = 1$. It follows that

$$\begin{aligned}\Delta(3, b+4) - \Delta(3, b) &= \sum_{n \in A_{1+}} \frac{1}{n^{b+4}} \left(S_1(3) - \frac{1}{n^3} - n^4 S_1(3) - n \right) \\ &= S_1(b+4) + S_1(b+3).\end{aligned}$$

Then, $\Delta(3, b)$ can be found recursively with recursion length $r_3 = 4$, and $\Delta(3, b+4) - \Delta(3, b) = D(3, b+4) - D(3, b)$. Finally, a direct calculation shows that $\Delta(3, b) = D(3, b)$ for $b = 1, 2, 3, 4$. $\square$

Remark 7.10. Let $q = 2$ and $a = 3$. Then, $\phi(i, j) = 1 - j + 4i$. The condition $b - \phi(i, 0) > 3$ is equivalent to $i \le (b-5)/4$. Since $j_{3,\max} = 1$, the condition $b - \phi(i, j_{3,\max}) > 3$ is equivalent to $i \le (b-4)/4$. Therefore, the proof of Theorem 7.9 confirms Conjecture 2.3 of [16].

Acknowledgments

This work has been developed under the direction of Dr. Dinesh S. Thakur at the University of Arizona and Dr. Gabriel D. Villa Salvador at the Departamento de Control Automático del Centro de Investigación y de Estudios Avanzados del IPN (Cinvestav-IPN) in México City. I thank Javier Diaz-Vargas for his suggestions and advice. I want to express my gratitude to the Universidad Autónoma de Yucatán and the Consejo Nacional de Ciencia y Tecnología for their financial support. I thank the contributors of the Sage project [22] for providing the development environment for this research.

References

[1] Roger Apery, Irrationalité de $\zeta(3)$ et $\zeta(3)$, *Astérisque*, **61** (1979) 11–13.

[2] Greg W. Anderson and Dinesh S. Thakur, Tensor powers of the Carlitz module and zeta values, *Ann. of Math. (2)*, **132(1)** (1990) 159–191.

[3] Greg W. Anderson and Dinesh S. Thakur, Multizeta values for $\mathbb{F}_q[t]$, their period interpretation and relations between them, *International Mathematics Research Notices*, **2009(11)** May (2009) 2038–2055.

[4] Victor Bautista-Ancona, Javier Diaz-Vargas and José Luis Maldonado-Bazán, Orders of vanishing of zeros of characteristic p zeta function, *Rocky Mountain J. Math.*, **39(2)** (2009) 399–412.

[5] Victor Bautista-Ancona, Javier Diaz-Vargas and Gabriel Villa-Salvador, Notes on the Riemann hypothesis in characteristic p, *Int. J. Pure Appl. Math.*, **63(3)** (2010) 341–353.

[6] Leonard Carlitz, On certain functions connected with polynomials in a Galois field, *Duke Math. J.*, **1(2)** (1935) 137–168.

[7] Leonard Carlitz, An analogue of the von Staudt-Clausen theorem, *Duke Math. J.*, **3(3)** (1937) 503–517.
[8] Leonard Carlitz, Some sums involving polynomials in a Galois field, *Duke Math. J.*, **5** (1939) 941–947.
[9] Javier Diaz-Vargas, Riemann hypothesis for $\mathbb{F}_q[t]$, *J. Number Theory*, **59(2)** (1996) 313–318.
[10] Javier Diaz-Vargas, On zeros of characteristic p zeta function, *J. Number Theory*, **117(2)** (2006) 241–262.
[11] Nathan J. Fine, Binomial coefficients modulo a prime, *Amer. Math. Monthly*, **54** (1947) 589–592.
[12] Ernst-Ulrich Gekeler, On power sums of polynomials over finite fields, *J. Number Theory*, **30(1)** (1988) 11–26.
[13] David Goss, Addendum to v-adic zeta functions, L-series, and measures for function fields, *Invent. Math.*, **55(2)** (1979) 117–119.
[14] David Goss, Basic structures of function field arithmetic, volume 35 of Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]. Springer-Verlag, Berlin, (1996).
[15] José Alejandro Lara Rodríguez, Some conjectures and results about multizeta values for $\mathbb{F}_q[t]$. Master's thesis, Autonomous University of Yucatan, Mexico, May (2009).
[16] José Alejandro Lara Rodríguez, Some conjectures and results about multizeta values for $\mathbb{F}_q[t]$, *J. Number Theory*, **130(4)** (2010) 1013–1023.
[17] José Alejandro Lara Rodríguez, Relations between multizeta values in characteristic p, *J. Number Theory*, **131(4)** (2011) 2081–2099.
[18] Herbert Leonard Lee, Power sums of polynomials in a Galois field, *Duke Math. J.*, **10** (1943) 277–292.
[19] Edouard Lucas, Sur les congruences des nombres eulériens et les coefficients différentiels des functions trigonométriques suivant un module premier, *Bull. Soc. Math. France*, **6** (1878) 49–54.
[20] Edouard Lucas, Théorie des Fonctions Numériques Simplement Périodiques, *Amer. J. Math.*, **1(3)** (1878) 197–240.
[21] Michael Rosen, Number theory in function fields, volume 210 of Graduate Texts in Mathematics, Springer-Verlag, New York (2002).
[22] William A. Stein, et al. Sage Mathematics Software (Version 4.4.4). The Sage Development Team, 2010. http://www.sagemath.org.
[23] Jeffrey T. Sheats, The Riemann hypothesis for the Goss zeta function for $\mathbb{F}_q[t]$, *J. Number Theory*, **71(1)** (1998) 121–157.
[24] Dinesh S. Thakur, Function field arithmetic, World Scientific Publishing Co. Inc., River Edge, NJ (2004).
[25] Dinesh S. Thakur, Relations between multizeta values for $\mathbb{F}_q[t]$, *International Mathematics Research Notices*, **2009(12)** June (2009) 2318–2346.
[26] Dinesh S. Thakur, Shuffle Relations for Function Field Multizeta Values, *Int. Math. Res. Not. IMRN*, **2010(11)** (2010) 1973–1980.
[27] Gabriel Daniel Villa Salvador, Topics in the theory of algebraic function fields, *Mathematics: Theory & Applications. Birkhäuser Boston Inc., Boston, MA* (2006).
[28] L. I. Wade, Certain quantities transcendental over $GF(p^n, x)$, *Duke Math. J.*, **8** (1941) 701–720.
[29] Michel Waldschmidt, Hopf algebras and transcendental numbers, In Zeta functions, topology and quantum physics, volume 14 of *Dev. Math.*, pages 197–219, Springer, New York (2005).
[30] Daqing Wan, On the Riemann hypothesis for the characteristic p zeta function, *J. Number Theory*, **58(1)** (1996) 196–212.
[31] Jing Yu, Transcendence and special zeta values in characteristic p, *Ann. of Math. (2)*, **134(1)** (1991) 1–23.

B.3. On von Staudt for Bernoulli-Carltiz numbers

Journal of Number Theory 132 (2012) 495–501

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On von Staudt for Bernoulli–Carlitz numbers

José Alejandro Lara Rodríguez [a,b]

[a] Departamento de Control Automático, Centro de Investigación y de Estudios Avanzados del IPN, Av. Instituto Politécnico Nacional 2508, San Pedro Zacatenco, 07360 México, D.F., Mexico
[b] Facultad de Matemáticas, Universidad Autónoma de Yucatán, Mérida, Yucatán, Mexico

ARTICLE INFO

Article history:
Received 26 May 2011
Accepted 14 December 2011
Available online xxxx
Communicated by David Goss

Keywords:
Function fields
Drinfeld modules
Denominators
Bernoulli numbers

ABSTRACT

In 1935, Carlitz introduced analogues of Bernoulli numbers for $\mathbb{F}_q[t]$. These are now called Bernoulli–Carlitz numbers B_m. He proved a von Staudt type theorem, with a much more subtle statement than the classical one, describing their denominators completely. As an analog of the important relative $\mathcal{B}_m/m$ of the usual Bernoulli number $\mathcal{B}_m$, Thakur considered an analog $B_m(m-1)!_C/m!_C$, where $m!_C$ is the Carlitz factorial. He described their denominator fully except when $q=2$ and m has a particular form. The purpose of this paper is to completely describe this last remaining situation. Also, we shall see that a group of symmetries recently discovered by Goss may be realized as symmetries of our results.

1. Introduction

In 1935, L. Carlitz introduced and studied in positive characteristic analogues of Bernoulli numbers [Car35], for which he was able to prove an analogue of the von Staudt–Clausen theorem [Car37, Car40]. See [Gos78] for an exposition in a self-contained and modern notation and [Gek89] for some identities between these analogues of Bernoulli numbers. We also refer to [Gos96,Tha04] for various related theorems for them and perspective of function field arithmetic.

Let us recall the classical situation. Bernoulli numbers $\mathcal{B}_m$ and their relatives $\mathcal{B}_m/m$ are important in various branches of mathematics. See e.g., [MS74,Leh88] and [Tha04, 4.16]. The von Staudt–Clausen theorem determines the fractional part of Bernoulli numbers. Specifically, for even $m>0$, $\mathcal{B}_m - \sum 1/p$ is integer, where the sum extends over the primes p such that $p-1$ divides m. Hence, the denominator of $\mathcal{B}_m$ is the product of all primes p such that $p-1$ divides m. The Lipschitz–Sylvester theorem says that $a^m(a^m-1)\mathcal{B}_m/m$ is integer for any integer a. Combining the two, it follows easily (choose

E-mail addresses: lrodri@uady.mx, jlara@ctrl.cinvestav.mx.

0022-314X/$ – see front matter © 2011 Published by Elsevier Inc.
doi:10.1016/j.jnt.2011.12.005

a to be a primitive root modulo p dividing m) that primes dividing the denominators of $\mathcal{B}_m$ and of $\mathcal{B}_m/m$ are exactly the same.

For m a multiple of $q-1$, the Bernoulli–Carlitz numbers B_m are in $\mathbb{F}_q(t)$. Carlitz was able to prove an analogue of the von Staudt–Clausen theorem (Theorem 3.5) over the rational function field $K=\mathbb{F}_q(t)$. The $q=2$ case is more subtle, as was already noticed by Carlitz in [Car41]. There he gives a correction if $q=2$, for his von Staudt–Clausen type theorem, as originally stated in [Car37,Car40] is not correct.

Note that B_m/m does not make sense for Bernoulli–Carlitz numbers B_m as m is in characteristic zero! On the other hand, D. Thakur shows that a good analogue to $\mathcal{B}_m/m$ in the function field case is $B_m(m-1)!_C/m!_C$, where $m!_C$ denotes the Carlitz factorial. Thakur gives a theorem [Tha04, Theorem 4.16.5] on comparing the prime decomposition of the denominators of B_m and $B_m(m-1)!_C/m!_C$. The $q>2$ case is settled and the case $q=2$ was settled except for a sequence of possible exceptions. The purpose of this paper is to complete this case.

2. Frequently used notation

$\mathbb{Z}_+$	{positive integers}
q	a power of a prime p, $q=p^n$
$\mathbb{F}_q$	a finite field of q elements
A	the polynomial ring $\mathbb{F}_q[t]$
K	the function field $\mathbb{F}_q(t)$
$[i]$	$=t^{q^i}-t$
D_i	$=[i][i-1]^q\cdots[1]^{q^{i-1}}$
L_i	$=[1][2]\cdots[i]$
A-even	divisible by the number of units of A
$\lfloor x\rfloor$	the largest integer not greater than x

3. Bernoulli–Carlitz numbers

Here we concentrate on the $A=\mathbb{F}_q[t]$ case, where $q=p^n$, p a prime.

The factorial function for A was defined by Carlitz [Car37] as follows:

Definition 3.1. Let $m\in\mathbb{Z}_+$ and let $m=\sum m_i q^i$ be its q-adic expansion. Then, the factorial of m is defined by

$$m!_C := \prod_i D_i^{m_i}.$$

The Carlitz factorial has divisibility properties analogous to those of the classical factorial [Tha04, Chapter 4].

Example 3.2.

(1) With this definition, we have, for instance, that $q^l!_C=D_l$.
(2) For any positive integer m, $(qm-1)!_C=(q(m-1))!_C$. Indeed, if $m-1=\sum_{i=0}^{\nu} n_i q^i$ is the q-adic expansion of $m-1$, then, $qm-1=q-1+\sum_{i=0}^{\nu} n_i q^{i+1}$ is the q-adic expansion of $qm-1$.

Now we use the Carlitz factorial to define the Carlitz's analogues of Bernoulli numbers. For positive integer m, define the Bernoulli–Carlitz numbers $B_m\in\mathbb{F}_q(t)$ by means of the generating function

$$\frac{z}{e_C(z)}=\sum_{m=0}^{\infty}\frac{B_m}{m!_C}z^m,$$

where e_C is the Carlitz exponential

$$e_C(z) = \sum_{j=0}^{\infty} \frac{z^{q^j}}{D_j}.$$

Remark 3.3.

(1) Note that the summation defining the Bernoulli–Carlitz numbers B_m contains A-even terms only.
(2) Here, B_m differs from the corresponding B_m in Carlitz's papers by $(-1)^m$.
(3) For any l, we have [Tha04]

$$\frac{B_{p^l m}}{(p^l m)!_C} = \left(\frac{B_m}{m!_C}\right)^{p^l}.$$

We see this by taking the p-th power of the generating function and comparing it by substituting z with z^p.

Define $A_m^{(k)}$ by means of

$$e_C(z)^{q^k-1} = \sum_{m=q^k-1}^{\infty} \frac{A_m^{(k)}}{m!_C} z^m. \tag{3.3.1}$$

Carlitz showed [Car37] that

$$B_m = \sum_{q^k \leqslant m+1} \frac{A_m^{(k)}}{L_k}, \tag{3.3.2}$$

where $A_m^{(k)}$ is integral and a multiple of $(q^k-1)!_C$. Let $C_m^{(k)} \in A$ such that $A_m^{(k)} = C_m^{(k)}(q^k-1)!_C$. Then,

$$\frac{A_m^{(k)}}{L_k} = \frac{C_m^{(k)}(q^k-1)!_C}{L_{k-1}} \frac{1}{[k]} = C_m^{(k)} \frac{(D_1 \cdots D_{k-1})^{q-1}}{L_{k-1}} \frac{1}{[k]}. \tag{3.3.3}$$

Now L_{k-1} divides $(D_1 \cdots D_{k-1})^{q-1}$, and except when $q = 2 = k$, the primes in $[k]$ of degree less than k divide the resulting quotient. Further, except for the case $q = 2 = k$, the irreducible factors of the denominator of $(q^k-1)!_C/L_k$ are all of degree k.

Let $m = \sum m_i p^i$ be the p-adic expansion of m. Let us consider the conditions

$$h = \frac{\sum m_i}{n(p-1)} \in \mathbb{Z}_+, \quad q^h - 1 \mid m. \tag{3.3.4}$$

Remark 3.4. Carlitz showed [Car37, p. 514] [Car40, p. 63] that if P is a prime of degree k, and k does not satisfy the conditions (3.3.4), then $A_m^{(k)} \equiv 0 \bmod P$.

Both classical Bernoulli numbers $\mathcal{B}_m$ and $\mathcal{B}_m/m$ are important as they occur in many investigations: power sums, measures and special values of zeta and L-functions and topology, just to mention a few. See for example Appendix B of Milnor's book [MS74] for applications to topology. Von Staudt proved that the primes dividing the denominators of $\mathcal{B}_m$ or of $\mathcal{B}_m/m$ are exactly the same.

The numbers $B_m(m-1)!_C/m!_C$ can be thought [Tha04, 4.16] as analogues of $\mathcal{B}_m/m$, although they do not seem to satisfy congruences of Kummer type. Thakur proved an analogue of Lipschitz–Sylvester theorem [Tha04, Theorem 4.16.3] for them. (See also weaker variants in [Car37, Theorem 5] and [Car41, Theorem 3].) But he also noted that it does not imply the primes dividing the denominators in the analogous situation are the same. Hence both the theorems below describing the two denominators separately can be considered to be analogs of von Staudt–Clausen theorem!

Let P_k denote the product of all the monic primes of degree k. Now we state Carlitz's von Staudt–Clausen type theorem for the Bernoulli–Carlitz numbers.

Theorem 3.5. *(Carlitz, see [Car37,Car40,Car41].) Let $A = \mathbb{F}_q[t]$, with $q = p^n$, p a prime. Let $m \in \mathbb{Z}_+$ be A-even, and let $m = \sum m_i p^i$ be its p-adic decomposition. Let $d(m)$ denote the monic denominator of B_m for A. Let h be as in* (3.3.4)*. Then,*

(1) *Let $q > 2$. If h is an integer and $q^h - 1$ divides m, then $d(m) = P_h$, otherwise $d(m) = 1$.*
(2) *Let $q = 2$. Let $h \neq 2$. If $q^h - 1$ divides m, then $d(m) = P_h$, otherwise $d(m) = 1$. Let $h = 2$. If $q^h - 1 = 3$ divides m, then $d(m) = P_2$ for m a multiple of 2 and $d(m) = [2] = P_1P_2$ otherwise. If $q^h - 1$ does not divide m, then for m not a multiple of 2, $d(m) = P_1$ and otherwise $d(m) = 1$.*

Remark 3.6. For $q = 2$, the result as originally stated in [Car37,Car40,Gos78] is not correct. A corrected version is given in [Car41].

Theorem 3.7.

(1) *Let $q > 2$. Then, the primes dividing the denominators of B_m or $B_m(m-1)!_C/m!_C$ are the same. In fact, if q^k is the maximum power of q dividing m, and if the denominator of B_m is P_h, then the denominator of $B_m(m-1)!_C/m!_C$ is $P_h^{\lfloor k/h \rfloor + 1}$.*
(2) *Let $q = 2$. Then, the primes dividing the denominators of B_m or of $B_m(m-1)!_C/m!_C$ are the same, unless m is of the form $2 + 2^\alpha$ with $\alpha > 1$. If 2^k is the maximum power of 2 dividing m, and if the denominator of B_m is $\mathcal{D}$, then the denominator of $B_m(m-1)!_C/m!_C$ is $\mathcal{D}^{\lfloor k/h \rfloor + 1}$.*
(3) *Let $q = 2$. Let $m = 2 + 2^\alpha$, $\alpha > 1$.*
    (a) *If $m \equiv 0 \bmod 3$, then the denominator of $B_m(m-1)!_C/m!_C$ is $P_1P_2 = t(t+1)(t^2+t+1)$.*
    (b) *If $m \equiv 1 \bmod 3$, then the denominator of $B_m(m-1)!_C/m!_C$ is $P_1 = t(t+1)$.*

Proof. (1) See [Tha04, Theorem 4.16.5].

Because of practical reasons, we shall prove part (3) before part (2).

(3) Note that for general q,

$$\frac{(m-1)!_C}{m!_C} = \frac{1}{L_k} \tag{3.7.1}$$

where q^k is the maximum power of q dividing m.

Let us write $B_m = N_m/d(m)$ with N_m and $d(m)$ coprime.

If $m \equiv 0 \bmod 3$, it follows that $m = 2 + 2^{2i}$, $(i \geqslant 1)$. Then $h = 2$, $q^h - 1 = 3$ divides m and m is even. Thus, $d(m) = P_2 = t^2 + t + 1$. Since $(m-1)!_C/m!_C = 1/L_1$, we have

$$B_m = \frac{N_m}{P_2}, \qquad B_m \frac{(m-1)!_C}{m!_C} = \frac{N_m}{P_2} \frac{1}{P_1}.$$

If $m = 2 + 2^{2i+1}$, then $h = 2$, $q^h - 1 = 3$ does not divide m, and m is even. Thus $d(m) = 1$. Therefore,

$$B_m = N_m, \qquad B_m \frac{(m-1)!_C}{m!_C} = \frac{N_m}{1} \frac{1}{P_1}.$$

It remains to prove that P_1 does not divide N_m. Since m is not a power of 2, by (3.3.1) it follows that $A_m^{(1)} = 0$. Let $k > 2$ and $2^k - 1 \leqslant m$. Clearly, k does not satisfy (3.3.4). Now, if P is a prime of degree k, by Remark 3.4 it follows that P_k divides $C_m^{(k)}$ so that $A_m^{(k)}/L_k$ belongs to A. Also, from (3.3.3), it follows that P_1 divides $A_m^{(k)}/L_k$. Therefore,

$$B_m = G_m + \frac{A_m^{(2)}}{L_2}, \tag{3.7.2}$$

where $G_m \in \mathbb{F}_q[t]$ is divisible by P_1 and

$$G_m = \sum_{q^k-1\leqslant m,\, k\neq 2} \frac{A_m^{(k)}}{L_k}. \tag{3.7.3}$$

Let us assume first that $m = 2 + 2^{2i}$. Then

$$\frac{A_m^{(2)}}{L_2} = \frac{t^2 + t^{2^{2i}}}{[1][2]} = \frac{[2i-1]^2}{P_1^2 P_2} = \frac{N}{P_2},$$

where $N = [2i-1]^2/P_1^2 \in A$ and N is relatively prime to P_2. By Euclidean algorithm, there are unique $Q(t)$ and $R(t)$ in A such that $N = P_2 Q(t) + R(t)$, where R is nonzero and $\deg R < 2$. Since N and P_2 are invariant with respect to the automorphism $t \to t+1$ of A, it follows that $R(t) = R(t+1)$, so that R is not t nor $t+1$. Hence $R = 1$. Now, since N is prime to P_1^2, then $N \equiv 1 \bmod P_1^2$. Then, $Q(t)P_2 \equiv 0 \bmod P_1^2$. Since P_2 and P_1^2 are coprime, it follows that $Q \equiv 0 \bmod P_1^2$. We have

$$B_m = \frac{1}{P_2}(G_m + Q + 1),$$

where P_1 divides $G_m + Q$. Therefore, the numerator of B_m is not divisible by P_1.

Now, let $m = 2 + 2^{2i+1}$, $(i \geqslant 1)$. Then

$$\frac{A_m^{(2)}}{L_2} = \frac{t^2 + t^{2^{2i+1}}}{[1][2]} = \frac{[2i]^2}{P_1^2 P_2}.$$

Thus $A_m^{(2)}/L_2$ is in A and is not divisible by P_1. Since $B_m = G_m + A_m^{(2)}/L_2$, where G_m is divisible by P_1, it follows that the numerator of B_m is not divisible by P_1.

(2) Now we turn to the case when m is an integer which is not of the form $2 + 2^\alpha$, with $\alpha > 1$. If $k = 0$, i.e., if m is odd, by (3.7.1) we have $B_m = B_m(m-1)!_C/m!_C$. Indeed, if $h \neq 2$, by the part already proved by Thakur [Tha04, Theorem 4.16.5], we have that the primes dividing the denominators of B_m or of $B_m(m-1)!_C/m!_C$ are exactly the same.

If $m = 4 + 2^\alpha$, with $\alpha > 2$, write $m = 2m'$, where $m' = 2 + 2^{\alpha-1}$. Then,

$$\begin{aligned}\frac{(2m'-1)!_C B_{2m'}}{(2m')!_C} &= \frac{(2m'-1)!_C}{(2(m'-1))!_C}\frac{(2(m'-1))!_C}{(m'-1)!_C^2}\left(\frac{(m'-1)!_C B_{m'}}{m'!_C}\right)^2 \\ &= [1][\alpha]\left(\frac{(m'-1)!_C B_{m'}}{m'!_C}\right)^2.\end{aligned}$$

By part (3),

$$\frac{(2m'-1)!_C B_{2m'}}{(2m')!_C} = \begin{cases} \frac{[1][\alpha]N_{m'}^2}{P_1^2} & \text{if } \alpha \text{ is even,} \\ \frac{[1][\alpha]N_m^2}{P_1^2 P_2^2} & \text{if } \alpha \text{ is odd.} \end{cases}$$

Then, the denominator of $B_m(m-1)!_C/m!_C$ is 1 or P_2^2, depending on α being even or not.

Next we do induction on $k > 2$. Since,

$$\frac{(2m-1)!_C B_{2m}}{(2m)!_C} = [1][2]\cdots[k][\alpha+1]\left(\frac{(m-1)!_C B_m}{m!_C}\right)^2,$$

we see that if prime P divides the denominator of $B_{2m}(2m-1)!_C/(2m)!_C$, then divides the denominator of $B_m(m-1)!_C/m!_C$, which by induction hypothesis implies that P divides the denominator of B_m. The comparison of the Theorem 3.5 statement conditions for m as for qm implies that P divides the denominator of B_{2m}.

Note that $[i]$ is the product of the monic primes in A whose degree divides i. Then $P_h^{\lfloor k/h \rfloor}$ is the maximum power of P_h dividing L_k. Then, it follows that the denominator of $B_m(m-1)!_C/m!_C$ is as claimed. $\square$

Remark 3.8. David Goss notes that our results fit into the setting of his work [Gos11]. Indeed, we shall see below that the group $S_{(q)}$ (defined below) may be realized as symmetries of our von Staudt–Clausen type theorem.

Let q be a power of p and let $x \in \mathbb{Z}_p$. Write x q-adically as

$$x = \sum_{i=0}^{\infty} c_i q^i$$

where $0 \leqslant c_i < q$ for all i. Let ρ be a permutation of the set $\{0, 1, 2, \ldots\}$. David Goss defines [Gos11] $\rho_*(x)$, $x \in \mathbb{Z}_p$, by

$$\rho_*(x) := \sum_{i=0}^{\infty} c_i q^{\rho(i)}.$$

Let $S_{(q)}$ be the subgroup of permutations of $\mathbb{Z}_p$ obtained as ρ varies over all permutations of $\{0, 1, 2, \ldots\}$.

Let $\partial(m)$ denote the denominator of $B_m(m-1)!_C/m!_C$ for A. The following corollary shows that the condition that a prime divides $\partial(m)$ satisfies the symmetries given by Corollaries 5 and 6 in [Gos11].

Corollary 3.9. *Let q be arbitrary. Let $\mathfrak{P}$ be a prime of degree h. If $q = 2$ and $h = 1$, then the condition $v_{\mathfrak{P}}(\partial(m)) > 0$ is an invariant of the subgroup $\tilde{S}_4$ of $S_{(4)}$ arising from the permutations of $\{0, 1, 2, \ldots\}$ fixing 0. Otherwise, the condition $v_{\mathfrak{P}}(\partial(m)) > 0$ is an invariant of the action of $S_{(q^h)}$ on the positive integers divisible by $q-1$.*

Acknowledgments

This work has been developed under the direction of Dr. Dinesh S. Thakur at the University of Arizona and Dr. Gabriel D. Villa Salvador at the Departamento de Control Automático del Centro de Investigación y de Estudios Avanzados del IPN (Cinvestav-IPN) in Mexico City. I want to express my gratitude to the Universidad Autónoma de Yucatán and the Consejo Nacional de Ciencia y Tecnología for their financial support. I thank the Sage project [S+11] contributors for providing the environment to develop this research. I thank David Goss for his useful suggestions.

References

[Car35] Leonard Carlitz, On certain functions connected with polynomials in a Galois field, Duke Math. J. 1 (2) (1935) 137–168.
[Car37] Leonard Carlitz, An analogue of the von Staudt–Clausen theorem, Duke Math. J. 3 (3) (1937) 503–517.
[Car40] Leonard Carlitz, An analogue of the Staudt–Clausen theorem, Duke Math. J. 7 (1940) 62–67.
[Car41] Leonard Carlitz, An analogue of the Bernoulli polynomials, Duke Math. J. 8 (1941) 405–412.
[Gek89] Ernst-Ulrich Gekeler, Some new identities for Bernoulli–Carlitz numbers, J. Number Theory 33 (2) (1989) 209–219.
[Gos78] David Goss, Von Staudt for $\mathbf{F}_q[T]$, Duke Math. J. 45 (4) (1978) 885–910.
[Gos96] David Goss, Basic Structures of Function Field Arithmetic, Ergeb. Math. Grenzgeb. (3) (Results in Mathematics and Related Areas (3)), vol. 35, Springer-Verlag, Berlin, 1996.
[Gos11] David Goss, Noncommutative geometry, arithmetic, and related topics, in: Proceedings of the Twenty-First Meeting of the Japan–US Mathematics Institute, Baltimore, The Johns Hopkins University Press, 2011.
[Leh88] D.H. Lehmer, A new approach to Bernoulli polynomials, Amer. Math. Monthly 95 (10) (1988) 905–911.
[MS74] John W. Milnor, James D. Stasheff, Characteristic Classes, Ann. of Math. Stud., vol. 76, Princeton University Press, Princeton, NJ, 1974, .
[S+11] William A. Stein, et al., Sage Mathematics Software (Version 4.6.1), The Sage Development Team, 2011, http://www.sagemath.org.
[Tha04] Dinesh S. Thakur, Function Field Arithmetic, World Scientific Publishing Co. Inc., River Edge, NJ, 2004.

Referencias

[AET01] Shigeki Akiyama, Shigeki Egami, and Yoshio Tanigawa. Analytic continuation of multiple zeta-functions and their values at non-positive integers. *Acta Arith.*, 98(2):107–116, 2001. 1.1.1

[And86] Greg W. Anderson. t-motives. *Duke Math. J.*, 53(2):457–502, 1986. 3.1

[Apé79] Roger Apéry. Irrationalité de $\zeta(2)$ et $\zeta(3)$. *Astérisque*, 61:11–13, 1979. 1.1.1

[AT] Greg W. Anderson and Dinesh S. Thakur. Ihara power series for $\mathbb{F}_q[t]$. *Preprint.* 1.3

[AT90] Greg W. Anderson and Dinesh S. Thakur. Tensor powers of the Carlitz module and zeta values. *Ann. of Math. (2)*, 132(1):159–191, 1990. 1.2.2

[AT09] Greg W. Anderson and Dinesh S. Thakur. Multizeta values for $\mathbb{F}_q[t]$, their period interpretation and relations between them. *International Mathematics Research Notices*, 2009(11):2038–2055, May 2009. 1.3, 3.1

[BADVMB09] Victor Bautista-Ancona, Javier Diaz-Vargas, and José Luis Maldonado-Bazán. Orders of vanishing of zeros of characteristic p zeta function. *Rocky Mountain J. Math.*, 39(2):399–412, 2009. 1.2.2

[BADVVS10] Víctor Bautista-Ancona, Javier Diaz-Vargas, and Gabriel Villa-Salvador. Notes on the Riemann Hypothesis in characteristic p. *Int. J. Pure Appl. Math.*, 63(3):341–353, 2010. 1.2.2

[BBBL98] Jonathan Michael Borwein, David M. Bradley, David J. Broadhurst, and Petr Lisoněk. Combinatorial aspects of multiple zeta values. *Electron. J. Combin.*, 5:Research Paper 38, 12 pp. (electronic), 1998. 1.1.1

[BK97] David J. Broadhurst and Dirk Kreimer. Association of multiple zeta values with positive knots via Feynman diagrams up to 9 loops. *Phys. Lett. B*, 393(3-4):403–412, 1997. 1.1.1

[BR01] Keith Ball and Tanguy Rivoal. Irrationalité dúne infinité de valeurs de la fonction zêta aux entiers impairs. *Invent. Math.*, 146(1):193–207, 2001. 1.1.1

[Car35] Leonard Carlitz. On certain functions connected with polynomials in a Galois field. *Duke Math. J.*, 1(2):137–168, 1935. (document), 1.2, 1.2.2, 4.1

[Car37] Leonard Carlitz. An analogue of the von Staudt-Clausen theorem. *Duke Math. J.*, 3(3):503–517, 1937. (document), 1.2.2, 4.1, 4.2, 4.2, 4.2.4, 4.2, 4.2.5, 4.2.6

[Car39] Leonard Carlitz. Some sums involving polynomials in a Galois field. *Duke Math. J.*, 5:941–947, 1939. b

[Car40] Leonard Carlitz. An analogue of the Staudt-Clausen theorem. *Duke Math. J.*, 7:62–67, 1940. 4.1, 4.2.4, 4.2.5, 4.2.6

[Car41] Leonard Carlitz. An analogue of the Bernoulli polynomials. *Duke Math. J.*, 8:405–412, 1941. 4.1, 4.2, 4.2.5, 4.2.6

[Dic02] Leonard Eugene Dickson. Theorems on the residues of multinomial coefficients with respect to a prime modulus. *Quart. J. Pure Appl. Math.*, 33:378–384, 1902. 3

[DV96] Javier Diaz-Vargas. Riemann hypothesis for $\mathbb{F}_q[t]$. *J. Number Theory*, 59(2):313–318, 1996. 1.2, 1.2.2

[DV06] Javier Diaz-Vargas. On zeros of characteristic p zeta function. *J. Number Theory*, 117(2):241–262, 2006. 1.2.2

[Eul75] Leonard Euler. Meditationes circa singvlare seriervm genus. *Novi Commentarii academiae scientiarum Petropolitanae*, 20:140–186, 1775. 1.1, 1.1.1

[Fin47] Nathan J. Fine. Binomial coefficients modulo a prime. *Amer. Math. Monthly*, 54:589–592, 1947. 3

[Gek88] Ernst-Ulrich Gekeler. On power sums of polynomials over finite fields. *J. Number Theory*, 30(1):11–26, 1988. a, b

[Gek89] Ernst-Ulrich Gekeler. Some new identities for Bernoulli-Carlitz numbers. *J. Number Theory*, 33(2):209–219, 1989. 4.1

[Gos78] David Goss. von Staudt for $\mathbf{F}_q[T]$. *Duke Math. J.*, 45(4):885–910, 1978. 4.1, 4.2.6

[Gos79] David Goss. Addendum to v-adic zeta functions, L-series, and measures for function fields. *Invent. Math.*, 55(2):117–119, 1979. 1.2

[Gos96] David Goss. *Basic structures of function field arithmetic*, volume 35 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1996. 1.2.2, 1.3, 2.1, 4.1

[Gos11] David Goss. Zeta phenomenology. In *Noncommutative geometry, arithmetic, and related topics: Proceedings of the Twenty-First Meeting of the Japan-US Mathematics Institute*, pages 159–182. Johns Hopkins Univ. Press, Baltimore, MD, 2011. (document), 4.2.8, 4.2

[Has33] Helmut Hasse. Beweis des Analogons der Riemannschen Vermutung für die Artinschen und FK Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen. Vorl. Mitt.(German). *Nachr. Ges. Wiss. Göttingen, Math.-Phys. Kl. I*, 42:253–262, 1933. 1.2

[Lar09] José Alejandro Lara Rodríguez. Some conjectures and results about multizeta values for $\mathbb{F}_q[t]$. Master's thesis, Universidad Autónoma de Yucatán, México, Mayo 2009. 1.4.7, 1.5

[Lar10] José Alejandro Lara Rodríguez. Some conjectures and results about multizeta values for $\mathbb{F}_q[t]$. *J. Number Theory*, 130(4):1013–1023, 2010. (document), 1.4.7, 1.5, 2.6

[Lar11] José Alejandro Lara Rodríguez. Relations between multizeta values in characteristic *p*. *J. Number Theory*, 131(4):2081–2099, 2011. 2

[Lar12a] José Alejandro Lara Rodríguez. On von Staudt for Bernoulli-Carlitz numbers. *J. Number Theory*, 132(4):495 – 501, 2012.

[Lar12b] José Alejandro Lara Rodríguez. Special relations between function field multizeta values and parity results. *Journal of the Ramanujan Mathematical Society*, 27(3):275–293, 2012.

[Lee43] Herbert Leonard Lee. Power sums of polynomials in a Galois field. *Duke Math. J.*, 10:277–292, 1943. a

[Leh88] D. H. Lehmer. A new approach to Bernoulli polynomials. *Amer. Math. Monthly*, 95(10):905–911, 1988. 4.1

[LM95] Tu Quoc Thang Le and Jun Murakami. Kontsevich's integral for the Homfly polynomial and relations between values of multiple zeta functions. *Topology Appl.*, 62(2):193–206, 1995. 1.1.1

[Luc78a] Edouard Lucas. Sur les congruences des nombres eulériens et les coefficients différentiels des functions trigonométriques suivant un module premier. *Bull. Soc. Math. France*, 6:49–54, 1878. 3

[Luc78b] Edouard Lucas. Théorie des Fonctions Numériques Simplement Périodiques. *Amer. J. Math.*, 1(3):197–240, 1878. 3

[Mas05] Riad Masri. Multiple Dedekind zeta functions and evaluations of extended multiple zeta values. *J. Number Theory*, 115(2):295–309, 2005. 1.1.2

[Mas06] Riad Masri. Multiple zeta values over global function fields. In *Multiple Dirichlet series, automorphic forms, and analytic number theory*, volume 75 of *Proc. Sympos. Pure Math.*, pages 157–175. Amer. Math. Soc., Providence, RI, 2006. 1.2.1

[MS74] John W. Milnor and James D. Stasheff. *Characteristic classes*. Princeton University Press, Princeton, N. J., 1974. Annals of Mathematics Studies, No. 76. 4.1, 4.2

[Riv02] Tanguy Rivoal. Irrationalité dáu moins un des neuf nombres $\zeta(5)$, $\zeta(7)$, $\ldots$, $\zeta(21)$. *Acta Arith.*, 103(2):157–167, 2002. 1.1.1

[Ros02] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002. 1.2

[S^+11] William A. Stein et al. *Sage Mathematics Software (Version 4.7.2)*. The Sage Development Team, 2011. `http://www.sagemath.org`. 3.4

[She98] Jeffrey T. Sheats. The Riemann hypothesis for the Goss zeta function for $\mathbb{F}_q[t]$. *J. Number Theory*, 71(1):121–157, 1998. 1.2, 1.2.2

[Tha04] Dinesh S. Thakur. *Function field arithmetic*. World Scientific Publishing Co. Inc., River Edge, NJ, 2004. (document), 1.2, 1.2.2, 1.3, 2.1, 3.1, 3.4.1, 4.1, 4.2, 3, 4.2, 4.2, 4.2

[Tha09a] Dinesh S. Thakur. Power sums with applications to multizeta and zeta zero distribution for $\mathbb{F}_q[t]$. *Finite Fields Appl.*, 15(4):534–552, 2009. 2

[Tha09b] Dinesh S. Thakur. Relations between multizeta values for $\mathbb{F}_q[t]$. *International Mathematics Research Notices*, 2009(12):2318–2346, June 2009. (document), 1.3, 1, 1, 1.5.1, 1.5.3, 1.5.3, 2.2, 2.3.17, 2.3.18, 2.3.22, 2.4, 2.4.7, 2.4.9, 2.4, 3, 2.5, a, 2.6, 2.6, 2.6, 2.6.3, 2, 1, 2, A.0.1

[Tha10] Dinesh S. Thakur. Shuffle Relations for Function Field Multizeta Values. *Int. Math. Res. Not. IMRN*, 2010(11):1973–1980, 2010. (document), 1.4, 2.2, 2.5, 3.1, 3.4.1, 3.5, A.0.1

[Tha12] Dinesh S. Thakur. personal communication, 2012. 3.4.1, 3.4.2

[Vil06] Gabriel Daniel Villa Salvador. *Topics in the theory of algebraic function fields*. Mathematics: Theory & Applications. Birkhäuser Boston Inc., Boston, MA, 2006. 1.2

[Wad41] L. I. Wade. Certain quantities transcendental over $GF(p^n, x)$. *Duke Math. J.*, 8:701–720, 1941. 1.2.2

[Wal00] Michel Waldschmidt. Valeurs zêta multiples. Une introduction. *J. Théor. Nombres Bordeaux*, 12(2):581–595, 2000. Colloque International de Théorie des Nombres (Talence, 1999). 3.5.1

[Wan96] Daqing Wan. On the Riemann hypothesis for the characteristic p zeta function. *J. Number Theory*, 58(1):196–212, 1996. 1.2, 1.2.2

[Wei40] André Weil. Sur les fonctions algébriques á corps de constantes fini. *C. R. Acad. Sci. Paris*, 210:592–594, 1940. 1.2

[Wei41] André Weil. On the Riemann hypothesis in function fields. *Proc. Nat. Acad. Sci. U. S. A.*, 27:345–347, 1941. 1.2

[Yu91] Jing Yu. Transcendence and special zeta values in characteristic p. *Ann. of Math. (2)*, 134(1):1–23, 1991. 1.2.2

[Zag93] Don Zagier. Periods of modular forms, traces of Hecke operators, and multiple zeta values. *Sūrikaisekikenkyūsho Kōkyūroku*, (843):162–170, 1993. Research into automorphic forms and L functions (Japanese) (Kyoto, 1992). 1.1.1

[Zag94] Don Zagier. Values of zeta functions and their applications. In *First European Congress of Mathematics, Vol. II (Paris, 1992)*, volume 120 of *Progr. Math.*, pages 497–512. Birkhäuser, Basel, 1994. 1.1, 1.1.1

[Zha00] Jianqiang Zhao. Analytic continuation of multiple zeta functions. *Proc. Amer. Math. Soc.*, 128(5):1275–1283, 2000. 1.1.1