"Construcción de Conjuntos B_h Modulares, $h = 2, 3, 4$"

JAVIER ALONSO RUIZ ORDÓÑEZ

UNIVERSIDAD DEL CAUCA
FACULTAD DE CIENCIAS NATURALES, EXACTAS Y DE LA EDUCACIÓN
DEPARTAMENTO DE MATEMÁTICAS
POPAYÁN, CAUCA
2011

"Construcción de Conjuntos B_h Modulares, $h = 2, 3, 4$"

JAVIER ALONSO RUIZ ORDÓÑEZ

Trabajo de grado en la modalidad "Trabajo de investigación"
presentado como requisito parcial para optar al título de
Matemático

Director:
Dr. CARLOS ALBERTO TRUJILLO SOLARTE

UNIVERSIDAD DEL CAUCA
FACULTAD DE CIENCIAS NATURALES, EXACTAS Y DE LA EDUCACIÓN
DEPARTAMENTO DE MATEMÁTICAS
POPAYÁN, CAUCA
2011

Nota de Aceptación

Dr. Carlos Alberto Trujillo Solarte
Director

Mg. Carlos Alexis Gómez Ruiz
Jurado

Profesor. Wilson Arley Martinez Flor
Jurado

Popayán, 10 de Marzo, 2011

Agradecimientos

Agradezco a mis padres y hermanos por brindarme el apoyo necesario durante este proceso.
A mi director, el maestro Carlos Alberto Trujillo Solarte, por permitirme trabajar en este proyecto, sus valiosos aportes, consejos y dedicación me han ayudado a crecer en todos los aspectos.
A mis Jurados Carlos Alexis Gómez, Wilson Arley Martinez y Diego Ruiz por el acompañamientos durante este proceso.
Por último a todos mis compañeros y amigos que durante estos años estuvieron a mi lado brindándome todo su apoyo.

Javier Ruiz

Introducción

El presente documento contiene el informe final del trabajo de grado titulado "Construcción de Conjuntos B_h Modulares, $h = 2, 3, 4$" realizado en la modalidad "Trabajo de investigación"por Javier Alonso Ruiz Ordóñez. Este trabajo se encuentra al interior del proyecto de investigación Conjuntos $B_3, B_4, B_2\,[2]$- Enteros y Modulares con código VRI: 2551, desarrollado por los profesores Carlos Alberto Trujillo, Jhon Jairo Bravo y Diego Ruiz.

Un conjunto de enteros A es un conjunto B_h, si para todo entero positivo n, existe a lo sumo una representación de la forma

$$n = a_1 + a_2 + \cdots + a_h \text{ con } a_1 \leq a_2 \leq \cdots \leq a_h \text{ y } a_i \in A.$$

Es decir, un conjunto A es B_h, si todas las posibles sumas de h de sus elementos, son distintas. Además, si $m \geq 2$ es entero, tal que las sumas de h elementos de A son todas incongruentes módulo m, se dice que A es un conjunto B_h módulo m.

Existen distintas maneras de construir conjuntos B_h módulo m, en este trabajo nos ocupamos de las construcciones que realizan I. Ruzsa en [1], R.C Bose y S. Chowla en [5], A. Gómez y C. Trujillo en [6].
Este documento se divide en cuatro capítulos y un apéndice. En el primer capítulo se define formalmente un conjunto B_h sobre grupos conmutativos, junto con la propiedad de invarianza bajo homomorfismos inyectivos la cual cumplen este tipo de conjuntos, y como requisito básico se presentan los polinomios simétricos elementales y las Identidades de Newton.

El capítulo 2, presenta la Construcción de conjuntos de Sidon módulo $p^2 - p$ debida a Imre Ruzsa, algunas extensiones y propiedades junto con un enfoque moderno para esta construcción.
El capítulo 3, presenta la Construcción de R.C Bose y S. Chowla, algunas propiedades y una versión moderna. El capítulo 4, consta de la Construcción Gómez-Trujillo y una Construcción nueva que utiliza potencias de elementos sobre campos finitos. Por último se presentan las conclusiones y los resultados importantes obtenidos en el desarrollo del trabajo. En el apéndice se presentan algunos resultados necesarios de la Teoría de Campos Finitos.

Índice general

CAPÍTULO 1

Preliminares

En este capítulo presentamos los conceptos, la notación y los resultados básicos que necesitamos para el desarrollo de los siguientes capítulos.

1.1. Conjuntos B_h

Sean $\langle G, + \rangle$ un grupo conmutativo notado aditivamente, y $A = \{a_1, \ldots, a_k\}$ un subconjunto de G y $h \geq 2$ un entero.
Decimos que A es **un conjunto** B_h **en** G, si todas las sumas de h elementos de A, no necesariamente distintos, son diferentes. Esto es, si todas las expresiones de la forma

$$a_{i_1} + \cdots + a_{i_h} \ ,$$

sujetas a la restricción

$$1 \leq i_1 \leq \cdots \leq i_h \leq k \ ,$$

producen elementos distintos en G. Cuando $h = 2$, esto es los conjuntos B_2 se llaman **conjuntos de Sidon**. Si A es un conjunto B_h en G se escribe $A \in B_h\,(G)$ y si A es un conjunto B_h en el grupo de los enteros módulo N, es decir en $\mathbb{Z}_N$, escribimos $A \in B_h(m\acute{o}d\ N)$. Como

nuestro grupo aditivo fundamental es el de los enteros módulo N, utilizamos aquí el sistema de representantes de mínimo residuo no negativo, es decir

$$\mathbb{Z}_N = \{0, 1, 2, \ldots, N-1\}.$$

Es conveniente tener en cuenta que algunas veces nos referimos y usamos un elemento $x \in \mathbb{Z}_N$ como si fuese un entero corriente, esto se hace en forma natural.
Definimos además el **conjunto suma** de A, notado $A + A$, como el conjunto de todas las sumas de dos elementos en A, es decir

$$A + A := \{x + y : x, y \in A\}.$$

En forma análoga, el **conjunto diferencia** de A, que se nota $A - A$, lo definimos como el conjunto de todas las diferencias de dos elementos en A, es decir

$$A - A := \{x - y : x, y \in A\}.$$

Según lo anterior, es claro que una forma alterna para definir un conjunto B_2 es la siguiente

$$A \in B_2 \text{ sobre } G, \text{ si y solo si, } |A + A| = \tbinom{|A|+1}{2}.$$

ó, equivalentemente

$$A \in B_2 \text{ sobre } G, \text{ si y solo si, } |A - A| = 2\tbinom{|A|}{2} + 1.$$

Aquí, hemos usado la notación $|X|$ para representar el cardinal del conjunto X.
La forma como procederemos para demostrar que un conjunto es B_h, consiste en suponer que existen dos h-sumas iguales:

$$x_1 + x_2 + \cdots + x_h = y_1 + y_2 + \cdots + y_h,$$

y probamos que los elementos que intervienen en cada uno de los lados son los mismos, es decir

$$\{x_1, x_2, \ldots, x_h\} = \{y_1, y_2, \ldots, y_h\}.$$

Ejemplo 1.1.1. El conjunto de los números primos es un conjunto B_h en $\mathbb{Z}^+$, con la operación producto definida usualmente.
En efecto, sean $p_1, p_2, \ldots, p_h,\ q_1, q_2, \ldots, q_h$ números primos en $\mathbb{Z}^+$ y supongamos que

$$p_1 p_2 \ldots p_h = q_1 q_2 \ldots q_h,$$

por la factorización única en $\mathbb{Z}^+$ sabemos que

$$\{p_1, p_2, \ldots, p_h\} = \{q_1, q_2, \ldots, q_h\},$$

y por tanto, la igualdad $p_1 p_2 \ldots p_h = q_1 q_2 \ldots q_h$ se tiene solamente si los primos que intervienen en el producto de la izquierda y los que intervienen en el producto de la derecha son los mismos (todo entero positivo se puede expresar como producto de primos en forma única, excepto por el orden de los factores).

Ejemplo 1.1.2. El conjunto

$$A := \left\{(x, \log x) : x \in \mathbb{R}^+\right\},$$

es un conjunto de Sidon en el grupo $\langle \mathbb{R} \times \mathbb{R}, + \rangle$.
De hecho, sean $a, b, c, d \in \mathbb{R}^+$ y supongamos que

$$(a, \log a) + (b, \log b) = (c, \log c) + (d, \log d),$$

se sigue entonces que

$$(a + b, \log a + \log b) = (c + d, \log c + \log d),$$

es decir

$$\begin{aligned} a + b &= c + d, \\ \log a + \log b &= \log c + \log d, \end{aligned}$$

por propiedades de la función logaritmo

$$\begin{aligned} a + b &= c + d, \\ \log(ab) &= \log(cd), \end{aligned}$$

dado que la función logaritmo es inyectiva, se obtiene

$$\begin{aligned} a + b &= c + d, \\ ab &= cd. \end{aligned}$$

Luego, los conjuntos $\{a,b\}$ y $\{c,d\}$ son raíces del mismo polinomio en $\mathbb{R}[x]$, de grado 2, esto es

$$x^2 - sx + p = (x-a)(x-b) = (x-c)(x-d),$$

donde $s = a+b = c+d$ y $p = ab = cd$.

Dado que $\mathbb{R}[x]$ es D.F.U. (Dominio de factorización única), tenemos que

$$\{a,b\} = \{c,d\}.$$

Ejemplo 1.1.3. El conjunto $B := \{(x,x^2) : x \in \mathbb{R}\}$ es un conjunto de Sidon en el grupo $\langle \mathbb{R}\times\mathbb{R}, +\rangle$.

Sean $a,b,c,d \in \mathbb{R}$, supongamos que

$$\left(a,a^2\right) + \left(b,b^2\right) = \left(c,c^2\right) + \left(d,d^2\right),$$

de donde,

$$\left(a+b, a^2+b^2\right) = \left(c+d, c^2+d^2\right),$$

es decir

$$a+b = c+d, \tag{1.1}$$

$$a^2+b^2 = c^2+d^2, \tag{1.2}$$

si tomamos el cuadrado en ambos lados de la igualdad (1.1) tenemos

$$(a+b)^2 = a^2+2ab+b^2 = c^2+2cd+d^2 = (c+d)^2, \tag{1.3}$$

de (1.2), aplicado en (1.3) se obtiene

$$2ab = 2cd.$$

Por tanto,

$$ab = cd \tag{1.4}$$

Luego, por (1.1) y (1.4) los conjuntos $\{a,b\}$ y $\{c,d\}$ tienen como elementos a las raíces del mismo polinomio de grado 2 en $\mathbb{R}[y]$, esto es

$$y^2 - my + n = (y-a)(y-b) = (y-c)(y-d),$$

donde $m = a+b = c+d$ y $n = ab = cd$. Puesto que $\mathbb{R}[y]$ es D.F.U. Tenemos

$$\{a,b\} = \{c,d\}.$$

1.2. Una propiedad importante

Una propiedad de gran importancia y utilidad durante el desarrollo de este trabajo, consiste en el hecho de ser conjunto B_h se preserva bajo homomorfismos inyectivos.

Lema 1.2.1. *Sean* $\langle G_1, + \rangle$ *y* $\langle G_2, * \rangle$ *grupos conmutativos y* $\varphi : G_1 \longrightarrow G_2$ *un homomorfismo inyectivo de grupos. Si* $A \in B_h(G_1)$ *entonces* $\varphi(A) \in B_h(G_2)$.

Prueba. Sean $a_1, \ldots, a_h \ , \ b_1, \ldots, b_h \in A$, supongamos que

$$\varphi(a_1) * \cdots * \varphi(a_h) \ = \ \varphi(b_1) * \cdots * \varphi(b_h),$$

como φ es un homomorfismo tenemos

$$\varphi(a_1 + \cdots + a_h) \ = \ \varphi(b_1 + \cdots + b_h) \ ,$$

por ser φ un homomorfismo inyectivo

$$a_1 + \cdots + a_h \ = \ b_1 + \cdots + b_h.$$

Ahora, como $A \in B_h(G_1)$ se tiene que

$$\{a_1, \ldots, a_h\} \ = \ \{b_1, \ldots, b_h\},$$

luego

$$\{\varphi(a_1), \ldots, \varphi(a_h)\} \ = \ \{\varphi(b_1), \ldots, \varphi(b_h)\},$$

así, $\varphi(A) \in B_h(G_2)$. □

1.3. Polinomios simétricos elementales

Definición 1.3.1. Los polinomios simétricos elementales en n variables $x_1, x_2, \ldots, x_n$ notados mediante

$$\sigma_k(x_1, x_2, \ldots, x_n), \text{ para } k = 0, 1, \ldots, n,$$

se definen como

$$\begin{aligned}
\sigma_0(x_1, x_2, \ldots, x_n) &= 1, \\
\sigma_1(x_1, x_2, \ldots, x_n) &= \sum_{1 \le j \le n} x_j, \\
\sigma_2(x_1, x_2, \ldots, x_n) &= \sum_{1 \le j < k \le n} x_j x_k, \\
&\vdots \\
\sigma_n(x_1, x_2, \ldots, x_n) &= \sum_{1 \le j_1 < j_2 < \ldots < j_k \le n} x_{j_1} \ldots x_{j_k} = x_1 x_2 \ldots x_n.
\end{aligned}$$

En general, para $k \geq 0$, definimos

$$\sigma_k(x_1, x_2, \ldots, x_n) = \sum_{1 \le j_1 < j_2 < \ldots < j_k \le n} x_{j_1} \ldots x_{j_k}.$$

Así, para cada entero positivo k, menor o igual que n, existe exactamente un polinomio simétrico[1] de grado k en n variables.

Ejemplo 1.3.1. Los n polinomios simétricos elementales para los primeros cuatro valores positivos de n (en todo caso $\sigma_0 = 1$, es uno de tales polinomios), son los siguientes:
Para $n = 1$

$$\sigma_1(x_1) = x_1.$$

Para $n = 2$

$$\begin{aligned}
\sigma_1(x_1, x_2) &= x_1 + x_2, \\
\sigma_2(x_1, x_2) &= x_1 x_2.
\end{aligned}$$

Para $n = 3$

$$\begin{aligned}
\sigma_1(x_1, x_2, x_3) &= x_1 + x_2 + x_3, \\
\sigma_2(x_1, x_2, x_3) &= x_1 x_2 + x_1 x_3 + x_2 x_3, \\
\sigma_3(x_1, x_2, x_3) &= x_1 x_2 x_3.
\end{aligned}$$

[1] Un polinomio $f \in R[x_1, x_2, \ldots, x_n]$, se llama simétrico si $f(x_{i_1}, x_{i_2}, \ldots, x_{i_n}) = f(x_1, x_2, \ldots, x_n)$ para cualquier permutación $i_1, i_2, \ldots, i_n$ de los enteros $1, 2, \ldots, n$.

Para $n = 4$

$$\begin{aligned}
\sigma_1(x_1, x_2, x_3, x_4) &= x_1 + x_2 + x_3 + x_4, \\
\sigma_2(x_1, x_2, x_3, x_4) &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4, \\
\sigma_3(x_1, x_2, x_3, x_4) &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4, \\
\sigma_4(x_1, x_2, x_3, x_4) &= x_1x_2x_3x_4.
\end{aligned}$$

Los polinomios simétricos elementales aparecen cuando expandimos un producto de factores lineales de un polinomio mónico:

$$\prod_{j=1}^{n}(\lambda - x_j) = \lambda^n - \sigma_1(x_1, x_2, \ldots, x_n)\lambda^{n-1} + \cdots + (-1)^n \sigma_n(x_1, x_2, \ldots, x_n).$$

Esto es, cuando substituimos las variables $x_1, x_2, \ldots, x_n$ por valores numéricos, obtenemos el polinomio mónico con variable λ cuyas raíces son los valores que substituyen a $x_1, x_2, \ldots, x_n$ y cuyos coeficientes son los polinomios simétricos elementales. Así, por ejemplo:

$$\begin{aligned}
&(\lambda - a)(\lambda - b)(\lambda - c)(\lambda - d) = \\
&\lambda^4 - (a + b + c + d)\lambda^3 + (ab + ac + ad + bc + bd + cd)\lambda^2 \\
&- (abc + abd + acd + bcd)\lambda + abcd.
\end{aligned}$$

1.4. Identidades de Newton y polinomios simétricos elementales

Las Identidades de Newton (fórmulas de Newton-Girard) nos permiten relacionar dos tipos de polinomios simétricos: las sumas de potencias y los polinomios simétricos elementales, en particular, nos permiten expresar recursivamente sumas de potencias en términos de polinomios simétricos elementales y recíprocamente. Estas identidades, evaluadas en las raíces de un polinomio mónico en una variable, nos permiten expresar las sumas de potencias k-ésimas de todas las raíces (contadas con multiplicidad) en términos de los coeficientes del polinomio, sin encontrar las raíces. Estas identidades fueron encontradas por Isaac Newton alrededor de 1666, ignorando aparentemente el trabajo anterior de Albert Girard (1629).

Sea $x_1, x_2, \ldots, x_n$ variables, denotamos mediante $p_k(x_1, x_2, \ldots, x_n)$ la suma de las potencias k-ésimas

$$p_k(x_1, x_2, \ldots, x_n) = x_1^k + \cdots + x_n^k = \sum_{i=1}^n x_i^k,$$

y para $k \geq 0$, $\sigma_k(x_1, x_2, \ldots, x_n)$ es el polinomio simétrico elemental (suma de todos los productos distintos de k variables distintas). Entonces las identidades de Newton pueden establecerse como

$$k\sigma_k(x_1, x_2, \ldots, x_n) = \sum_{i=1}^k (-1)^{i-1} \sigma_{k-i}(x_1, x_2, \ldots, x_n)\, p_i(x_1, x_2, \ldots, x_n),$$

valido para todo k, $1 \leq k \leq n$.

Concretamente, para los tres primeros valores de k tenemos:

$$\begin{aligned}
\sigma_1(x_1, x_2, \ldots, x_n) &= p_1(x_1, x_2, \ldots, x_n). \\
2\sigma_2(x_1, x_2, \ldots, x_n) &= \sigma_1(x_1, x_2, \ldots, x_n)\, p_1(x_1, x_2, \ldots, x_n) - p_2(x_1, x_2, \ldots, x_n). \\
3\sigma_3(x_1, x_2, \ldots, x_n) &= \sigma_2(x_1, x_2, \ldots, x_n)\, p_1(x_1, x_2, \ldots, x_n) \\
&\quad - \sigma_1(x_1, x_2, \ldots, x_n)\, p_2(x_1, x_2, \ldots, x_n) \\
&\quad + p_3(x_1, x_2, \ldots, x_n).
\end{aligned}$$

La forma y validez de estas ecuaciones no depende del número de variables (después de la n-ésima identidad el lado izquierdo se hace cero), esto hace posible establecer las identidades en el anillo de funciones simétricas. En tal anillo tenemos

$$\begin{aligned}
\sigma_1 &= p_1, \\
2\sigma_2 &= \sigma_1 p_1 - p_2, \\
3\sigma_3 &= \sigma_2 p_1 - \sigma_1 p_2 + p_3, \\
4\sigma_4 &= \sigma_3 p_1 - \sigma_2 p_2 + \sigma_1 p_3 - p_4,
\end{aligned}$$

y así sucesivamente; aquí el lado izquierdo nunca sera cero. Estas ecuaciones permiten expresar recursivamente los σ_i en términos de los p_k; Como también, expresar recursivamente los p_k en términos de los σ_i.

$$\begin{aligned}
p_1 &= \sigma_1, \\
p_2 &= \sigma_1 p_1 - 2\sigma_2, \\
p_3 &= \sigma_1 p_2 - \sigma_2 p_1 + 3\sigma_3, \\
p_4 &= \sigma_1 p_3 - \sigma_2 p_2 + \sigma_3 p_1 - 4\sigma_4.
\end{aligned}$$

CAPÍTULO 2

Construcción de conjuntos de Sidon módulo $p^2 - p$ (Ruzsa 1993)

En este capítulo presentamos la construcción de conjuntos de Sidon debida a Imre Ruzsa, junto con algunas extensiones y generalizaciones, analizamos algunas de sus propiedades e incluimos observaciones relacionadas con dicha construcción.

2.1. La construcción original de Ruzsa

En el artículo [1], Sección 4, Imre Ruzsa presenta varios resultados sobre conjuntos de Sidon; en particular, demuestra el siguiente teorema ([1], Teorema 4.4).

Teorema 2.1.1. (Ruzsa 1993). *Sea p un primo. Existe una colección $a_1, \ldots, a_{p-1}$ de $p-1$ enteros tales que las sumas $a_i + a_j$ son todas diferentes módulo $p(p-1)$. Es fácil ver que contando las diferencias $a_i - a_j$ no pueden haber p de tales números.*

Prueba. Sea g una raíz primitiva módulo p. Para $i = 1, \ldots, p-1$, sea a_i la solución de las congruencias

$$a_i \equiv i \ (mód\ p-1), \quad a_i \equiv g^i \ (mód\ p).$$

Nuestro objetivo es demostrar que para r arbitrario la congruencia

$$a_i + a_j \equiv r \ (mód\ p(p-1)), \tag{2.1}$$

tiene a lo sumo una solución en i, j (salvo permutación).
(2.1) es equivalente al sistema de dos congruencias

$$a_i + a_j \equiv r \ (mód \ (p-1)), \quad a_i + a_j \equiv r \ (mód \ p),$$

esto es

$$i + j \equiv r \ (mód \ (p-1)), \quad g^i + g^j \equiv r \ (mód \ p).$$

Los enteros $x_1 = g^i$, $x_2 = g^j$ satisfacen

$$x_1 + x_2 \equiv r \ (mód \ p), \quad x_1 x_2 \equiv g^r \ (mód \ p),$$

y en consecuencia $(x - x_1)(x - x_2)$ es la factorización del polinomio $x^2 - rx + g^r$ módulo p. De la unicidad de la factorización inferimos la unicidad de i, j salvo permutación. □

Ejemplo 2.1.1. Sean $p = 7, g = 3$. Resolviendo el sistema de congruencias

$$a_i \equiv i \ (mód \ 6)$$
$$a_i \equiv 3^i \ (mód \ 7)$$

para cada $i \in \{1, 2, 3, 4, 5, 6\}$, tenemos que el conjunto

$$\{2, 4, 5, 27, 31, 36\},$$

es un conjunto de Sidon módulo 42.

Comentario 2.1.1. Por el Teorema Chino de los restos, para cada $i = 1, 2, \ldots, p-1$ y cada g raíz primitiva módulo p, la única solución módulo $p(p-1)$ del sistema

$$a_i \equiv i \ (mód \ p-1), \quad a_i \equiv g^i \ (mód \ p),$$

viene dada por

$$a_i \equiv pi - g^i (p-1) \ (mód \ p(p-1)),$$

por lo tanto, el conjunto obtenido en la construcción de Ruzsa es:

$$R(p, g) := \{pi - g^i (p-1) \ (mód \ p(p-1)) : i = 1, 2, \ldots, p-1\}.$$

2.2. Una extensión de Lindström

En el artículo [2], Sección 4, Bernt Lindström afirma que él extiende la construcción de Ruzsa incluyendo un factor adicional en el sistema de las dos congruencias.
Sean u un entero tal que $1 \leq u \leq p-1$ y relativamente primo con $p-1$, y sea g una raíz primitiva módulo p. Lindström define el conjunto

$$R(p,u) := \left\{ pui + (p-1)\, g^i (mód\ p(p-1)) : 1 \leq i \leq p-1 \right\},$$

y demuestra el siguiente teorema ([2], Teorema 4.1).

Teorema 2.2.1. *$R(p,u)$ es un conjunto B_2 módulo $p(p-1)$.*

Prueba. Sea

$$pu(i+j) + (p-1)(g^i + g^j) \equiv a\ (mód\ p(p-1)),$$

la suma de dos elementos. Entonces encontramos

$$g^i + g^j \equiv -a\ (mód\ p), \tag{2.2}$$

y $u(i+j) \equiv a\ (mód\ p-1)$. Como u es relativamente primo con $p-1$, existe un entero h tal que $uh \equiv 1\ (mód\ p-1)$. Se sigue que $i+j \equiv ah\ (mód\ p-1)$ y por el pequeño teorema de Fermat tenemos

$$g^i g^j \equiv g^{ah}\ (mód\ p). \tag{2.3}$$

Por (2.2) y (2.3), g^i y g^j son las raíces de $X^2 + aX + g^{ah} = 0$ en $\mathbb{Z}_p$. De aquí, g^i y g^j son únicos y determinan unívocamente a $\{i,j\}$. □

Ejemplo 2.2.1. Sean $p = 7, g = 3, u \in \{1,5\}$, entonces:

$$R(7,1) = \{6, 10, 15, 23, 25, 26\},$$
$$R(7,5) = \{6, 11, 15, 37, 38, 40\}.$$

2.3. Una partición asociada con la construcción de Ruzsa

En el artículo [3], Teorema 2, los autores demuestran el siguiente resultado.

Teorema 2.3.1. *Para todo primo p existe una partición del intervalo entero $[1, p^2 - p]$ en p conjuntos $A_0, A_1, \ldots, A_{p-1}$. Cada conjunto tiene $p-1$ elementos, A_0 consiste de los múltiplos de p y A_i es un conjunto de Sidon módulo $p^2 - p$ para todo $i \neq 0$.*

Prueba. Sean p un primo, g una raíz primitiva módulo p, y v un entero tal que $0 \leq v \leq p-1$. Definimos $A_v = A(p, g, v) = \{x_1, x_2, \ldots, x_{p-1}\}$, donde para cada $i = 1, 2, \ldots, p-1$, x_i es la única solución de las congruencias

$$x_i \equiv i \ (mód\ p-1), \tag{2.4}$$

$$x_i \equiv vg^i \ (mód\ p), \tag{2.5}$$

con la condición que $1 \leq x_i \leq p^2 - p$. Es decir

$$A(p, g, v) := \{pi - vg^i (p-1) \ (mód\ p(p-1)) : i = 1, 2, \ldots, p-1\}.$$

Probemos que los conjuntos $A_0, A_1, \ldots, A_{p-1}$, satisfacen lo afirmado en el teorema.
Por definición, para todo $v \in \mathbb{Z}_p^*$, se cumple que

$$|A_v| = p - 1. \tag{2.6}$$

Mostremos que $A_0 = \{p, 2p, \ldots, p^2 - p\}$. De la definición de A_0, (2.4) y (2.5), con $v = 0$, tenemos:

$$x \in A_0 \Longleftrightarrow x_i \equiv i \ (mód\ p-1), \text{ para algún } i,\ 1 \leq i \leq p-1,\ x \equiv 0 \ (mód\ p)$$

$$\Longleftrightarrow x \text{ es múltiplo de } p \text{ y } 1 \leq x \leq p^2 - p.$$

Si $v \in \mathbb{Z}_p^*$, entonces A_v es un conjunto de Sidon módulo $p^2 - p$.
En efecto, sean $v \in \mathbb{Z}_p^*$, $a, b, c, d \in A_v$ si

$$a + b \equiv c + d \ (mód\ p^2 - p),$$

entonces

$$a + b \equiv c + d \ (mód\ p-1), \quad a + b \equiv c + d \ (mód\ p). \tag{2.7}$$

Ahora, por definición de A_v, existen i, j, s, t, $1 \leq i, j, s, t \leq p-1$, tales que:

$$a \equiv i \ (mód\ p-1) \text{ y } a \equiv ug^i \ (mód\ p),\ \ b \equiv j \ (mód\ p-1) \text{ y } b \equiv ug^j \ (mód\ p),$$

$$c \equiv s \ (mód\ p-1) \text{ y } c \equiv ug^s \ (mód\ p),\ \ d \equiv t \ (mód\ p-1) \text{ y } d \equiv ug^t \ (mód\ p).$$

De (2.7) tenemos

$$i + j \equiv s + t \ (mód\ p-1), \tag{2.8}$$

$$u\left(g^i + g^j\right) \equiv u\left(g^s + g^t\right) \ (mód\ p), \tag{2.9}$$

por (2.8) y (2.9) respectivamente se tiene

$$g^i g^j \equiv g^s g^t \ (mód\ p) \text{ y } g^i + g^j \equiv g^s + g^t \ (mód\ p),$$

lo cual es equivalente a tener

$$\left(X + g^i\right)\left(X + g^j\right) = \left(X + g^k\right)\left(X + g^l\right),$$

en el campo $\mathbb{Z}_p$, dado que $\mathbb{Z}_p[X]$ es D.F.U tenemos que

$$\{g^i, g^j\} = \{g^s, g^t\},$$

de donde

$$\{i, j\} = \{s, t\},$$

y por tanto

$$\{a, b\} = \{c, d\}.$$

Lo cual prueba que A_v es un conjunto de Sidon módulo $p^2 - p$.

Por ultimo, probemos que $P = \{A_v : v \in \mathbb{Z}_p\}$ es una partición de $[1, p^2 - p]$.

Sean $A_u, A_v \in P$ y $x \in A_u \cap A_v$, existe un k, con $1 \leq k \leq p-1$ tal que

$$x \in A_u \Rightarrow x \equiv k \ (mód\ p-1) \text{ y } \underbrace{x \equiv ug^k \ (mód\ p)}_{*}, \text{ y}$$

$$x \in A_v \Rightarrow x \equiv k \ (mód\ p-1) \text{ y } \underbrace{x \equiv vg^k \ (mód\ p)}_{**}.$$

Restando * y ** se tiene que $g^k[u - v] \equiv 0\ mód\ p)$ y como $u, v \in \mathbb{Z}_p$, entonces $u = v$.

Finalmente probemos que la unión de los A_v, con $v \in \mathbb{Z}_p$ es $[1, p^2 - p]$.

Como los A_v son disjuntos, por (2.6) tenemos

$$\left|\bigcup_{v \in \mathbb{Z}_p} A_v\right| = \sum_{v \in \mathbb{Z}_p} |A_v| = p(p-1) = p^2 - p.$$

Lo cual finaliza la prueba del teorema. □

Ejemplo 2.3.1. Sean $p = 7, g = 3$. Entonces

$$A_0 = A(7,3,0) = \{7,14,21,28,35,42\},$$
$$A_1 = A(7,3,1) = \{2,4,5,27,31,36\},$$
$$A_2 = A(7,3,2) = \{13,17,22,30,32,33\},$$
$$A_3 = A(7,3,3) = \{20,24,29,37,39,40\},$$
$$A_4 = A(7,3,4) = \{3,8,16,18,19,41\},$$
$$A_5 = A(7,3,5) = \{1,9,11,12,34,38\},$$
$$A_6 = A(7,3,6) = \{6,10,15,23,25,26\}.$$

Comentario 2.3.1. Es bastante claro que la construcción de Ruzsa corresponde al conjunto $A(p,g,1)$, es decir tomar $v = 1$ en la construcción anterior.

2.4. Extensión de Trujillo

Analizando la construcción de Ruzsa, la extensión de Lindström y la extensión dada en [3], Trujillo [4], observa que las extensiones anteriores se pueden combinar y generaliza como sigue. Sean p un primo, g una raíz primitiva módulo p, u un entero primo relativo con $p-1$ donde $1 \leq u \leq p-1$, y v un entero con $1 \leq v \leq p-1$. Definimos el siguiente conjunto

$$R(p,g,u,v) := \left\{pui - vg^i (p-1) \,(mód\ p(p-1)) : i = 1,2,\ldots,p-1\right\}. \tag{2.10}$$

Teorema A 1. *Con p, g, u, v definidos como antes, el conjunto $R(p,g,u,v)$ es un conjunto de Sidon módulo $p(p-1)$.*

Si ahora fijamos g y u, mientras permitimos que v varíe desde 0 hasta $p-1$, tenemos

Teorema A 2. *Para todo primo p, todo g raíz primitiva módulo p y todo entero u, primo relativo con $p-1$, la colección $\{R(p,g,u,v) : v = 0,1,\ldots,p-1\}$, es una partición del intervalo entero $[1, p^2-p]$, tal que: para todo $v \neq 0$, $R(p,g,u,v)$ es un conjunto de Sidon módulo $p(p-1)$, con $p-1$ elementos y $R(p,g,u,0) = \{p, 2p, \ldots, p(p-1)\}$.*

Ejemplo 2.4.1. Sean $p = 7, g = 3$. Entonces, el módulo es $m = 7 \times 6 = 42$. Y las particiones son las siguientes.

Para $u = 1$:

$$v = 0 : \{7, 14, 21, 28, 35, 42\},$$
$$v = 1 : \{2, 4, 5, 27, 31, 36\},$$
$$v = 2 : \{13, 17, 22, 30, 32, 33\},$$
$$v = 3 : \{20, 24, 29, 37, 39, 40\},$$
$$v = 4 : \{3, 8, 16, 18, 19, 41\},$$
$$v = 5 : \{1, 9, 11, 12, 34, 38\},$$
$$v = 6 : \{6, 10, 15, 23, 25, 26\}.$$

Para $u = 5$:

$$v = 0 : \{7, 14, 21, 28, 35, 42\},$$
$$v = 1 : \{16, 17, 19, 27, 32, 36\},$$
$$v = 2 : \{4, 8, 30, 31, 33, 41\},$$
$$v = 3 : \{1, 23, 24, 26, 34, 39\},$$
$$v = 4 : \{2, 3, 5, 13, 18, 22\},$$
$$v = 5 : \{9, 10, 12, 20, 25, 29\},$$
$$v = 6 : \{6, 11, 15, 37, 38, 40\}.$$

Ejemplo 2.4.2. Si en el Ejemplo 2.4.1, tomamos $g = 5$. Entonces, Las particiones son las siguientes.

Para $u = 1$:

$$v = 0 : \{7, 14, 21, 28, 35, 42\},$$
$$v = 1 : \{16, 17, 19, 27, 32, 36\},$$
$$v = 2 : \{4, 8, 30, 31, 33, 41\},$$
$$v = 3 : \{1, 23, 24, 26, 34, 39\},$$
$$v = 4 : \{2, 3, 5, 13, 18, 22\},$$
$$v = 5 : \{9, 10, 12, 20, 25, 29\},$$
$$v = 6 : \{6, 11, 15, 37, 38, 40\}.$$

Para $u = 5$:

$$v = 0 : \{7, 14, 21, 28, 35, 42\},$$
$$v = 1 : \{2, 4, 5, 27, 31, 36\},$$
$$v = 2 : \{13, 17, 22, 30, 32, 33\},$$
$$v = 3 : \{20, 24, 29, 37, 39, 40\},$$
$$v = 4 : \{3, 8, 16, 18, 19, 41\},$$
$$v = 5 : \{1, 9, 11, 12, 34, 38\},$$
$$v = 6 : \{6, 10, 15, 23, 25, 26\}.$$

2.5. Propiedades especiales de esta construcción

Presentamos ahora algunas propiedades de esta construcción:

Lema 2.5.1. *Para todo $a \in R(p, g, u, v)$, como se define en (2.10), tenemos $a \not\equiv 0 \ (mód\ p)$.*

Prueba. Sea $a \in R(p, g, u, v)$, entonces existe $i \in [1, p-1]$ tal que

$$a = pui - vg^i (p-1) \ (mód\ p(p-1)),$$

de aquí

$$a \equiv vg^i \ (mód\ p),$$

como ni v, ni g^i es cero módulo p, se sigue que $a \not\equiv 0 \ (mód\ p)$.

□

Teorema 2.5.1. *Sean, p un primo, g una raíz primitiva módulo p, u entero primo relativo con $p-1$, v entero no divisible entre p. Definimos*

$$A = R(p, g, u, v) := \{a_1, a_2, \ldots, a_{p-1}\},$$

donde cada a_i, $1 \leq i \leq p-1$, satisface el sistema de congruencias

$$a_i \equiv ui \ (mód\ p-1), \quad a_i \equiv vg^i \ (mód\ p);$$

Y

$$M_p := \{p, 2p, \ldots, (p-2)\, p\}\,,$$
$$M_{p-1} := \{p-1, 2\,(p-1)\,, \ldots, (p-1)\,(p-1)\}\,.$$

Entonces $\{A-A, M_p, M_{p-1}\}$ *es una partición de* $\mathbb{Z}_{p(p-1)}$.

Prueba. Primero probemos que los conjuntos $A-A, M_p$ y M_{p-1} son disjuntos por pares. Por definición, $M_p \cap M_{p-1} = \emptyset$.
Si $x \in (A-A) \cap M_p$, entonces existen $i, j \in [1, p-1]$ tales que

$$\begin{aligned} x &= a_i - a_j \\ &\equiv g^i - g^j \\ &\equiv 0(m\acute{o}d\ p), \end{aligned}$$

de donde $i = j$ y $a_i = a_j$, y así $x = 0$, lo que no es posible ya que $0 \notin M_p$. Así que $(A-A) \cap M_p = \emptyset$.
Si $x \in (A-A) \cap M_{p-1}$, entonces existen $i, j \in [1, p-1]$ tales que

$$\begin{aligned} x &= a_i - a_j \\ &\equiv i - j \\ &\equiv 0\ (m\acute{o}d\ p-1), \end{aligned}$$

de donde $i = j$ y $a_i = a_j$, y así $x = 0$, lo que no es posible porque $0 \notin M_{p-1}$. Así que $(A-A) \cap M_{p-1} = \emptyset$.
Ahora demostremos que $A - A = \mathbb{Z}_{p(p-1)} \setminus (M_p \cup M_{p-1})$.
Como A es un conjunto de Sidon con $(p-1)$ elementos tenemos

$$\begin{aligned} |A-A| &= 2\binom{p-1}{2} + 1 \\ &= (p-1)\,(p-2) + 1 \\ &= p^2 - 3p + 3, \end{aligned}$$

y como los tres conjuntos son disjuntos por pares, se sigue que

$$\begin{aligned} p\,(p-1) &= \left|\mathbb{Z}_{p(p-1)}\right| \\ &\geq |A-A| + |M_p \cup M_{p-1}| \\ &\geq p^2 - 3p + 3 + 2p - 3 \\ &\geq p^2 - p, \end{aligned}$$

lo que permite concluir la demostración. □

Comentario 2.5.1. No importa quienes son g, u, v el conjunto $A - A$ es fijo:

$$A - A = \mathbb{Z}_{p(p-1)} \setminus (M_p \cup M_{p-1}).$$

Ejemplo 2.5.1. Del Ejemplo 2.4.1, $A = R\,(7,3,1,1) = \{2,4,5,27,31,36\}$, así:

2	4	5	27	31	36
0	2	3	25	29	34
40	0	1	23	27	32
39	41	0	22	26	31
17	19	20	0	4	9
13	15	16	38	0	5
8	10	11	33	37	0

$$A - A = \mathbb{Z}_{42} \setminus \{6,7,12,14,18,21,24,28,30,35,36\}.$$

2.6. Construcción en dos dimensiones

La construcción anterior se puede mirar como si fuese en dos dimensiones, esto es, en el grupo aditivo, (componente a componente)

$$G = \mathbb{Z}_{(p-1)} \times \mathbb{Z}_p.$$

Sea p un número primo,$\mathbb{U}_p$ el grupo multiplicativo de unidades módulo p[1] y g una raíz primitiva módulo p, esto es :

[1] Por notación identificaremos a $\mathbb{U}_p$ con $\mathbb{Z}_p^*$

$$\langle g\rangle = \{g, g^2, \ldots, g^{p-1} = 1\} = \mathbb{U}_p,$$

además consideremos $u \in \mathbb{U}_n$, y $v \in \mathbb{U}_p$, donde $\mathbb{U}_n$ representan el grupo de unidades módulo n. Definimos el conjunto

$$R\left(p, g, u, v\right) = \{(ui, vg^i) : i = 1, 2, \ldots, p-1\} \subseteq G.$$

A continuación presentamos el teorema sobre la construcción de la sección anterior, vista en dos dimensiones:

Teorema 2.6.1. *Para todo primo p y todo g generador de $\mathbb{Z}_p^*$, tenemos que $R\left(p, g, u, v\right)$ es un conjunto de Sidon en el grupo $\langle \mathbb{Z}_{p-1} \times \mathbb{Z}_p, +\rangle$.*

Prueba. Sean $(ui, vg^i), (uj, vg^j), (uk, vg^k), (ul, vg^l) \in R\left(p, g, u, v\right)$, supongamos que

$$(ui, vg^i) + (uj, vg^j) = (uk, vg^k) + (ul, vg^l),$$

esto es

$$\left(u\left(i+j\right), v(g^i + g^j)\right) = \left(u\left(k+l\right), v(g^k + g^l)\right),$$

luego

$$\begin{aligned} u\left(i+j\right) &\equiv u\left(k+l\right)\left(mód\ p-1\right), \\ v\left(g^i + g^j\right) &\equiv v\left(g^k + g^l\right)\ \left(mód\ p\right), \end{aligned}$$

dado que $u \in \mathbb{U}_{p-1}$, y $v \in \mathbb{Z}_p^*$ tenemos,

$$\left(i+j\right) \equiv \left(k+l\right)\left(mód\ p-1\right), \tag{2.11}$$

$$\left(g^i + g^j\right) \equiv \left(g^k + g^l\right)\ \left(mód\ p\right), \tag{2.12}$$

de (2.11),

$$g^{i+j} \equiv g^{k+l}\ \left(mód\ p\right). \tag{2.13}$$

Esto es válido por la siguiente propiedad:

$$i \equiv j\ \left(mód\ p-1\right)\ \Leftrightarrow\ g^i \equiv g^j\ \left(mód\ p\right).$$

De (2.13)

$$g^i g^j \equiv g^k g^l\ \left(mód\ p\right),$$

por tanto, obtenemos el sistema de congruencias

$$\left(g^i + g^j\right) \equiv \left(g^k + g^l\right) (mód\ p),$$
$$g^i g^j \equiv g^k g^l\ (mód\ p),$$

lo cual es equivalente a tener

$$\left(X + g^i\right)\left(X + g^j\right) = \left(X + g^k\right)\left(X + g^l\right),$$

en virtud de que $\mathbb{Z}_p[X]$, es D.F.U, tenemos que

$$\{g^i, g^j\} = \left\{g^k, g^l\right\},$$

de donde

$$\{i, j\} = \{k, l\},$$

y por tanto

$$\{(ui, vg^i)\ ,\ (uj, vg^j)\} = \left\{(uk, vg^k)\ ,\ (ul, vg^l)\right\}.$$

□

Ejemplo 2.6.1. $p = 7, g = 3$

$$R(7,3,1,1) = \{(1,3),(2,2),(3,6),(4,4),(5,5),(0,1)\},$$
$$R(7,3,1,2) = \{(1,6),(2,4),(3,5),(4,1),(5,3),(0,2)\},$$
$$R(7,3,1,3) = \{(1,2),(2,6),(3,4),(4,5),(5,1),(0,3)\},$$
$$R(7,3,1,4) = \{(1,5),(2,1),(3,3),(4,2),(5,6),(0,4)\},$$
$$R(7,3,1,5) = \{(1,1),(2,3),(3,2),(4,6),(5,4),(0,5)\},$$
$$R(7,3,1,6) = \{(1,4),(2,5),(3,1),(4,3),(5,2),(0,6)\}.$$

Comentario 2.6.1. $R(p,g,u,v)$ es un conjunto de Sidon en el grupo $\langle \mathbb{Z}_{p-1} \times \mathbb{Z}_p, + \rangle$, el cual por el Teorema Chino de los restos es isomorfo a $\left\langle \mathbb{Z}_{(p-1)p}, + \right\rangle$, por lo tanto, usando el Lema 1.2.1 y el isomorfismo

$$\tau : \mathbb{Z}_{p-1} \times \mathbb{Z}_p \longrightarrow \mathbb{Z}_{(p-1)p},$$

definido mediante

$$\tau(a,b) \ = x,$$

donde x es la única solución del sistema

$$x \equiv a \ (mód\ p-1),$$
$$x \equiv b \ (mód\ p),$$

obtenemos un conjunto de Sidon módulo $(p-1)\,p$, este es el conjunto

$$\tau(R\,(p,g,u,v)).$$

Esto corresponde a la construcción de Ruzsa y sus generalizaciones.

Ejemplo 2.6.2. Del ejemplo 2.6.1 y el comentario anterior, tomando $R_v = \tau(R\,(7,3,1,v))$ tenemos

$$R_1 = \{2,4,5,27,31,36\}\,,$$
$$R_2 = \{13,17,22,30,32,33\}\,,$$
$$R_3 = \{20,24,29,37,39,40\}\,,$$
$$R_4 = \{3,8,16,18,19,41\}\,,$$
$$R_5 = \{1,9,11,12,34,38\}\,,$$
$$R_6 = \{6,10,15,23,25,26\}\,.$$

2.7. Versión Moderna

Una manera nueva de observar esta construcción, consiste en considerar el siguiente conjunto

$$R := \left\{(x, \log_\theta x) : x \in \mathbb{F}_q^*\right\} \subseteq \mathbb{F}_q \times \mathbb{Z}_{q-1},$$

donde q es una potencia prima y θ es un elemento primitivo de $\mathbb{F}_q$. ([8], Definición 2.9).

Teorema 2.7.1. *R es un conjunto de Sidon en el grupo $\langle \mathbb{F}_q \times \mathbb{Z}_{q-1}, + \rangle$. Donde la operación suma es componente a componente.*

Prueba. Consideremos $a, b, c, d \in \mathbb{F}_q^*$, y supongamos que

$$(a, \log_\theta a) + (b, \log_\theta b) = (c, \log_\theta c) + (d, \log_\theta d)\,,$$

se sigue que

$$a + b = c + d \quad (\text{en } \mathbb{F}_q), \tag{2.14}$$

$$\log_\theta (ab) = \log_\theta (cd) \quad (\text{en } \mathbb{Z}_{q-1}), \tag{2.15}$$

dado que la función logaritmo discreto[2]es inyectiva, se tiene

$$ab = cd \quad (\text{en } \mathbb{F}_q), \tag{2.16}$$

de (2.14) y (2.16) obtenemos que los conjuntos $\{a, b\}$ y $\{c, d\}$ son los conjuntos de raíces de un polinomio mónico de grado dos, $s(x)$ en $\mathbb{F}_q[x]$, por la factorización única, obtenemos que

$$\{a, b\} = \{c, d\}.$$

De aquí, R es un conjunto de Sidon en el grupo $\langle \mathbb{F}_q \times \mathbb{Z}_{q-1}, + \rangle$. □

Como el teorema anterior es válido para toda potencia prima $q = p^n$ y como el grupo aditivo $\langle \mathbb{F}_{p^n}, + \rangle$ es claramente isomorfo al grupo $\langle \mathbb{F}_p^n, + \rangle$, tenemos el siguiente resultado.

Teorema 2.7.2. *Para todo primo p y todo entero positivo n, existe un conjunto de Sidon en el grupo $\langle \mathbb{F}_p^n \times \mathbb{Z}_{p^n-1}, + \rangle$, con $p^n - 1$ elementos.*

Prueba. Se sigue inmediatamente del isomorfismo entre los grupos

$$\langle \mathbb{F}_{p^n} \times \mathbb{Z}_{p^n-1}, + \rangle \text{ y } \langle \mathbb{F}_p^n \times \mathbb{Z}_{p^n-1}, + \rangle,$$

y la construccion del teorema anterior.
Específicamente, todo $\alpha \in \mathbb{F}_{p^n}$ puede verse como una n-tupla de elementos en $\mathbb{F}_p$. Identificamos a

$$\alpha = a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}, \quad a_i \in \mathbb{F}_p,$$

con

$$\phi(\alpha) = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_p^n.$$

[2]La función $\log_\theta : \mathbb{F}_q^* \longrightarrow \mathbb{Z}_{q-1}$ es un isomorfismo, llamado Logaritmo Discreto.

□

Es claro que si, en el teorema anterior, tomamos $n = 1$, se obtiene la construcción de Ruzsa.

Ejemplo 2.7.1. Consideramos el campo $\mathbb{F}_3 = \{0, 1, 2\}$ y construyamos el campo $\mathbb{F}_{3^2} = \mathbb{F}_9$, para ello utilicemos el polinomio irreducible sobre $\mathbb{F}_9$ de grado 2, $P(x) = x^2 + x + 2$; Luego

$$\begin{aligned}\mathbb{F}_3[x] / \left(x^2 + x + 2\right) \cong \mathbb{F}_{3^2} = \mathbb{F}_9 &= \{a + b\theta : a, b \in \mathbb{F}_3\} \\ &= \{0, 1, 2, \theta, 2\theta, 1 + \theta, 1 + 2\theta, 2 + \theta, 2 + 2\theta\}.\end{aligned}$$

Donde θ es raíz del polinomio $P(x)$, $\theta^2 = -\theta - 2 = 2\theta + 1$ la cual resulta ser un elemento primitivo de $\mathbb{F}_9$, es decir $\langle\theta\rangle = \mathbb{F}_9^*$. Las potencias de θ se presentan en la siguiente tabla:

k	1	2	3	4	5	6	7	8
θ^k	θ	$2\theta + 1$	$2\theta + 2$	2	2θ	$\theta + 2$	$\theta + 1$	1

de donde obtenemos el conjunto B_2 en el grupo $\langle\mathbb{F}_9 \times \mathbb{Z}_8, +\rangle$

$$R = \{(\theta, 1), (2\theta + 1, 2), (2\theta + 2, 3), (2, 4), (2\theta, 5), (\theta + 2, 6), (\theta + 1, 7), (1, 0)\},$$

con conjunto suma $R + R$

$(\theta, 1)$	$(2\theta + 1, 2)$	$(2\theta + 2, 3)$	$(2, 4)$	$(2\theta, 5)$	$(\theta + 2, 6)$	$(\theta + 1, 7)$	$(1, 0)$
$(2\theta, 2)$	$(1, 3)$	$(2, 4)$	$(\theta + 2, 5)$	$(0, 6)$	$(2\theta + 2, 7)$	$(2\theta + 1, 0)$	$(\theta + 1, 1)$
	$(\theta + 2, 4)$	$(\theta, 5)$	$(2\theta, 6)$	$(\theta + 1, 7)$	$(0, 0)$	$(2, 1)$	$(2\theta + 2, 2)$
		$(\theta + 1, 6)$	$(2\theta + 1, 7)$	$(\theta + 2, 0)$	$(1, 1)$	$(0, 2)$	$(2\theta, 3)$
			$(1, 0)$	$(2\theta + 2, 1)$	$(\theta + 1, 2)$	$(\theta, 3)$	$(0, 4)$
				$(\theta, 2)$	$(2, 3)$	$(1, 4)$	$(2\theta + 1, 5)$
					$(2\theta + 1, 4)$	$(2\theta, 5)$	$(\theta, 6)$
						$(2\theta + 2, 6)$	$(\theta + 2, 7)$
							$(2, 0)$

Utilizando el isomorfismo natural entre $\langle\mathbb{F}_{3^2}, +\rangle$ y $\langle\mathbb{F}_3^2, +\rangle$, abusando un poco de la notación, obtenemos el conjunto

$$A := \widetilde{\phi}(R) = \{(0, 1, 1), (1, 2, 2), (2, 2, 3), (2, 0, 4), (0, 2, 5), (2, 1, 6), (1, 1, 7), (1, 0, 0)\},$$

donde

$$\begin{aligned} \widetilde{\phi} = (\phi, i_d) : \mathbb{F}_{p^n} \times \mathbb{Z}_{p^n-1} &\longrightarrow \mathbb{F}_p^n \times \mathbb{Z}_{p^n-1}, \\ \left(a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}, m\right) &\longmapsto (a_0, a_1, \ldots, a_{n-1}, m) \end{aligned}$$

por lo cual A es un conjunto B_2 en el grupo $\langle \mathbb{F}_3 \times \mathbb{F}_3 \times \mathbb{Z}_8, + \rangle$.

Y su conjunto suma $A + A$ es

$(0,1,1)$	$(1,2,2)$	$(2,2,3)$	$(2,0,4)$	$(0,2,5)$	$(2,1,6)$	$(1,1,7)$	$(1,0,0)$
$(0,2,2)$	$(1,0,3)$	$(2,0,4)$	$(2,1,5)$	$(0,0,6)$	$(2,2,7)$	$(1,2,0)$	$(1,1,1)$
	$(2,1,4)$	$(0,1,5)$	$(0,2,6)$	$(1,1,7)$	$(0,0,0)$	$(2,0,1)$	$(2,2,2)$
		$(1,1,6)$	$(1,2,7)$	$(2,1,0)$	$(1,0,1)$	$(0,0,2)$	$(0,2,3)$
			$(1,0,0)$	$(2,2,1)$	$(1,1,2)$	$(0,1,3)$	$(0,0,4)$
				$(0,1,2)$	$(2,0,3)$	$(1,0,4)$	$(1,2,5)$
					$(1,2,4)$	$(0,2,5)$	$(0,1,6)$
						$(2,2,6)$	$(2,1,7)$
							$(2,0,0)$

El conjunto diferencia de A esta dado por:

$(0,1,1)$	$(1,2,2)$	$(2,2,3)$	$(2,0,4)$	$(0,2,5)$	$(2,1,6)$	$(1,1,7)$	$(1,0,0)$
$(0,0,0)$	$(1,1,1)$	$(2,1,2)$	$(2,2,3)$	$(0,1,4)$	$(2,0,5)$	$(1,0,6)$	$(1,2,7)$
$(2,2,7)$	$(0,0,0)$	$(1,0,1)$	$(1,1,2)$	$(2,0,3)$	$(1,2,4)$	$(0,2,5)$	$(0,1,6)$
$(1,2,6)$	$(2,0,7)$	$(0,0,0)$	$(0,1,1)$	$(1,0,2)$	$(0,2,3)$	$(2,2,4)$	$(2,1,5)$
$(1,1,5)$	$(2,2,6)$	$(0,2,7)$	$(0,0,0)$	$(1,2,1)$	$(0,1,2)$	$(2,1,3)$	$(2,0,4)$
$(0,2,4)$	$(1,0,5)$	$(2,0,6)$	$(2,1,7)$	$(0,0,0)$	$(2,2,1)$	$(1,2,2)$	$(1,1,3)$
$(1,0,3)$	$(2,1,4)$	$(0,1,5)$	$(0,2,6)$	$(1,1,7)$	$(0,0,0)$	$(2,0,1)$	$(2,2,2)$
$(2,0,2)$	$(0,1,3)$	$(1,1,4)$	$(1,2,5)$	$(2,1,6)$	$(1,0,7)$	$(0,0,0)$	$(0,2,1)$
$(2,1,1)$	$(0,2,2)$	$(1,2,3)$	$(1,0,4)$	$(2,2,5)$	$(1,1,6)$	$(0,1,7)$	$(0,0,0)$

Según la tabla anterior, notamos que

$$A - A = \mathbb{F}_3^2 \times \mathbb{Z}_8 \setminus \{(a,0) : a \in \mathbb{F}_3^2\} \cup \{(0,b) : b \in \mathbb{Z}_8,\ 0 \in \mathbb{F}_3^2\}.$$

2.8. Algoritmos en MuPad

2.8.1. Algoritmo 2.1

Este algoritmo calcula el conjunto de Sidon módulo $m = p(p-1)$, con $p-1$ elementos, según la construcción generalizada de Ruzsa, Teorema A 1. Aquí, p es un primo, g es una raíz primitiva módulo p, $1 \leq f \leq p-1$ con $mcd(f, p-1) = 1$, y $1 \leq u \leq p-1$.

```
ruzsa := proc(p,g,f,u)
local A, t, p1, m;
begin
p1:= p-1; m:= p*p1; A:= {};
for i from 1 to p1 do
     t:= [p*f*i - u*(p-1)*(g^i)] mod m;
     A:= {op(A),t};
end_for;
end_proc;
```

2.8.2. Algoritmo 2.2

Este algoritmo calcula una partición del intervalo entero $[1, m]$, de acuerdo con el Teorema A 2. Aquí, p es un primo, g es una raíz primitiva módulo p, $1 \leq f \leq p-1$, primo relativo con $p-1$ y $m = p(p-1)$.

```
partiruzsa:= proc(p,g,f)
local p1, L, u;
begin
p1:= p-1; L:=[];
for u from 0 to p1 do
L:=[op(L),ruzsa(p,g,f,u)];
end_for;
end_proc;
```

CAPÍTULO 3

Construcción de Bose y Chowla (1962-63)

En este capítulo presentamos la construcción de conjuntos B_h debida a Bose y Chowla, junto con una extensión, y algunas propiedades.

3.1. La construcción original de Bose y Chowla

En el artículo [5], sección 2, los autores prueban, entre otros resultados, el siguiente teorema.

Teorema 3.1.1. *Si $m = p^n$ (donde p es primo), podemos encontrar m enteros no cero (menores que m^r)*

$$d_1 = 1, d_2, \ldots, d_m,$$

tales que las sumas

$$d_{i_1} + d_{i_2} + \cdots + d_{i_r},$$

$1 \leq i_1 \leq i_2 \leq \ldots \leq i_r \leq m$, *son todas diferentes módulo* $(m^r - 1)$.

Prueba. Sean $\alpha_1 = 0, \alpha_2, \ldots, \alpha_m$ todos los diferentes elementos del campo $\mathbb{F}_{p^n}$. Sea x un elemento primitivo del campo extensión $\mathbb{F}_{p^{nr}}$.
Entonces x no puede satisfacer alguna ecuación de grado menor que r con coeficientes en

$\mathbb{F}_{p^n}$. Sean

$$x^{d_i} = x + \alpha_i, \quad i = 1, 2, \ldots, m; \quad d_i < p^{nr} \ , \tag{3.1}$$

entonces el conjunto de enteros requerido es

$$d_1 = 1, d_2, \ldots, d_m.$$

si fuese posible tener

$$d_{i_1} + d_{i_2} + \cdots + d_{i_r} \equiv d_{j_1} + d_{j_2} + \cdots + d_{j_r} \ (m\acute{o}d\ m^r - 1),$$

donde $1 \leq i_1 \leq i_2 \leq \ldots \leq i_r \leq m$; $1 \leq j_1 \leq j_2 \leq \ldots \leq j_r \leq m$, y

$$(i_1, i_2, \ldots, i_r) \neq (j_1, j_2, \ldots, j_r)\,;$$

entonces

$$x^{d_{i_1}} x^{d_{i_2}} \ldots x^{d_{i_r}} = x^{d_{j_1}} x^{d_{j_2}} \ldots x^{d_{j_r}}.$$

De aquí, por (3.1)

$$(x + \alpha_{i_1})\,(x + \alpha_{i_2}) \ldots (x + \alpha_{i_r}) = (x + \alpha_{j_1})\,(x + \alpha_{j_2}) \ldots (x + \alpha_{j_r})\,.$$

Después de cancelar la máxima potencia de x en ambos lados nos quedamos con una ecuación de grado a lo sumo $(r-1)$ en x, con coeficientes en $GF(p^n)$, lo cual es imposible. De aquí el teorema. □

Comentario 3.1.1. Analizando la demostración original, podemos detallar un poco la construcción que realizan Bose y Chowla.
Sean q una potencia de un primo, $\mathbb{F}_q = \{\alpha_1 = 0, \alpha_2, \ldots, \alpha_q\}$ un campo finito con q elementos, θ un elemento primitivo del campo finito $\mathbb{F}_{q^h}$, es decir θ es un generador del grupo multiplicativo de unidades de este campo, en particular el grado de θ sobre $\mathbb{F}_q$ es h (h es el grado del polinomio mínimal de θ sobre $\mathbb{F}_q$). Por (3.1), los q enteros que se escogen para formar el conjunto B_h módulo $q^h - 1$, vienen determinados por la ecuación

$$\theta^{d_i} = \theta + \alpha_i, \ \text{ para } i = 1, 2, \ldots, q,$$

es decir, se trata de escoger q enteros $d_i \in \left[1, q^h - 1\right]$, recordemos que el orden de θ es el cardinal del grupo, esto es $q^h - 1$, para los cuales

$$\theta^{d_i} - \theta = \alpha_i, \text{ para } i = 1, 2, \ldots, q,$$

es decir

$$\theta^{d_i} - \theta \in \mathbb{F}_q,$$

de otra forma, se escogen los enteros $a \in \left[1, q^h - 1\right]$, tales que

$$\theta^a - \theta \in \mathbb{F}_q.$$

En la siguiente sección haremos uso de este comentario.

3.2. Versión Moderna

En esta sección, presentamos una versión generalizada del Teorema 3.1.1, la cual construye conjuntos B_h sobre un campo arbitrario. Iniciemos entonces considerando el siguiente ejemplo

Ejemplo 3.2.1. Afirmamos que el conjunto

$$\sqrt{2} + \mathbb{Q} := \left\{\sqrt{2} + a : a \in \mathbb{Q}\right\},$$

es un conjunto B_2 en el grupo multiplicativo $\left(\mathbb{Q}\left(\sqrt{2}\right)^*, \cdot\right)$. En efecto, sean $a, b, c, d \in \mathbb{Q}$ y supongamos que

$$\left(\sqrt{2} + a\right)\left(\sqrt{2} + b\right) = \left(\sqrt{2} + c\right)\left(\sqrt{2} + d\right),$$
$$\sqrt{2}\,(a + b) + ab = \sqrt{2}\,(c + d) + cd,$$

esto es

$$((a + b) - (c + d))\,\sqrt{2} + (ab - cd) = 0\ .$$

De donde

$$a + b = c + d \text{ y } \ ab = cd,$$

y de aquí $\{a, b\} = \{c, d\}$. En consecuencia

$$\left\{\sqrt{2} + a, \sqrt{2} + b\right\} = \left\{\sqrt{2} + c, \sqrt{2} + d\right\};$$

y así $\sqrt{2}+\mathbb{Q}$ es un conjunto B_2 en $\left(\mathbb{Q}\left(\sqrt{2}\right)^*,\cdot\right)$.

Esta situación puede generalizarse como sigue.

Consideremos ahora $\mathbb{K},\mathbb{F}$ campos tales que $\mathbb{K}\subseteq\mathbb{F}$, es decir $\mathbb{F}$ es una extensión de $\mathbb{K}$. Es claro que $\mathbb{F}$ se puede ver como un espacio vectorial sobre $\mathbb{K}$, cuya dimensión se denota como $[\mathbb{F}:\mathbb{K}]=\dim_{\mathbb{K}}\mathbb{F}$. Para nuestro propósito supongamos que $[\mathbb{F}:\mathbb{K}]=n\geq 2$.

Si $\alpha\in\mathbb{F}$ y $\alpha\notin\mathbb{K}$, $\mathbb{K}(\alpha)$ es el menor subcampo de $\mathbb{F}$ tal que $\alpha\in\mathbb{K}(\alpha)$ y $\mathbb{K}\subseteq\mathbb{K}(\alpha)$.

$$\begin{array}{c}\mathbb{F}\\ |\\ \mathbb{K}(\alpha)\\ |\\ \mathbb{K}\end{array}$$

Sea $h=[\mathbb{K}(\alpha):\mathbb{K}]$, sabemos que $h\mid n$ y $h\geq 2$ (h es el grado de α sobre $\mathbb{K}$) definimos el conjunto

$$A(\alpha,\mathbb{K}):=\alpha+\mathbb{K}:=\{\alpha+a:a\in\mathbb{K}\}\subseteq\mathbb{K}(\alpha),\ \alpha\notin\mathbb{K}.$$

Con esta notación, enunciamos entonces nuestro siguiente teorema.

Teorema 3.2.1. *Si $[\mathbb{K}(\alpha):\mathbb{K}]=h$, entonces $A(\alpha,\mathbb{K})$ es un conjunto B_h en el grupo multiplicativo $\mathbb{K}(\alpha)^*$.*

Prueba. Sean $a_1,a_2\ldots,a_h$ y $b_1,b_2\ldots,b_h$ elementos en $\mathbb{K}$, y supongamos que

$$(\alpha+a_1)(\alpha+a_2)\cdots(\alpha+a_h)\ =(\alpha+b_1)(\alpha+b_2)\cdots(\alpha+b_h),$$

esto es

$$\prod_{k=1}^{h}(\alpha+a_k)\ =\ \prod_{k=1}^{h}(\alpha+b_k)\ .$$

Sabemos que,

$$\prod_{k=1}^{h}(X+t_k)=X^h+\sigma_1(t)X^{h-1}+\sigma_2(t)X^{h-2}+\cdots+\sigma_{h-1}(t)X+\sigma_h(t),$$

donde $\sigma_k(t)$ denota la k - ésima función simétrica elemental en $t=\{t_1,\ldots,t_h\}$.

Por tanto para $a=\{a_1,\ldots,a_h\}$ y $b=\{b_1,\ldots,b_h\}$, tenemos

$$\alpha^h + \sigma_1(a)\,\alpha^{h-1} + \cdots + \sigma_{h-1}(a)\,\alpha + \sigma_h(a) = \alpha^h + \sigma_1(b)\,\alpha^{h-1} + \cdots + \sigma_{h-1}(b)\,\alpha + \sigma_h(b),$$

cancelando la mayor potencia de α e igualando a cero

$$(\sigma_1(a) - \sigma_1(b))\,\alpha^{h-1} + \cdots + (\sigma_{h-1}(a) - \sigma_{h-1}(b))\,\alpha + (\sigma_h(a) + \sigma_h(b)) \;=\; 0. \qquad (3.2)$$

Luego, $[\mathbb{K}(\alpha) : \mathbb{K}] \leq h-1$, lo cual no es posible ya que $[\mathbb{K}(\alpha) : \mathbb{K}] = h$. A no ser de que el polinomio en (3.2) sea cero, en tal caso, si definimos

$$\begin{aligned} f_1 &:= \sigma_1(a) = \sigma_1(b), \\ &\vdots \\ f_{h-1} &:= \sigma_{h-1}(a) = \sigma_{h-1}(b), \\ f_h &:= \sigma_h(a) = \sigma_h(b), \end{aligned}$$

entonces los "conjuntos" $\{a_1, \ldots, a_h\}$ y $\{b_1, \ldots, b_h\}$ están ambos conformados por las raíces del polinomio

$$y^h - f_1 y^{h-2} + \cdots + f_{h-1} y - f_h \in \mathbb{K}[y],$$

y por lo tanto deben coincidir

$$\{a_1, \ldots, a_h\} = \{b_1, \ldots, b_h\}.$$

□

Comentario 3.2.1. Si $\mathbb{K}$ es finito, $\alpha + \mathbb{K}$ tiene tantos elementos como tenga $\mathbb{K}$.

Comentario 3.2.2. Si en el teorema 3.2.1, tomamos $\mathbb{K} = \mathbb{F}_q$, con q potencia prima y α de grado h sobre $\mathbb{F}_q$, tenemos que $\mathbb{K}(\alpha) = \mathbb{F}_{q^h}$, y el teorema nos dice que el conjunto

$$A(\alpha, \mathbb{F}_q) := \alpha + \mathbb{F}_q,$$

es un conjunto B_h con q elementos en el grupo multiplicativo $\mathbb{F}^*_{q^h}$. Ahora, como este grupo es cíclico de orden $q^h - 1$, también sabemos que es isomorfo al grupo aditivo de los enteros módulo $q^h - 1$, $\mathbb{Z}_{q^h-1}$. Es este isomorfismo (logaritmo discreto) el que nos permite construir el conjunto B_h módulo $q^h - 1$, como sigue. Consideremos el isomorfismo

$$\begin{aligned} \mathbb{F}^*_{q^h} &\longrightarrow \mathbb{Z}_{q^h-1}, \\ x &\longmapsto \log_\theta x \end{aligned}$$

entonces el conjunto $\alpha + \mathbb{F}_q$ es enviado en el conjunto

$$\log_\theta(\alpha + \mathbb{F}_q) := \{\log_\theta(\alpha + a) : a \in \mathbb{F}_q\},$$

y este es un conjunto B_h módulo $q^h - 1$. Si además tomamos $\alpha = \theta$, obtenemos la construcción de Bose y Chowla, de acuerdo con el Comentario 3.1.1.

3.3. Casos particulares y ejemplos

En esta sección presentamos en más detalle la construcción de Bose y Chowla, considerando específicamente los casos $h = 2, 3$, y 4.

3.3.1. Conjuntos B_2

Sea q una potencia prima, trabajando en la extensión $\mathbb{F}_{q^2}$ de $\mathbb{F}_q$.

$$\begin{array}{c} \mathbb{F}_{q^2} \\ | \\ \mathbb{F}_q \end{array}$$

tenemos los siguientes resultados. Y su tabla de productos es :

Corolario 3.3.1. *Para todo $\alpha \in \mathbb{F}_{q^2}$, $\alpha \notin \mathbb{F}_q$, el conjunto*

$$\alpha + \mathbb{F}_q = \{\alpha + a : a \in \mathbb{F}_q\},$$

es un conjunto B_2 en el grupo $\left\langle \mathbb{F}_{q^2}^*, \cdot \right\rangle$, con q elementos.

Ejemplo 3.3.1. Sean $q = 5$, $P(x) = x^2 + x + 2 \in \mathbb{F}_5[x]$. Este polinomio resulta ser primitivo y si θ es una raíz de $P(x)$ entonces $\mathbb{F}_{25}^*$ es generado por θ.
En efecto

k	θ^k	k	θ^k
1	θ	13	$\theta^{13} = 4\theta$
2	$\theta^2 = 4\theta + 3$	14	$\theta^{14} = \theta + 2$
3	$\theta^3 = 4\theta + 2$	15	$\theta^{15} = \theta + 3$
4	$\theta^4 = 3\theta + 2$	16	$\theta^{16} = 2\theta + 3$
5	$\theta^5 = 4\theta + 4$	17	$\theta^{17} = \theta + 1$
6	$\theta^6 = 2$	18	$\theta^{18} = 3$
7	$\theta^7 = 2\theta$	19	$\theta^{19} = 3\theta$
8	$\theta^8 = 3\theta + 1$	20	$\theta^{20} = 2\theta + 4$
9	$\theta^9 = 3\theta + 4$	21	$\theta^{21} = 2\theta + 1$
10	$\theta^{10} = \theta + 4$	22	$\theta^{22} = 4\theta + 1$
11	$\theta^{11} = 3\theta + 3$	23	$\theta^{23} = 2\theta + 2$
12	$\theta^{12} = 4$	24	$\theta^{24} = 1$

Si tomamos $\alpha = \theta$, entonces el conjunto

$$\theta + \mathbb{F}_5 = \{\theta, \theta + 1, \theta + 2, \theta + 3, \theta + 4\},$$

es un conjunto B_2 en el grupo multiplicativo $\mathbb{F}_{25}^*$. Y su tabla de productos

θ	$\theta+1$	$\theta+2$	$\theta+3$	$\theta+4$
$4\theta+3$	3	$\theta+3$	$2\theta+3$	$3\theta+3$
	$\theta+4$	2θ	$3\theta+1$	$4\theta+2$
		$3\theta+2$	$4\theta+4$	1
			2	θ
				$2\theta+4$

Corolario 3.3.2. *Para toda potencia prima q, todo α de grado 2 sobre $\mathbb{F}_q$ y todo generador θ de $\mathbb{F}_{q^2}^*$, el conjunto*

$$\log_\theta(\alpha + \mathbb{F}_q) = \{\log_\theta(\alpha + a) : a \in \mathbb{F}_q\},$$

es un conjunto B_2 módulo $q^2 - 1$ con q elementos.

Ejemplo 3.3.2. Utilizando el Ejemplo 3.3.1 y el corolario anterior, el conjunto

$$\begin{aligned}\log_\theta(\alpha+\mathbb{F}_q) &= \{1,17,14,15,10\}\\ &= \{1,10,14,15,17\},\end{aligned}$$

es un conjunto B_2 módulo 24. Y su tabla de sumas es:

1	10	14	15	17
2	11	15	16	18
	20	0	1	3
		4	5	7
			6	8
				10

3.3.2. Conjuntos B_3

Sea q una potencia prima, consideramos ahora la extensión $\mathbb{F}_{q^3}$ de $\mathbb{F}_q$.

$$\begin{array}{c}\mathbb{F}_{q^3}\\ |\\ \mathbb{F}_q\end{array}$$

y obtenemos resultados similares al caso anterior.

Corolario 3.3.3. *Para todo $\alpha \in \mathbb{F}_{q^3}$, $\alpha \notin \mathbb{F}_q$, el conjunto*

$$\alpha+\mathbb{F}_q = \{\alpha+a : a \in \mathbb{F}_q\},$$

es un conjunto B_3 en el grupo $\left\langle \mathbb{F}_{q^3}^*, \cdot \right\rangle$, con q elementos.

Corolario 3.3.4. *para toda potencia prima q, todo α de grado 3 sobre $\mathbb{F}_q$ y todo generador θ de $\mathbb{F}_{q^3}^*$, el conjunto*

$$\log_\theta(\alpha+\mathbb{F}_q) := \{\log_\theta(\alpha+a) : a \in \mathbb{F}_q\},$$

es un conjunto B_3 módulo q^3-1 con q elementos.

Ejemplo 3.3.3. Sean $q = 5$, $P(x) = x^3 - 2x + 2 \in \mathbb{F}_5[x]$, α una raíz de $P(x)$.
Como $P(x)$ es irreducible sobre $\mathbb{F}_5$, entonces $\mathbb{F}_{5^3} \cong \mathbb{F}_5/(P(x)) = \mathbb{F}_5(\alpha)$. Un elemento primitivo es $\theta = 2\alpha^2 - 2\alpha - 2$. Entonces el conjunto

$$\theta + \mathbb{F}_5 = \{2\alpha^2 - 2\alpha - 2, 2\alpha^2 - 2\alpha - 1, 2\alpha^2 - 2\alpha, 2\alpha^2 - 2\alpha + 1, 2\alpha^2 - 2\alpha + 2\},$$

es un conjunto B_3 en el grupo $\langle \mathbb{F}_{125}^*, \cdot \rangle$. Mientras que el conjunto

$$A := \log_\theta(\alpha + \mathbb{F}_5) = \{1, 10, 12, 66, 110\},$$

es un conjunto B_3 módulo $5^3 - 1 = 124$. El conjunto de todas las $\binom{5+2}{3} = 35$ sumas de tres elementos de A (módulo 124) es

$$\{3, 6, 8, 9, 10, 12, 14, 18, 20, 23, 25, 30, 32, 34, 36, 38, 53, 62, 64,$$
$$68, 74, 77, 79, 82, 86, 88, 90, 97, 106, 108, 112, 118, 121, 123\}.$$

3.3.3. Conjuntos B_4

Sea q una potencia prima, consideramos ahora la extensión $\mathbb{F}_{q^4}$ de $\mathbb{F}_q$.

$$\begin{array}{c} \mathbb{F}_{q^4} \\ | \\ \mathbb{F}_q \end{array}$$

donde ahora tenemos dos corolarios similares a los considerados en las extensiones de grado 2 y 3.

Corolario 3.3.5. *Para todo $\alpha \in \mathbb{F}_{q^4}$, $gr(\alpha, \mathbb{F}_q) = 4$, $\alpha \notin \mathbb{F}_q$, el conjunto*

$$\alpha + \mathbb{F}_q = \{\alpha + a : a \in \mathbb{F}_q\},$$

es un conjunto B_4 en el grupo $\left\langle \mathbb{F}_{q^4}^*, \cdot \right\rangle$, con q elementos.

Corolario 3.3.6. *Para toda potencia prima q, todo α de grado 4 sobre $\mathbb{F}_q$, y todo generador θ de $\mathbb{F}_{q^4}^*$, el conjunto*

$$\log_\theta(\alpha + \mathbb{F}_q) := \{\log_\theta(\alpha + a) : a \in \mathbb{F}_q\},$$

es un conjunto B_4 módulo $q^4 - 1$ con q elementos.

Ejemplo 3.3.4. Sean $q = 5$, $P(x) = x^4 - 2x^3 + 2x^2 + 1 \in \mathbb{F}_5[x]$, α una raíz de $P(x)$. Como $P(x)$ es irreducible sobre $\mathbb{F}_5$, entonces $\mathbb{F}_{5^4} \cong \mathbb{F}_5/(P(x)) = \mathbb{F}_5(\alpha)$. Un elemento primitivo de $\mathbb{F}_{5^4}^*$ es $\theta = \alpha^2 - 1$. Entonces el conjunto

$$\theta + \mathbb{F}_5 = \{\alpha^2 - 1, \alpha^2, \alpha^2 + 1, \alpha^2 + 2, \alpha^2 + 3\},$$

es un conjunto B_4 en el grupo $\langle \mathbb{F}_{625}^*, \cdot \rangle$. Mientras que el conjunto

$$A := \log_\theta(\alpha + \mathbb{F}_5) = \{1, 198, 308, 563, 593\},$$

es un conjunto B_4 módulo $5^4 - 1 = 624$. El conjunto de todas las $\binom{5+3}{4} = 70$ sumas de cuatro elementos de A (módulo 624) es

$$\begin{aligned}\{&4, 15, 19, 45, 49, 75, 77, 81, 105, 107, 125, 129, 137, 139, 155, 159,\\ &168, 169, 185, 187, 191, 201, 215, 217, 239, 247, 249, 269, 274, 278,\\ &279, 301, 304, 311, 334, 336, 366, 380, 384, 388, 398, 410, 414, 440,\\ &442, 444, 446, 470, 472, 476, 494, 498, 500, 502, 504, 508, 524, 532,\\ &533, 534, 554, 556, 563, 564, 566, 586, 595, 596, 608, 618\}.\end{aligned}$$

3.4. Algunas Propiedades Especiales

Sean q una potencia prima, $h \geq 2$ un entero, $\mathbb{F}_q$ el campo finito con q elementos, $\mathbb{F}_{q^h}$ su extensión de grado h; $\alpha, \theta \in \mathbb{F}_{q^h}$ donde α es de grado h sobre $\mathbb{F}_q$ y θ es un elemento primitivo de $\mathbb{F}_{q^h}$. Como sabemos, el conjunto

$$B := B(q, h, \alpha, \theta) := \log_\theta(\alpha + \mathbb{F}_q), \tag{3.3}$$

es un conjunto B_h módulo $q^h - 1$ con q elementos. En esta sección consideramos algunas propiedades especiales de este conjunto.

Lema 3.4.1. *Con la notación anterior tenemos*
(i) Para todo $x \in B$, x no es divisible entre $q+1$ ($x \not\equiv 0$ (mód $q+1$)).
(ii) Para todo $x, y \in B$, con $x \neq y$, $x - y \not\equiv 0$ (mód $q+1$).

Prueba. (i) Si $x \in B$, entonces por (3.3) existe $b \in \mathbb{F}_q$ tal que

$$\begin{aligned} x &= \log_\theta(\alpha + b) \ \in [1, q^h - 1], \\ \theta^x &= \alpha + b \ \in \mathbb{F}_{q^h}^*, \end{aligned}$$

Si $x \equiv 0 \ (mód\ q+1)$, entonces $x = t(q+1)$, para algún entero positivo t, de donde

$$\alpha + b = \theta^x = (\theta^{q+1})^t \in \mathbb{F}_q^*,$$

porque $\mathbb{F}_q^* = \langle \theta^{q+1} \rangle$, luego $\alpha \in \mathbb{F}_q$ que no es posible puesto que el grado de α sobre $\mathbb{F}_q$ es $h \geq 2$. Esto prueba la primera parte del lema.
Para probar (ii), supongamos que $x, y \in B$ con $x \neq y$, entonces por (3.3), existen $a, b \in \mathbb{F}_q$ tales que

$$x = \log_\theta(\alpha + a), \quad y = \log_\theta(\alpha + b), \quad a \neq b,$$

de donde

$$\begin{aligned} x - y &= \log_\theta\left(\frac{\alpha + a}{\alpha + b}\right), \\ \theta^{x-y} &= \frac{\alpha + a}{\alpha + b}\ . \end{aligned}$$

Si tuviésemos que $x \equiv y \ (mód\ q+1)$, entonces $x - y = t(q+1)$ para algún entero t, y en consecuencia tendríamos

$$\frac{\alpha + a}{\alpha + b} = \theta^{x-y} = (\theta^{q+1})^t =: c \in \mathbb{F}_q^*\ ,$$

y por lo tanto α satisface la ecuación lineal

$$(1 - c)\theta + (a - bc) = 0,$$

con coeficientes en $\mathbb{F}_q$, esto no es posible a menos que $c = 1$ y $a = b$, contradiciendo el supuesto $x \neq y$. Esto termina la prueba de (ii). □

Cuando $h = 2$, el lema anterior nos permite caracterizar completamente el conjunto diferencia $B - B$, como lo establece el siguiente resultado.

Teorema 3.4.1. *Para toda potencia prima q, todo $\alpha \in \mathbb{F}_{q^2}$ de grado 2 sobre $\mathbb{F}_q$ y todo elemento primitivo θ de $\mathbb{F}_{q^2}$, el conjunto B definido en (3.3) es tal que su conjunto de diferencias satisface*

$$B - B = \mathbb{Z}_{q^2-1} \setminus M_{q+1},$$

donde $M_{q+1} = \{t\,(q+1) : t = 1, 2, \ldots, q-2\}$.

Prueba. Como B es un conjunto de Sidon $(mód\ q^2-1)$, con q elementos, tenemos que

$$|B - B| = 2\binom{q}{2} + 1 = q^2 - q + 1.$$

Por otro lado, el Lema 3.4.1 (ii) implica que $(B - B) \cap M_{q+1} = \emptyset$, y así:

$$\begin{aligned} |(B - B) \cup M_{q+1}| &= |(B - B)| + |M_{q+1}| \\ &= (q^2 - q + 1) + (q - 2) \\ &= q^2 - 1 \\ &= |\mathbb{Z}_{q^2-1}|\,. \end{aligned}$$

Esto finaliza la prueba del teorema. □

Ejemplo 3.4.1. Sea B el conjunto de Sidon módulo 24 obtenido en el Ejemplo 3.3.1

$$B = \{1, 10, 14, 15, 17\},$$

entonces $B - B$ se representa en la siguiente tabla

-	1	10	14	15	17
1	0	9	13	14	16
10	15	0	4	5	7
14	11	20	0	1	3
15	10	19	23	0	2
17	8	17	21	22	0

Como puede observarse solo hacen falta los elementos

$$6, 12, 18.$$

CAPÍTULO 4

Otras Construcciones.

En este capítulo presentamos otras construcciones de los conjuntos que nos ocupan. En primer lugar mostramos una construcción reciente obtenida por Alexis Gómez y Carlos Trujillo (ver [6]); posteriormente se presenta una nueva construcción que extiende la construcción de conjuntos B_2 en dimensión dos que aparece en la tesis doctoral del director de este proyecto (ver [7]).

4.1. Construcción Gómez y Trujillo 2007

En esta construcción se hace uso de conjuntos B_h en el grupo $\mathbb{Z}_{p^h-1}$, tipo Bose y Chowla, apartir del cual se construye un conjuntos B_{h+1} en dimensión dos en el grupo $\mathbb{Z}_p \times \mathbb{Z}_{p^h-1}$.

4.1.1. Los casos $h = 2$ y $h = 3$

Iniciemos entonces el estudio de esta construcción, consideremos el caso $h = 2$ para obtener los conjuntos B_3 tipo Gómez - Trujillo. Tenemos el siguiente teorema.

Teorema 4.1.1. *Para todo primo p existe un conjunto B_3 módulo $p(p^2-1)$ con p elementos.*

Prueba. Sean θ una raíz primitiva del campo con p^2 elementos, $\mathbb{F}_{p^2}$. Consideremos ahora el conjunto

$$T = T(p,\theta) := \{(a, \log_\theta(\theta + a)) : a \in \mathbb{F}_p\} \subseteq \mathbb{F}_p \times \mathbb{Z}_{p^2-1}.$$

Y supongamos que

$$(a_1, \log_\theta(\theta + a_1)) + (a_2, \log_\theta(\theta + a_2)) + (a_3, \log_\theta(\theta + a_3)) =$$
$$(b_1, \log_\theta(\theta + b_1)) + (b_2, \log_\theta(\theta + b_2)) + (b_3, \log_\theta(\theta + b_3)),$$

por la definición de T tenemos

$$a_1 + a_2 + a_3 \equiv b_1 + b_2 + b_3 \ (mód\ p). \tag{4.1}$$

$$\log_\theta(\theta + a_1) + \log_\theta(\theta + a_2) + \log_\theta(\theta + a_3) \equiv$$
$$\log_\theta(\theta + b_1) + \log_\theta(\theta + b_2) + \log_\theta(\theta + b_3) \ \ (mód\ p^2 - 1).$$

Por propiedades del logaritmo discreto

$$(\theta + a_1)(\theta + a_2)(\theta + a_3) = (\theta + b_1)(\theta + b_2)(\theta + b_3) \ \ en\ \mathbb{F}_{p^2}^*. \tag{4.2}$$

de (4.2) tenemos

$$\theta^3 + (a_1 + a_2 + a_3)\theta^2 + (a_1a_2 + a_1a_3 + a_2a_3)\theta + a_1a_2a_3 =$$
$$\theta^3 + (b_1 + b_2 + b_3)\theta^2 + (b_1b_2 + b_1b_3 + b_2b_3)\theta + b_1b_2b_3\ ,$$

cancelando la mayor potencia de θ

$$(a_1 + a_2 + a_3)\theta^2 + (a_1a_2 + a_1a_3 + a_2a_3)\theta + a_1a_2a_3 =$$
$$(b_1 + b_2 + b_3)\theta^2 + (b_1b_2 + b_1b_3 + b_2b_3)\theta + b_1b_2b_3.$$

Ahora bien,

$$\prod_{k=1}^{3}(X + t_k) = X^3 + \sigma_1(t)X^2 + \sigma_2(t)X + \sigma_3(t)\ , \tag{4.3}$$

donde $\sigma_k(t)$ es la k-ésima función simétrica elemental en $t = \{t_1, t_2, t_3\}$.
Por (4.1), $\sigma_1(a) = \sigma_1(b)$ para $a = \{a_1, a_2, a_3\}$ y $b = \{b_1, b_2, b_3\}$. Además de (4.3)

$$\sigma_2(a)\theta + \sigma_3(a) = \sigma_2(b)\theta + \sigma_3(b)\ en\ \mathbb{F}_{p^2}^*,$$

y dado que $\{1, \theta\}$ es una base de $\mathbb{F}_{p^2}$ sobre $\mathbb{F}_p$, tenemos

$$\sigma_k(a) \equiv \sigma_k(b) \ (mód\ p), \tag{4.4}$$

donde $1 \leq k \leq 3$. Luego de (4.4),(4.5) y por la factorización única en $\mathbb{F}_p[X]$ se tendrá que $a = b$ y así

$$\{(a_k, \log_\theta(\theta + a_k)) : 1 \leq k \leq 3\} = \{(b_k, \log_\theta(\theta + b_k)) : 1 \leq k \leq 3\},$$

por lo tanto T es un conjunto B_3 en el grupo aditivo $\mathbb{F}_p \times \mathbb{Z}_{p^2-1}$. Como este grupo es isomorfo, vía Teorema Chino de los Residuos, al grupo $\mathbb{Z}_{p(p^2-1)}$ el teorema está demostrado.

□

Ejemplo 4.1.1. Con $p = 5$, el conjunto

$$\{(0,1), (1,17), (2,14), (3,15), (4,10)\},$$

es un conjunto B_3 en el grupo aditivo $\mathbb{Z}_5 \times \mathbb{Z}_{24}$, y utilizando Teorema Chino de los Residuos, el conjunto

$$\{25, 34, 41, 62, 63\},$$

es un conjunto B_3 módulo 120, cuyo conjunto de $\binom{5+2}{3} = 35$ sumas módulo 120 es :

$$\{1, 2, 3, 8, 9, 10, 11, 17, 18, 24, 25, 29, 30, 31, 38, 39, 40, 45, 46, 47,$$
$$66, 67, 68, 69, 75, 84, 91, 93, 100, 102, 107, 109, 112, 113, 116\}.$$

Presentamos ahora la construcción de conjuntos B_4.

Teorema 4.1.2. *Para todo primo p existe un conjunto B_4 módulo $p(p^3 - 1)$ con p elementos.*

Prueba. Similar a la prueba del Teorema 4.1.1, solo que ahora se utiliza la construcción de conjuntos B_3 tipo Bose y Chowla.
Si θ es un elemento primitivo del campo con p^3 elementos, $\mathbb{F}_{p^3}$, entonces el conjunto

$$T = T(p, \theta) := \{(a, \log_\theta(\theta + a)) : a \in \mathbb{F}_p\} \subseteq \mathbb{F}_p \times \mathbb{Z}_{p^3-1},$$

es un conjunto B_4 en el grupo aditivo $\mathbb{F}_p \times \mathbb{Z}_{p^3-1}$, que es isomorfo con $\mathbb{Z}_p \times \mathbb{Z}_{p^3-1}$, que como sabemos es isomorfo con el grupo aditivo de los enteros módulo $p(p^3 - 1)$. □

4.1.2. Caso general $h \geq 2$

De los casos particulares anteriores podemos presentar el teorema general de Gómez y Trujillo ([6]), por completitud incluimos la demostración original.

Teorema 4.1.3. (Construcción de conjuntos B_{h+1} a partir de conjuntos B_h). *Para todo primo p y todo entero $h \geq 2$, existe una colección $x_1, x_2, \cdots, x_p$ de p enteros, que es un conjunto B_{h+1} módulo $p(p^h - 1)$.*

Prueba. Sea θ un elemento primitivo de $\mathbb{F}_{p^h}$. Consideremos el conjunto

$$T = \{(a, \log_\theta(\theta + a)) : a \in \mathbb{Z}_p\} \subseteq \mathbb{Z}_p \times \mathbb{Z}_{p^h-1}.$$

Supongamos que

$$\bigoplus_{k=1}^{h+1} (a_k, \log_\theta(\theta + a_k)) = \bigoplus_{k=1}^{h+1} (b_k, \log_\theta(\theta + b_k)),$$

donde $\bigoplus$ denota la suma componente a componente de $\mathbb{Z}_p \times \mathbb{Z}_{p^h-1}$. Entonces

$$\sum_{k=1}^{h+1} a_k \equiv \sum_{k=1}^{h+1} b_k \pmod{p},$$

$$\sum_{k=1}^{h+1} \log_\theta(\theta + a_k) \equiv \sum_{k=1}^{h+1} \log_\theta(\theta + b_k) \pmod{p^h - 1}.$$

De las propiedades del logaritmo discreto se tiene

$$\sum_{k=1}^{h+1} a_k \equiv \sum_{k=1}^{h+1} b_k \pmod{p} \tag{4.5}$$

$$\prod_{k=1}^{h+1} (\theta + a_k) = \prod_{k=1}^{h+1} (\theta + b_k) \quad \text{en } \mathbb{F}^*_{p^h}$$

Por otra parte ,

$$\prod_{k=1}^{h+1} (X + t_k) = X^{h+1} + \sigma_1(t) X^h + \sigma_2(t) X^{h-1} + \cdots + \sigma_h(t) X + \sigma_{h+1}(t), \tag{4.6}$$

donde $\sigma_k(t)$ denota la k - ésima función simétrica elemental en $t = \{t_1, \ldots, t_h\}$.
Por tanto para $a = \{a_1, \ldots, a_{h+1}\}$ y $b = \{b_1, \ldots, b_{h+1}\}$, de (4.5) y (4.6) se sigue

$$\sum_{k=2}^{h+1} \sigma_k(a) \theta^{h+1-k} = \sum_{k=2}^{h+1} \sigma_k(b) \theta^{h+1-k} \quad \text{en} \quad \mathbb{F}^*_{p^h},$$

y dado que $\left\{1, \theta, \theta^2, \ldots, \theta^{h-1}\right\}$ es una base de $\mathbb{F}_{p^h}$ sobre $\mathbb{F}_p = \mathbb{Z}_p$, se tiene

$$\sigma_k(a) \equiv \sigma_k(b) \quad (m\acute{o}d\ p), \tag{4.7}$$

sujeto a la restricción $1 \leq k \leq h+1$.

Luego de (4.6),(4.7) y en virtud de que $\mathbb{Z}_p[X]$ es D.F.U, se tendrá que $a = b$ y así

$$\{(a_k, \log_\theta(\theta + a_k)) : 1 \leq k \leq h+1\} = \{(b_k, \log_\theta(\theta + b_k)) : 1 \leq k \leq h+1\}.$$

De esta forma T es un conjunto B_{h+1} en el grupo aditivo $\mathbb{Z}_p \times \mathbb{Z}_{p^h-1}$.

Del Teorema Chino de los Restos y el Lema 1.2.1, se obtiene la construcción de conjuntos B_{h+1} módulo $p\left(p^h - 1\right)$ con p elementos, la cual está dado por el conjunto

$$\left\{p^h \log_\theta(\theta + a) - \left(p^h - 1\right) a : a \in \mathbb{Z}_p\right\} \subseteq \mathbb{Z}_{p(p^h-1)}.$$

□

Comentario 4.1.1. Esta construcción puede extenderse al caso en el que p se reemplaza por una potencia prima $q = p^n$. Es suficiente considerar el conjunto

$$T = \{(a, \log_\theta(\theta + a)) : a \in \mathbb{F}_q\} \subseteq \mathbb{F}_q \times \mathbb{Z}_{q^h-1},$$

donde θ es un elemento primitivo de $\mathbb{F}_{q^h}$. En este caso el grupo aditivo $\mathbb{F}_q \times \mathbb{Z}_{q^h-1}$ puede identificarse con $\mathbb{Z}_p^n \times \mathbb{Z}_{p^{nh}-1}$, y tenemos entonces un conjunto B_{h+1} con $q = p^n$ elementos en un grupo de orden $p^n \times (p^{nh} - 1) = p^{n(h+1)} - p^n$, grupo que no es cíclico si $n \geq 2$.

En cierto sentido, esta construcción mejora la construcción de Bose y Chowla, para todo $h \geq 3$.

4.2. Una construcción nueva

En esta sección presentamos una "nueva" construcción, que utiliza potencias de elementos en un campo. Podemos construir conjuntos B_2, B_3, B_4, y en general, conjuntos B_h, utilizando cuadrados, cubos, y potencias h-ésimas en un campo. Como ha sido usual, comenzamos con los primeros casos, $h = 2, 3$ y 4.

4.2.1. Conjuntos B_2 usando cuadrados

Sea $\mathbb{F}$ un campo, definimos el siguiente conjunto

$$A := \{(x, x^2) : x \in \mathbb{F}\}.$$

De donde, se tiene el siguiente teorema.

Teorema 4.2.1. *Si la característica de $\mathbb{F}$ es diferente de 2, entonces A es un conjunto B_2 en el grupo $\langle \mathbb{F} \times \mathbb{F}, + \rangle$.*

Prueba. Sean $a, b, c, d \in \mathbb{F}$ y supongamos que

$$(a, a^2) + (b, b^2) = (c, c^2) + (d, d^2),$$

dado que en $\mathbb{F} \times \mathbb{F}$ la suma es componente a componente, obtenemos el siguiente sistema

$$a + b = c + d, \tag{4.8}$$

$$a^2 + b^2 = c^2 + d^2, \tag{4.9}$$

tomando el cuadrado de (4.8)

$$(a + b)^2 = a^2 + 2ab + b^2 = c^2 + 2cd + d^2 = (c + d)^2,$$

pero por (4.9) y dado que $\mathbb{F}$ tiene característica diferente a 2, tenemos

$$ab = cd, \tag{4.10}$$

luego, de (4.8) y (4.10) se tiene que los elementos de los conjuntos $\{a, b\}$ y $\{c, d\}$ son raíces del mismo polinomio $p(x)$ en $\mathbb{F}[x]$,

$$p(x) = (x - a)(x - b) = (x - c)(x - d),$$

nuevamente, por ser $\mathbb{F}[x]$ D.F.U tenemos que $\{a, b\} = \{c, d\}$, lo cual concluye la prueba del teorema. □

Corolario 4.2.1. *Para todo primo impar p y todo entero positivo n, existe un conjunto de Sidon con p^n elementos en el grupo aditivo $\mathbb{Z}_p^{2n}$.*

Prueba. Sea $q = p^n$, consideremos el conjunto

$$C := \{(x, x^2) : x \in \mathbb{F}_q\},$$

es un conjunto de Sidon en el grupo $\mathbb{F}_q^2 = \mathbb{F}_{p^n}^2$ que resulta ser isomorfo con el grupo $\mathbb{Z}_p^{2n}$, así la imagen del conjunto C es un conjunto de Sidon como se requiere.

□

Ejemplo 4.2.1. El conjunto

$$\{(0,0),(1,1),(2,4),(3,2),(4,2),(5,4),(6,1)\},$$

es un conjunto B_2 en el grupo $\mathbb{Z}_7^2$. Y su conjunto de sumas es

$(0,0)$	$(1,1)$	$(2,4)$	$(3,2)$	$(4,2)$	$(5,4)$	$(6,1)$
$(0,0)$	$(1,1)$	$(2,4)$	$(3,2)$	$(4,2)$	$(5,4)$	$(6,1)$
	$(2,2)$	$(3,5)$	$(4,3)$	$(5,3)$	$(6,5)$	$(0,2)$
		$(4,1)$	$(5,6)$	$(6,6)$	$(0,1)$	$(1,5)$
			$(6,4)$	$(0,4)$	$(1,6)$	$(2,3)$
				$(1,4)$	$(2,6)$	$(3,3)$
					$(3,1)$	$(4,5)$
						$(5,2)$

Su conjunto de diferencias es

$(0,0)$	$(1,1)$	$(2,4)$	$(3,2)$	$(4,2)$	$(5,4)$	$(6,1)$
$(0,0)$	$(1,1)$	$(2,4)$	$(3,2)$	$(4,2)$	$(5,4)$	$(6,1)$
$(6,6)$	$(0,0)$	$(1,3)$	$(2,1)$	$(3,1)$	$(4,3)$	$(5,0)$
$(5,3)$	$(6,4)$	$(0,0)$	$(1,5)$	$(2,5)$	$(3,0)$	$(4,4)$
$(4,5)$	$(5,6)$	$(6,2)$	$(0,0)$	$(1,0)$	$(2,2)$	$(3,6)$
$(3,5)$	$(4,6)$	$(5,2)$	$(6,0)$	$(0,0)$	$(1,2)$	$(2,6)$
$(2,3)$	$(3,4)$	$(4,0)$	$(5,5)$	$(6,5)$	$(0,0)$	$(1,4)$
$(1,6)$	$(2,0)$	$(3,3)$	$(4,1)$	$(5,1)$	$(6,3)$	$(0,0)$

Ejemplo 4.2.2. Sea $q = 3^2$, θ una raíz del polinomio $p(x) = x^2 + x + 2$, el cual es irreducible sobre $\mathbb{F}_3$. Entonces

$$\mathbb{F}_9 = \{0, 1, 2, \theta, 2\theta, \theta+1, 2\theta+1, \theta+2, 2\theta+2\}.$$

El conjunto $\{(a, a^2) : a \in \mathbb{F}_9\}$ es

$$\{(0,0),(1,1),(2,1),(\theta,2\theta+1),(2\theta,2\theta+1),$$
$$(\theta+1,\theta+2),(2\theta+1,2),(\theta+2,2),(2\theta+2,\theta+2)\}$$

que es un conjunto B_2 en el grupo aditivo $\mathbb{F}_9^2$, el cual es isomorfo con el grupo aditivo $\mathbb{Z}_3^4$, así que el conjunto

$$\{(0,0,0,0),(0,1,0,1),(0,2,0,1),(1,0,2,1),(2,0,2,1),$$
$$(1,1,1,2),(2,1,0,2),(1,2,0,2),(2,2,1,2)\},$$

es un conjunto de Sidon en $\mathbb{Z}_3^4$.

4.2.2. Conjuntos B_3 usando cuadrados y cubos

Si $\mathbb{F}$ es un campo, ahora utilizamos cuadrados y cubos.

Teorema 4.2.2. *Si $\mathbb{F}$ es un campo de característica cero o $p > 3$, entonces el conjunto*

$$A := \{(x, x^2, x^3) : x \in \mathbb{F}\},$$

es un conjunto B_3 en el grupo $\langle \mathbb{F}^3, + \rangle$.

Prueba. Sean $a, b, c, d, e, f \in \mathbb{F}$ y supongamos que

$$(a, a^2, a^3) + (b, b^2, b^3) + (c, c^2, c^3) = (d, d^2, d^3) + (e, e^2, e^3) + (f, f^2, f^3) \ ,$$

dado que en $\mathbb{F}^3$ la suma es componente a componente, obtenemos los sistemas

$$a + b + c = d + e + f, \tag{4.11}$$
$$a^2 + b^2 + c^2 = d^2 + e^2 + f^2, \tag{4.12}$$
$$a^3 + b^3 + c^3 = d^3 + e^3 + f^3, \tag{4.13}$$

tomando el cuadrado de (4.11) y realizando los respectivos cálculos tenemos

$$(a+b+c)^2 = a^2+b^2+c^2+2\,(ab+ac+bc) = d^2+e^2+f^2+2\,(de+df+ef) = (d+e+f)^2,$$

por (4.12) y dado que la característica de $\mathbb{F}$ es diferente de 2, tenemos

$$ab + ac + bc = de + df + ef. \tag{4.14}$$

Ahora, tomemos el cubo de (4.11), realizando los cálculos necesarios y teniendo en cuenta que la característica de $\mathbb{F}$ es cero o un primo $p > 3$, tenemos

$$\begin{aligned}(a+b+c)^3 &= a^3 + b^3 + c^3 + (a+b+c)(ab+ac+bc) - abc \\ &= d^3 + e^3 + f^3 + (d+e+f)(de+df+ef) - def \\ &= (d+e+f)^3\end{aligned}$$

luego, de (4.11),(4.13) y (4.14) se tiene

$$-abc = -def.$$

Esta igualdad junto con (4.11) y (4.14) implican que los conjuntos $\{a, b, c\}$ y $\{d, e, f\}$ son raíces del mismo polinomio $q(x)$ en $\mathbb{F}[x]$, esto es

$$q(x) = (x-a)(x-b)(x-c) = (x-d)(x-e)(x-f),$$

dado que $\mathbb{F}[x]$ es D.F.U, debemos tener $\{a, b, c\} = \{d, e, f\}$, lo cual concluye la prueba del teorema. □

Como en el caso anterior, tenemos el siguiente resultado.

Corolario 4.2.2. *Para todo primo $p > 3$ y todo entero positivo n, existe un conjunto B_3 con p^n elementos en el grupo aditivo $\mathbb{Z}_p^{3n}$.*

Prueba. Sea $q = p^n$, considerar el conjunto

$$C := \{(x, x^2, x^3) : x \in \mathbb{F}_q\},$$

es un conjunto B_3 en el grupo aditivo $\mathbb{F}_q^3 = \mathbb{F}_{p^n}^3$ que resulta ser isomorfo con el grupo $\mathbb{Z}_p^{3n}$, así la imagen del conjunto C es un conjunto B_3 como se requiere. □

Ejemplo 4.2.3. $p = 7$, el conjunto

$$\{(0,0,0), (1,1,1), (2,4,1), (3,2,6), (4,2,1), (5,4,6), (6,1,6)\},$$

es B_3 en $\mathbb{Z}_7^3$.

4.2.3. Conjuntos B_h usando potencias hasta de orden h

Los resultados anteriores pueden generalizarse a todo $h \geq 2$.

Teorema 4.2.3. *Si $\mathbb{F}$ es un campo de característica cero o $p > h$, entonces el conjunto*

$$A := \left\{ \left(x, x^2, x^3, \ldots, x^h \right) : x \in \mathbb{F} \right\},$$

es un conjunto B_h en el grupo $\left\langle \mathbb{F}^h, + \right\rangle$.

Prueba. Necesitamos recurrir a las Identidades de Newton-Girard que permite expresar las funciones simétricas elementales en términos de las sumas de potencias. Si

$$P_k \left(x_1, x_2, \ldots, x_h \right) = \sum_{i=1}^{h} x_i^k, \quad 1 \leq k \leq h,$$

denota la suma de las k-ésimas potencias de los x_i, entonces es posible obtener las funciones simétricas elementales en h-variables en forma recursiva

$$k\sigma_k \left(x_1, x_2, \ldots, x_h \right) = \sum_{i=1}^{k} (-1)^{i-1} \sigma_{k-i} \left(x_1, x_2, \ldots, x_h \right) P_i \left(x_1, x_2, \ldots, x_h \right).$$

Por lo tanto, de la igualdad de las sumas de las potencias k-ésimas

$$\begin{aligned} a_1 + a_2 + \ldots + a_h &= b_1 + b_2 + \ldots + b_h, \\ a_1^2 + a_2^2 + \ldots + a_h^2 &= b_1^2 + b_2^2 + \ldots + b_h^2, \\ &\vdots \\ a_1^h + a_2^h + \ldots + a_h^h &= b_1^h + b_2^h + \ldots + b_h^h, \end{aligned}$$

esto es $P_k \left(a_1, a_2, \ldots, a_h \right) = P_k \left(b_1, b_2, \ldots, b_h \right)$ para todo k con $1 \leq k \leq h$, se siguen las igualdades de las funciones simétricas elementales $\sigma_k \left(a_1, a_2, \ldots, a_h \right) = \sigma_k \left(b_1, b_2, \ldots, b_h \right)$, y en consecuencia la igualdad $\{a_1, a_2, \ldots, a_h\} = \{b_1, b_2, \ldots, b_h\}$.
Este hecho permite demostrar que el conjunto

$$A := \left\{ \left(x, x^2, x^3, \ldots, x^h \right) : x \in \mathbb{F} \right\},$$

es claramente un conjunto B_h en el grupo aditivo $\mathbb{F}^h$. □

Corolario 4.2.3. *Para todo primo $p > h$ y todo entero positivo n, existe un conjunto B_h con p^n elementos en el grupo aditivo $\mathbb{Z}_p^{hn}$.*

Prueba. Sea $q = p^n$, el conjunto definido en el teorema anterior es un conjunto B_h en el grupo aditivo $\mathbb{F}_q^h = \mathbb{F}_{p^n}^h$ que como sabemos es isomorfo con el grupo $\left(\mathbb{Z}_p^n\right)^h = \mathbb{Z}_p^{nh}$. por lo tanto, la imagen del conjunto A, a través del isomorfismo natural, (ver prueba del Teorema 2.7.2), resulta ser un conjunto B_h como lo requerimos. □

Conclusiones

En este capítulo se presentan los resultados más importantes que obtuvimos en el desarrollo de este trabajo, en especial, se hizo un estudio a fondo de algunas Construcciones de Conjuntos B_h Modulares, en particular para los casos $h = 2, 3, 4$. Dentro de las cuales se destacan las construcciones de I. Ruzsa (ver [1]), R. C. Bose y S. Chowla (ver [5]), A. Gómez y C. Trujillo (ver [6]).

Resultados importantes

1. Se aporta una nueva construcciones de conjuntos B_2, B_3, B_4 y en general, de conjuntos B_h, utilizando potencias de elementos de un campo, dicha construcción extiende la construcción de conjuntos B_2 en dimensión dos que aparece en la tesis doctoral del director de este proyecto. Destacamos principalmente el Teorema 4.2.3 y el Corolario 4.2.3.

2. El documento registra una versión generalizada del Teorema 2.6.1, (Construcción en dos dimensiones), dicha generalización se presenta en el Teorema 2.7.2, es de resaltar que si tomamos $n = 1$ en dicho teorema obtenemos la construcción de Ruzsa.

3. Se presenta una versión generalizada (Teorema 3.2.1) del Teorema 3.1.1 que contiene la construcción de conjuntos B_h original de Bose y Chowla. Mediante esta generalización

podemos construir conjuntos B_h en un campo arbitrario, en particular sobre campos finitos.

4. Se encontraron algunas propiedades estructurales como lo son, identificar el conjunto $A-A=\mathbb{Z}_{p(p-1)}\backslash(M_p\cup M_{p-1})$, en la construcción de Ruzsa, y como también, identificar el conjunto $B-B=\mathbb{Z}_{q^2-1}\setminus M_{q+1}$, en la construcción de Bose y Chowla.

Preguntas importantes

- Hay $\varphi(p-1)$ particiones, una por cada entero f. Por lo tanto $\varphi(p-1)(p-1)$ conjuntos de Sidon módulo $p(p-1)$ obtenidos de esta forma. Cambiar de raíz primitiva no adiciona nada nuevo. ¿Existen otros conjuntos de Sidon con $p-1$ elementos no obtenidos de esta forma? ¿Cuántos? ¿Cómo obtenerlos todos?. Preguntas similares son válidas para la Construcción de Bose y Chowla.

- Para futuras investigaciones se propone estudiar los polinomios asociados a cada conjunto de Sidon obtenido. Por ejemplo

$$P_A(X)=\prod_{a\in A}(X-a),$$
$$P_{A,g}(X)=\prod_{a\in A}(X-g^a),$$

en el anillo polinomial $\mathbb{Z}_{p(p-1)}[X]$, para el caso de la Construcción de Ruzsa.

APÉNDICE A

Apéndice: Campos Finitos

En este apéndice presentamos algunas definiciones y resultados básicos de la teoría de campos finitos necesarias para el desarrollo de este trabajo. Algunos de los resultados que presentaremos no tendrán su respectiva demostración, pero sus pruebas pueden ser consultadas en [8,Cap. 1 y 2].

A.1. Campos Finitos y subcampos

Un Campo Finito, es un anillo con identidad $1 \neq 0$ tal que sus elementos no nulos forman un grupo abeliano bajo la multiplicación y tienen un número finito de elementos. Los campos de clases residuales $\mathbb{Z}/(p)$ son nuestros primeros ejemplos de campos finitos, esto es, de campos que contienen únicamente finitos elementos. A continuación presentamos algunos resultados básicos de la teoría de campos finitos.

Definición A.1.1. *Para un primo p, sea $\mathbb{F}_p$ el conjunto $\{0, 1, \ldots, p-1\}$ de enteros, y sea $\psi : \mathbb{Z}/(p) \longrightarrow \mathbb{F}_p$ la aplicación definida mediante $\psi([a]) = a$, para $a = 0, 1, \ldots, p-1$. Entonces $\mathbb{F}_p$, dotado con la estructura de campo inducida por ψ, es un campo finito, llamado el campo Galois de orden p.*

Teorema A.1.1. *Sea p un numero primo y q potencia prima,*

(a) Si $\mathbb{F}$ es un campo finito con característica p, entonces $|\mathbb{F}| = p^n$, donde n es el grado de $\mathbb{F}$ sobre un subcampo primo $\mathbb{F}_p$.

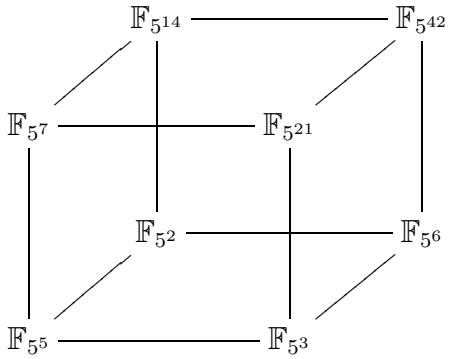
(b) Para todo entero positivo n, existe un campo finito con q^n elementos, además cualquier campo finito con q^n elementos es isomorfo al campo de descomposición de $x^{q^n} - x$, sobre $\mathbb{F}_q$.

(c) Si $\mathbb{F}$ es un campo finito con q elementos, entonces para todo $\alpha \in \mathbb{F}$ se cumple que $\alpha^q = \alpha$.

Por tanto, si $\mathbb{F}$ es un campo con q elementos, donde q es una potencia prima de la característica, y $\mathbb{L}$ es una extensión finita de $\mathbb{F}$ de grado h, entonces $\mathbb{L}$ se denota por $\mathbb{F}_{q^h}$, que consiste de las raíces de $x^{q^n} - x$, sobre $\mathbb{F}_p$.
Ahora, los subcampos de un campo finito $\mathbb{F}_{q^h}$, están caracterizados por los divisores positivos de h.

Teorema A.1.2 (Criterio de subcampos). *Sea $\mathbb{F}_{q^h}$, el campo finito con q^h elementos. Entonces todo subcampo de $\mathbb{F}_{q^h}$ tiene orden q^d, donde d es un divisor positivo de h. Recíprocamente, si d es un divisor positivo de h, entonces existe exactamente un subcampo de $\mathbb{F}_{q^h}$ con q^d elementos.*

Ejemplo A.1.1. Los subcampos de $\mathbb{F}_{5^{42}}$, están determinados por los divisores positivos de 42 y se relacionan mediante el siguiente diagrama.



A.2. El grupo de unidades de un campo finito

Para un campo finito $\mathbb{F}_q$, denotamos mediante $\mathbb{F}_q^*$ al *grupo multiplicativo* de los elementos no nulos de $\mathbb{F}_q$. El siguiente resultado enuncia una propiedad útil de este grupo.

Teorema A.2.1. *Para todo q potencia prima, el grupo multiplicativo $\mathbb{F}_q^*$ es cíclico.*

Prueba. Asumiendo que $q \geq 3$, sea $h = q-1 = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ la descomposición en factores primos del orden del grupo $\mathbb{F}_q^*$.
Para cada $0 \leq i \leq m$, el polinomio $x^{h/p_i} - 1$, tiene a lo mas h/p_i raíces en $\mathbb{F}_q$ y como $h/p_i < h$, se sigue que existe un elemento no nulo a_i en $\mathbb{F}_q$ que no es raíz de este polinomio. Considérese el elemento $b_i = a_i^{h/p_i^{r_i}}$. Nótese que $b_i^{p_i^{r_i}} = 1$, de esta manera el orden de b_i es un divisor de $p_i^{r_i}$ y es por tanto de la forma $p_i^{s_i}$, donde $0 \leq s_i \leq r_i$. Por otro lado,

$$b_i^{p_i^{r_i-1}} = a_i^{h/p_i} \neq 1$$

y asi el orden de b_i es $p_i^{r_i}$. Para terminar, se vera que $b = b_1 b_2 \ldots b_m$ tiene orden h.
Argumentando por contradicción, supóngase que el orden de b es un divisor propio de h y de esta forma, un divisor de al menos uno de los enteros h/p_i, $1 \leq i \leq m$. Sin perdida de generalidad, supóngase que h/p_1. Entonces

$$b_1^{h/p_1} b_2^{h/p_1} \ldots b_m^{h/p_1} = b^{h/p_1} = 1.$$

Ahora, si $2 \leq i \leq m$, entonces $p_i^{r_i}$ divide a h/p_1 y así $b_i^{h/p_1} = 1$. Luego $b_1^{h/p_1} = 1$, lo cual implica que el orden de b divide a h/p_1, que no es posible dado que el orden de b es $p_1^{r_1}$. Por tanto, $\mathbb{F}_q^*$ es un grupo cíclico generado por b. □

Un generador del grupo cíclico $\mathbb{F}_q^*$, como b en el Teorema anterior se llama un **elemento primitivo** de $\mathbb{F}_q$. Además, un polinomio $f \in \mathbb{F}_q[x]$ de grado $m \geq 1$, se llama un **polinomio primitivo** sobre $\mathbb{F}_q$, si es el polinomio mínimal sobre $\mathbb{F}_q$ de un elemento primitivo de $\mathbb{F}_q^m$. El siguiente Teorema muestra que un elemento primitivo es también un elemento que sirve para definir a $\mathbb{F}_q$, como una extensión de uno de sus subcampos.

Teorema A.2.2. *Sean, $\mathbb{F}_q$ un campo finito y $\mathbb{F}_q^h$ una extensión finita de $\mathbb{F}_q$. Entonces $\mathbb{F}_q^h$ es una extensión simple de $\mathbb{F}_q$ y si ξ es un elemento primitivo de $\mathbb{F}_q^h$, entonces $\mathbb{F}_q^h = \mathbb{F}_q(\xi)$.*

A.3. Polinomios sobre un campo finito

Dado un polinomio $p(x)$ irreducible sobre $\mathbb{F}_q$ de grado m, es importante notar, que a diferencia de los polinomios sobre un campo de característica cero, es suficiente extender $\mathbb{F}_q$ con una

raíz de $p(x)$ para obtener el campo de descomposición de $p(x)$ y sus m raíces están dadas de manera particular.

Teorema A.3.1. *Si $p(x)$ es un polinomio irreducible de grado m, sobre $\mathbb{F}_q$, entonces $p(x)$ tiene una raíz α en $\mathbb{F}_q^m$. Más aún, todas las raíces de $p(x)$ son simples y están dadas por los m elementos distintos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ de $\mathbb{F}_q^m$.*

Teorema A.3.2. *Sean, $p(x)$ un polinomio irreducible sobre $\mathbb{F}_q$ de grado n y $k \in \mathbb{N}$. entonces $p(x)$ se descompone en d polinomios irreducibles en $\mathbb{F}_{q^k}[x]$, del mismo grado n/d, donde $d = mcd(n,k)$.*

Una consecuencia inmediata es que $p(x) \in \mathbb{F}_q[x]$, sigue siendo irreducible sobre $\mathbb{F}_{q^k}$ si y sólo si $mcd(n,k) = 1$.

Bibliografía

[1] Ruzsa Imre Z. *Solving a linear equation in a set of integers I.* Acta Arithmetica **65** (1993), 259–282.

[2] Lindström B. *Finding Finite B_2-Sequences Faster.* Math. C.mput. **47** (1998), 1173–1178.

[3] Gómez S. Pisso P. Trujillo C. *Conjuntos de Sidon Módulo m y Particiones*. Unicauca Ciencia **7** (2002), 85–94.

[4] Trujillo C. *Construcción de conjuntos de Sidon módulo $p(p-1)$.* Preprint, no publicado, Universidad del Cauca, 2004.

[5] Bose R. C. and Chowla S. *Theorems in the additive theory of numbers*. Comment. Math. Helv. **37** (1962/1963), 141–147.

[6] Gómez A. Trujillo C. *Construcción de conjuntos B_{h+1} desde conjuntos B_h.* Preprint, no publicado, Universidad del Cauca, 2007.

[7] Trujillo C. *Sucesiones de Sidon*. Tesis doctoral, Universidad Politécnica de Madrid, 1998.

[8] Lidl R. and Niederreiter H. *Finite Fields.* Encyclopedia of Mathematics and its Applications. Cambridge University Press, second edition (1997).

[9] Documentos de trabajo del grupo ALTENUA.

[10] *Elementary symmetric polinomial* in http: //en.wikipedia.org/wiki/Elementary symmetric polynomial.

[11] *Newton identities* in http: //en.wikipedia.org/wiki/Newton27sidentities.