Vol. XIV Nº 2 Diciembre (2006)
Matemáticas: 65–70

Matemáticas:
Enseñanza Universitaria

Construcción de conjuntos B_h módulo m y particiones

Gilberto García P. Carlos Alberto Trujillo S.
Juan Miguel Velásquez S.

Recibido Abr. 18, 2006 Aceptado Jun. 13, 2006

Abstract

A set $\{a_1, a_2, \ldots, a_n, \ldots\}$ of positive integers is called a B_h-set, if all the sums $a_{i_1} + a_{i_2} + \cdots + a_{i_h}$ ($i_s = i_r$ is permitted) are different. In this paper we generalize the Bose-Chowla Theorem on construction of B_h-set on finite fields. Besides, we show the existence of a partition of an interval into B_h-sets.

Keywords: B_h-sets, Bose-Chowla Theorem, Finite Field, Partitions.

AMSC(2000): Primary: 11B50, Secondary: 11B75, 12E20, 05B10

Resumen

A un conjunto A de enteros positivos se le llama un conjunto B_h módulo m, si todas las sumas de h elementos de A, no necesariamente distintos, son incongruentes $\mod m$. Demostramos que cuando m es de la forma $q^n - 1$, para q potencia de un primo, los logaritmos discretos de las raíces de polinomios de Artin-Schreier en el campo finito con q^n elementos forman un conjunto B_h módulo m, siendo h un divisor de n. Este resultado generaliza un teorema clásico en construcción de conjuntos B_h. Además, demostramos que hay particiones de $\mathbb{Z}_{q^n}$ en conjuntos B_h, donde h recorre los divisores de n.

Palabras y frases claves: Conjuntos B_h, Teorema de Bose - Chowla, Campos Finitos, Particiones.

1 Introducción

Un conjunto A de enteros positivos es un conjunto B_h, o un conjunto de clase 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.

Cálculos sencillos muestran que $A = \left\{2^i : i \in \mathbb{N}\right\}$ es un conjunto B_2 y que $\{1, 12, 22, 29, 31, 34, 35\}$ es $B_2 \mod 48$.

El primer método para construir conjuntos B_h fue desarrollado por J. Singer, [3], con éste método se construyen conjuntos B_2 módulo $\left(q^2 + q + 1\right)$, con $q+1$ elementos. Los conjuntos del tipo Singer hacen parte de los llamados Conjuntos Perfectos en Diferencias, estos son conjuntos de residuos módulo m, tales que todos los elementos distintos de cero en dicho módulo se pueden representar de manera única como la diferencia de dos elementos del conjunto.

Por ejemplo, los conjuntos $\{1, 2, 4\}$ y $\{1, 2, 5, 7\}$ son Perfectos en Diferencia para los módulos 7 y 13, respectivamente.

Otro procedimiento para construir conjuntos B_h modulares, es el desarrollado por Bose-Chowla, [1], en el cual se garantiza que para h entero mayor o igual que dos y q una potencia de un primo, si θ es un elemento primitivo de $\mathbb{F}_q$, el campo finito con q^h elementos, entonces el conjunto $\left\{0 < a \leq q^h - 1 : \theta^a - \theta \in \mathbb{F}_q\right\}$ es B_h módulo $q^h - 1$.

2 Construcción de conjuntos B_h módulo m

El primer teorema que se presenta en esta sección, permite construir conjuntos B_h con q elementos por medio de los logaritmos discretos de las raíces de un tipo de polinomios en campos finitos.

Si q es una potencia de un primo, $h \geq 2$ es un entero y $K = \mathbb{F}_q$, $F = \mathbb{F}_{q^h}$, son los campos finitos con q y q^h elementos respectivamente, se sabe por un resultado clásico de Artin - Schreier, [2, Thm 2.25], que si $\gamma \in F$, la ecuación $x^q - x - \gamma = 0$ tiene una solución en F, si y sólo sí, la traza de γ sobre K es cero, si éste es el caso y $\alpha \in F$ es una raíz de la ecuación, los elementos de $\alpha + K$ son todas las raíces de la misma.

El siguiente teorema establece un método para construir conjuntos B_h a través de las raíces de los polinomios de la forma $x^q - x - \gamma$

Teorema 2.1. *Si K y F son los campos finitos con q y q^h elementos respectivamente, β, θ elementos de F, con θ un elemento primitivo de F, $\gamma = \beta^q - \beta$ y*

$$A(q, \theta, \beta) = \left\{0 \leq a \leq q^h - 1 : \theta^{aq} - \theta^a - \gamma = 0\right\}$$

Entonces:

1. *Si β tiene grado d sobre K, $A(q, \theta, \beta)$ es un conjunto con q elementos, de clase B_d módulo $q^h - 1$.*

2. *Si $\beta = 0$, $A(q, \theta, 0)$ está formado por los múltiplos de $m = \dfrac{q^h - 1}{q - 1}$ contenidos en $\left\{0, \ldots, q^h - 1\right\}$.*

Demostración.

1. Sea β un elemento de grado d sobre K, como consecuencia del resultado de Artin-Schreier, antes mencionado, se tiene que

   $$A(q, \theta, \beta) = \left\{0 \leq a \leq q^h - 1 : \theta^a \in \beta + K\right\}$$

   por lo tanto, es claro que $A(q, \theta, \beta)$ tiene q elementos, y que para cada $a_i \in A(q, \theta, \beta)$ existe un único $\alpha_i \in K$ tal que

$$\theta^{a_i} = \beta + \alpha_i \tag{1}$$

de aquí se sigue que, si

$$a_{i_1} + a_{i_2} + \cdots + a_{i_d} \equiv a_{j_1} + a_{j_2} + \cdots + a_{j_d} \mod q^h - 1 \tag{2}$$

donde

$$i_1 \leq i_2 \leq \cdots \leq i_d \ , \ j_1 \leq j_2 \leq \cdots \leq j_d$$

entonces

$$\theta^{a_{i_1}} \theta^{a_{i_2}} \cdots \theta^{a_{i_d}} = \theta^{a_{j_1}} \theta^{a_{j_2}} \cdots \theta^{a_{j_d}}$$

y de (1), se tiene

$$\prod_{i=1}^{d} (\beta + \alpha_i) = \prod_{i=1}^{d} (\beta + \alpha_i').$$

Al expandir el producto y simplificar β^d en ambos lados de la igualdad, se obtiene una ecuación con coeficientes en K, de grado menor que d que se anula en β, esto es imposible, a menos que el conjunto de los α y el de los α' sean iguales, en cuyo caso

$$\{a_{i_1}, a_{i_2}, \ldots, a_{i_d}\} = \{a_{j_1}, a_{j_2}, \ldots, a_{j_d}\}$$

y $A(q, \theta, \beta)$ es un conjunto B_d módulo $q^h - 1$.

2. Si $\beta = 0$, el conjunto $A(q, \theta, 0)$ viene dado por

$$A(q, \theta, 0) = \left\{ 0 \leq a \leq q^h - 1 : \theta^a \in K \right\} = \left\{ 0 \leq a \leq q^h - 1 : \theta^{aq} = \theta^a \right\}.$$

Por lo tanto, si $a \in A(q, \theta, 0)$, se cumple que $\theta^{(q-1)a} = 1$ y como $\theta^{(q-1)}$ tiene orden $m = \dfrac{q^h - 1}{q - 1}$, se sigue que a es un múltiplo de m.

□

Al hacer $\beta = \theta$ en el Teorema anterior, se obtiene el Teorema de Bose-Chowla, ver [1].

Convención. En adelante, y a falta de un mejor nombre, diremos que el conjunto $A(q, \theta, 0)$ es un conjunto $B_1 \mod (q^h - 1)$.

3 Particiones.

Una consecuencia del Teorema 2.1, es que para n en $\mathbb{Z}_{q^h}$, existe un conjunto B_d con q elementos que contiene a n, siendo d un divisor de h que depende de n.

Ejemplo 3.1. *Dado que* $f(z) = z^4 + z^3 + z^2 + 2z + 2$ *es irreducible en* $\mathbb{Z}_3$, *si* θ *es una de raíz de* $f(z)$, $K = \langle\theta^{10}\rangle \cup \{0\}$ *y* $F = \langle\theta\rangle \cup \{0\}$ *son los campos finitos con* 9 *y* 81 *elementos, respectivamente,* $\beta = \theta^{13} \in F$ *es de grado* 2 *sobre* K, *por lo tanto, los logaritmos en base* θ *de las raíces de los elementos de* $\theta^{13} + K$ *determinan un conjunto* $B_2 \mod 80$, *que contiene a* 13, *dicho conjunto es* $\{1, 13, 35, 48, 49, 66, 72, 74, 77\}$.

Si se aplica repetidamente el procedimiento anterior, variando n, se obtiene una partición de $\mathbb{Z}_{81}$ en conjuntos $B_2 \mod 80$, el conjunto $\{0, 10, 20, \ldots, 80\}$ aparece al tomar $\beta \in K$. En general se tiene el siguiente Teorema.

Teorema 3.2. *Existe una partición de* $\mathbb{Z}_{q^h}$ *en conjuntos* B_d *módulo* $(q^h - 1)$, *donde* d *recorre los divisores de* h.

Demostración. Sean K y F, los campos finitos con q y q^h elementos respectivamente, θ un elemento primitivo de F y $P = \{A(q, \theta, \beta) : \beta \in F\}$. Se mostrará que P satisface la afirmación. En efecto, si $n \in \mathbb{Z}_{q^h}$ es claro que $n \in A(q, \theta, \theta^n)$ y por lo tanto

$$\mathbb{Z}_{q^h} = \bigcup_{\beta \in F} A(q, \theta, \theta^n)$$

de otro lado, si $A(q, \theta, \alpha)$ y $A(q, \theta, \beta)$ son elementos de P tales que

$$A(q, \theta, \alpha) \cap A(q, \theta, \beta) \neq \emptyset$$

entonces, existe $n \in \mathbb{Z}_{q^h}$, tal que $\theta^n - \alpha$ y $\theta^n - \beta$ son elementos de K, así que, $(\alpha - \beta) \in K$ y $A(q, \theta, \alpha) = A(q, \theta, \beta)$. Lo que termina la prueba. □

Si en el Teorema anterior, se toma h primo, todos los elementos de la partición P, excepto $A(q, \theta, 0)$, son conjuntos B_h módulo $q^h - 1$. Si h es compuesto, para cada divisor d de h, se puede determinar cuántos conjuntos de la partición son de clase B_d módulo $q^h - 1$, tal como se muestra en el siguiente Teorema.

Teorema 3.3. *Si* K *y* F *son los campos finitos con* q *y* q^h *elementos, respectivamente y si* d *es un divisor de* h, *entonces* P_d, *la cantidad de conjuntos* B_d *módulo* $q^h - 1$ *en la partición de* $\mathbb{Z}_{q^h}$ *obtenida por aplicación del Teorema 3.2, es*

$$P_d = \frac{1}{q} \sum_{c|d} \mu\left(\frac{d}{c}\right) q^c.$$

Demostración. Del Teorema 2.1, se sigue que cada β en F de grado d sobre K, determina un conjunto B_d, además, como la cantidad de elementos en F de grado d sobre K es $\sum_{c|d} \mu\left(\frac{d}{c}\right) q^c$, [1] y dado que cada conjunto de la partición es de cardinal q, se sigue que

$$P_d = \frac{1}{q} \sum_{c|d} \mu\left(\frac{d}{c}\right) q^c$$

□

Ejemplo 3.4. *En la partición de $\mathbb{Z}_{q^6}$ obtenida por la aplicación del Teorema 3.2, se tiene que:*

$$\begin{aligned} P_1 &= \tfrac{1}{q}\sum_{c|1} \mu\left(\tfrac{1}{c}\right) q^c = 1 \\ P_2 &= \tfrac{1}{q}\sum_{c|2} \mu\left(\tfrac{2}{c}\right) q^c = q-1 \\ P_3 &= \tfrac{1}{q}\sum_{c|3} \mu\left(\tfrac{3}{c}\right) q^c = q^2-1 \\ P_6 &= \tfrac{1}{q}\sum_{c|6} \mu\left(\tfrac{6}{c}\right) q^c = q^5-q^2-q+1 \end{aligned}$$

P_1 es el conjunto de múltiplos de $\dfrac{q^6-1}{q-1}$. En total se tienen q^5 conjuntos, cada uno con q elementos, de los cuales $q-1$ son B_2, q^2-1 son B_3 y q^5-q^2-q+1 son B_6.

Ejemplo 3.5. *Al tomar $q = 9$ y $h = 2$, por el Teorema 3.3, existe una partición del conjunto $\mathbb{Z}_{81}$ en 9 conjuntos, cada uno con 9 elementos, uno de ellos está formado por los múltiplos de $\frac{9^2-1}{9-1} = 10$, a saber, $A_0 = \{0, 10, 20, 30, 40, 50, 60, 70, 80\}$, los demás, son conjuntos B_2 módulo 80, que se obtienen al aplicar el procedimiento descrito en el Ejemplo 3.1. Para este caso, una partición de $\mathbb{Z}_{81}$ viene dada por:*

$\{0, 10, 20, 30, 40, 50, 60, 70, 80\}; \{1, 13, 35, 48, 49, 66, 72, 74, 77\}$
$\{2, 4, 7, 11, 23, 45, 58, 59, 76\}; \{3, 25, 38, 39, 56, 62, 64, 67, 71\}$
$\{5, 18, 19, 36, 42, 44, 47, 51, 63\}; \{6, 12, 14, 17, 21, 33, 55, 68, 69\}$
$\{8, 9, 26, 32, 34, 37, 41, 53, 75\}; \{15, 28, 29, 46, 52, 54, 57, 61, 73\}$
$\{16, 22, 24, 27, 31, 33, 65, 78, 79\}.$

Referencias

[1] Bose and Chowla, Theorems in the additive theory of numbers. Comment. Math. Helvet. 37 (1962-63), 141-147. MR 26:2418.

[1] Donde μ es la función de Möbius. Ver sección 3.2 en [2]

[2] R. Lidl and H. Niederreiter, Finite fields. With a foreword by P. M. Cohn. Second edition. Encyclopedia of Mathematics and its Applications, 20. Cambridge University Press, Cambridge, 1997. MR 97i:11115.

[3] J. Singer, A theorem in finite projective geometry and some aplications to number theory, Trans. Am.math.Soc. 43, 377-385. MR 1501951.

Dirección de los autores: Gilberto García P., Universidad de Antioquia, gigarcia@matematicas.udea.edu.co — Carlos Alberto Trujillo S., Universidad del Cauca, trujillo@unicauca.edu.co — Juan Miguel Velásquez S., Universidad del Valle, jumiveso@univalle.edu.co