Vol. XIX, Nº 1, Junio (2011)
Matemáticas: 53–62

Matemáticas:
Enseñanza Universitaria

Una nueva construcción de conjuntos B_h modulares

Carlos Alexis Gómez Ruiz
Universidad del Valle

Carlos Alberto Trujillo Solarte
Universidad del Cauca

Recibido Sep. 23, 2009 Aceptado Feb. 02, 2011

Abstract

Since the appearance of the B_h-sequences with the study of Sidon sequences in finite Fourier analysis (1932), three classic constructions are known in the modular integers with specific modules contributed by J. Singer (1938), R. C. Bose and S. Chowla (1962), and I. Z. Ruzsa (1993). This article presents a new construction of B_h-sequences in modular integers, which can be seen as extension of Ruzsa construction.

Keywords: Sidon sequence, B_h-sequences and constructions.

MSC(2000): 76M10, 76D03

Resumen

Desde la aparición de los conjuntos B_h con el estudio de los conjuntos de Sidon en el análisis de Fourier finito (1932), se conocen tres construcciones clásicas en los enteros modulares con módulos específicos aportadas por J. Singer (1938), R. C. Bose y S. Chowla (1962), e I. Z. Ruzsa (1993). En este artículo se presenta una nueva construcción de conjuntos B_h en enteros modulares, la cual puede verse como una extensión de la construcción de Ruzsa.

Palabras y frases claves: Conjuntos de Sidon, Conjuntos B_h y construcciones.

1 Introducción

Sean $\langle G, + \rangle$ un grupo conmutativo notado aditivamente, $h \geq 2$ un entero y $A = \{g_1, g_2, \ldots, g_k\} \subseteq G$. A es un *conjunto B_h en G* si todas las sumas de h elementos de A (no necesariamente distintos) son diferentes. Es decir, si todas las expresiones de la forma

$$g_{i_1} + g_{i_2} + \cdots + g_{i_h}, \quad \text{con} \quad 1 \leq i_1 \leq i_2 \leq \cdots \leq i_h \leq k,$$

producen elementos distintos en G.

Cuando $h = 2$, los conjuntos B_2 se llaman *conjuntos de Sidon*; un texto introductorio a su estudio es el texto de Halberstam y Roth [6]. 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 $\mathbb{Z}_n$ se escribe $A \in B_h(\textit{mód } n)$, el cual se llama *un conjunto B_h módulo n*.

A continuación se presentan las construcciones clásicas de conjuntos B_h desde una perspectiva moderna, mediante cuerpos finitos. El siguiente lema es consecuencia directa de la definición de conjunto B_h y se utilizará para importar conjuntos B_h en un grupo cíclico a los enteros modulares.

Lema 1. *Sean $\langle G_1, + \rangle$ y $\langle G_2, * \rangle$ grupos conmutativos y $\varphi : G_1 \to G_2$ un homomorfismo inyectivo. Si $A \in B_h(G_1)$ entonces $\varphi(A) \in B_h(G_2)$.*

Para empezar se considera la construcción de Bose-Chowla [3], la cual generaliza la construcción de conjuntos de Sidon dada por Bose (1942) [2].

Teorema 1 (Construcción de Bose-Chowla, 1962)**.** *Para toda potencia prima q y todo $h \geq 2$ entero, existe un conjunto $B_h(\text{mód } q^h - 1)$ con q elementos.*

Demostración. Sea $\theta \in \mathbb{F}_{q^h}$ un elemento primitivo, entonces el polinomio minimal de θ tiene grado h y $\mathbb{F}_{q^h}^\star = \langle\theta\rangle$ (grupo cíclico generado por θ). A continuación se demostra que el conjunto

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

es un conjunto $B_h(\mathbb{F}_{q^h}^\star)$ multiplicativo, donde $\mathbb{F}_{q^h}^\star$ denota el grupo de unidades de $\mathbb{F}_{q^h}$.

Supóngase lo contrario, que se da la igualdad de dos productos de h elementos de $\theta + \mathbb{F}_q$

$$\prod_{k=1}^{h}(\theta + a_{i_k}) = \prod_{k=1}^{h}(\theta + a_{j_k}),$$

donde

$$\begin{gathered} 1 \leq i_1 \leq i_2 \leq \cdots \leq i_h \leq q, \qquad 1 \leq j_1 \leq j_2 \leq \cdots \leq j_h \leq q, \\ (i_1, i_2, \ldots, i_h) \neq (j_1, j_2, \ldots, j_h). \end{gathered} \tag{1}$$

Entonces por (1), el polinomio

$$p(X) = \prod_{k=1}^{h}(X + a_{i_k}) - \prod_{k=1}^{h}(X + a_{j_k}) \in \mathbb{F}_q[X]$$

es no nulo, tiene $g_r(p) < h$ y se anula en θ, lo cual no es posible.

Ahora, en virtud del Lema 1, el conjunto

$$\log_\theta(\theta + \mathbb{F}_q) := \{\log_\theta(a + \theta) : a \in \mathbb{F}_q\}, \tag{2}$$

es un conjunto $B_h(\text{mód } q^h - 1)$ bajo el isomorfismo

$$\begin{aligned} \log_\theta \;:\; \mathbb{F}_{q^h}^\star &\to \mathbb{Z}_{q^h-1}, \\ \theta^k &\to k \end{aligned}$$

llamado *logaritmo discreto base θ.* □

Observación 1. *Nótese que la contradicción a la que se llega en la demostración anterior consiste en que θ no puede ser cero de un polinomio de grado menor que h, para lo cual no es necesario tomar un elemento primitivo para sumar a $\mathbb{F}_q$, bastará con que se considere en su lugar $\beta \in \mathbb{F}_{q^h}$ de grado h sobre $\mathbb{F}_q$. Así,*

$$\beta + \mathbb{F}_q, \quad \textit{con } h \textit{ el grado de } \beta \textit{ sobre } \mathbb{F}_q$$

es un conjunto B_h multiplicativo en $\mathbb{F}^\star_{q^h}$. Sin embargo para el logaritmo discreto si es necesario un elemento primitivo. Así,

$$log_\theta(\beta + \mathbb{F}_q), \quad \textit{con } h \textit{ el grado de } \beta \textit{ sobre } \mathbb{F}_q,$$

es un $B_h(\text{mód } q^h-1)$. En particular si θ es un elemento primitivo de $\mathbb{F}_{q^h}$, entonces

$$i\theta + \mathbb{F}_q, \quad \textit{para cada } i \textit{ fijo en } \mathbb{F}^\star_q,$$

es un conjunto B_h en $\mathbb{F}^\star_{q^h}$, puesto que $i\theta$ también tiene grado h sobre $\mathbb{F}_q$ para cada i en $\mathbb{F}^\star_q$. Aunque resulta insignificante tomar $i\theta$ en lugar de θ en (2), la verdadera razón es que variando $i \in \mathbb{F}^\star_q$ se tendrán conjuntos $B_h(\text{mód } q^h-1)$ disjuntos, que hacen parte de una partición de $\mathbb{Z}_{q^h-1}$, ver [5].

La siguiente construcción aparece como el primer ejemplo de conjuntos de Sidon (1938) [1], sin relación aparente con la construcción de Bose. Pero actualmente, su generalización puede verse derivada de un conjunto B_h tipo Bose-Chowla como sigue.

Teorema 2 (Construcción de Singer generalizada, Bose-Chowla, 1962)**.** *Para toda potencia prima q y todo $h \geq 2$ entero, existe un conjunto $B_h(\text{mód } m)$ con $q+1$ elementos, donde $m = (q^{h+1}-1)/(q-1)$.*

Demostración. De nuevo, sea $\theta \in \mathbb{F}_{q^{h+1}}$ un elemento primitivo, entonces el polinomio minimal de θ tiene grado $h+1$ y $\mathbb{F}^\star_{q^{h+1}} = \langle\theta\rangle$. Antes que todo, nótese que $\mathbb{F}^\star_q$ es un subgrupo del grupo $\mathbb{F}^\star_{q^{h+1}}$ y que el grupo cociente $\mathbb{F}^\star_{q^{h+1}}/\,\mathbb{F}^\star_q$ es cíclico de orden $(q^{h+1}-1)/(q-1)$.

Ahora, se muestra que las clases de equivalencias módulo $\mathbb{F}^\star_q$

$$\{\overline{\theta + a} \,:\, a \in \mathbb{F}_q\} \cup \{\overline{1}\},$$

forman un conjunto B_h multiplicativo en $\mathbb{F}^\star_{q^{h+1}}/\,\mathbb{F}^\star_q$.

Supóngase que

$$1^{h-r}\prod_{k=1}^{r}(\theta + a_{i_k}) \;\equiv\; 1^{h-s}\prod_{k=1}^{s}(\theta + a_{j_k}) \;(\; \textit{mód } \mathbb{F}^\star_q \;),$$

con

$$\begin{gathered} 1 \leq i_1 \leq i_2 \leq \cdots \leq i_r \leq q, \qquad 1 \leq j_1 \leq j_2 \leq \cdots \leq j_s \leq q, \\ r, s \leq h. \end{gathered} \tag{3}$$

Entonces, para algún $\alpha \in \mathbb{F}^\star_q$,

$$\prod_{k=1}^{r}(\theta + a_{i_k}) = \alpha \prod_{k=1}^{s}(\theta + a_{j_k}),$$

y así, como consecuencia de (3), θ es raíz del polinomio de grado $\leq h$

$$p(X) = \alpha \prod_{k=1}^{s}(X + a_{j_k}) - \prod_{k=1}^{r}(X + a_{i_k}) \in \mathbb{F}_q[X],$$

lo cual sólo es posible si $p(X) = 0$. De esta forma, $r = s$, $\alpha = 1$ y

$$\{a_{i_k}\} = \{a_{j_k}\}.$$

Por último, como $\mathbb{F}^{\star}_{q^{h+1}}/\mathbb{F}^{\star}_q \cong \mathbb{Z}_m$, para $m = (q^{h+1} - 1)/(q - 1)$, del Lema 1 se tiene la conclusión del teorema. □

Observación 2. *Es importante resaltar de esta última construcción, que a partir de un conjunto B_{h+1} tipo Bose-Chowla se ha construido un conjunto B_h, variando adecuadamente los módulos y con la salvedad de un elemento más.*

Finalmente en el año 1993, aparece una nueva construcción de conjuntos de Sidon, la construcción de Ruzsa [4].

Teorema 3 (Construcción de Ruzsa, 1993)**.** *Para todo primo p, existe una colección $x_1, x_2, \ldots, x_{p-1}$ de $p - 1$ enteros, que es un conjunto de Sidon módulo $p^2 - p$.*

Demostración. Sea g una raíz primitiva módulo p. Considérese el conjunto

$$\{\,(i, g^i) \;:\; i = 1, 2, \cdots p - 1\} \subseteq \mathbb{Z}_{p-1} \times \mathbb{Z}_p, \tag{4}$$

el cual resulta ser es un conjunto de Sidon en el grupo $\mathbb{Z}_{p-1} \times \mathbb{Z}_p$ con la suma componente a componente.

Sea $(i, g^i) + (j, g^j) = (r, s) \in \mathbb{Z}_{p-1} \times \mathbb{Z}_p$, entonces

$$r = i + j \quad \text{en} \quad \mathbb{Z}_{p-1} \qquad \text{y} \qquad s = g^i + g^j \quad \text{en} \quad \mathbb{Z}_p.$$

De manera equivalente

$$g^r = g^i g^j \qquad \text{y} \qquad s = g^i + g^j, \quad \text{en} \quad \mathbb{Z}_p.$$

De esta forma, g^i y g^j son raíces del polinomio $P(X) = X^2 - sX + g^r \in \mathbb{Z}_p[X]$, el cual no puede tener mas de dos raíces. Así (r, s) son únicos.

Usando el Teorema Chino de los Restos, en el lema 1, con las siguientes ecuaciones de congruencias

$$x_i \equiv g^i \ (\textit{mód}\ p),$$
$$x_i \equiv i \ (\textit{mód}\ p - 1),$$

para $i = 1, 2, \ldots, p - 1$, se prueba el teorema. □

En la Sección 2 se presenta una nueva construcción, en la que a partir de un conjunto B_{h-1} tipo Bose-Chowla se construye un conjunto B_h, y se incluyen algunas rutinas en el sistema computacional MuPAD que han sido usadas para obtener los ejemplos suministrados; para mas detalle colsultar el trabajo de investigación [7]. En la Sección 3, se propone un problema derivado de la nueva construcción, desde el punto de vista combinatorio en grupos conmutativos y se exponen algunas observaciones obtenidas mediante búsqueda computacional.

2 Nueva construcción de conjuntos B_h

Considere el cuerpo finito $\mathbb{F}_{p^{h-1}}$, para $h \geq 3$ entero y θ un elemento primitivo de este. La siguiente construcción de conjuntos B_h es una construcción en dimensión dos en el grupo $\mathbb{Z}_p \times \mathbb{Z}_{p^{h-1}-1}$.

Teorema 4 (Un conjunto B_h a partir de un conjunto B_{h-1})**.** *Para todo primo p y todo $h \geq 3$ entero, existe una colección $x_1, x_2, \ldots, x_p$ de p enteros, que es un conjunto B_h módulo $p^h - p$.*

Demostración. Considérese el conjunto

$$\mathfrak{R} = \{\, (a, \log_\theta(\theta + a)) : a \in \mathbb{Z}_p \,\} \subseteq \mathbb{Z}_p \times \mathbb{Z}_{p^{h-1}-1}. \tag{5}$$

Suponiendo que

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

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

$$\begin{aligned} \sum_{k=1}^{h} a_k &\equiv \sum_{k=1}^{h} b_k \quad (\mathit{mód}\ p) \\ \sum_{k=1}^{h} \log_\theta(\theta + a_k) &\equiv \sum_{k=1}^{h} \log_\theta(\theta + b_k) \quad (\mathit{mód}\ p^{h-1} - 1). \end{aligned}$$

De las propiedades del logaritmo discreto se tiene

$$\begin{aligned} \sum_{k=1}^{h} a_k &\equiv \sum_{k=1}^{h} b_k \quad (\mathit{mód}\ p) \\ \prod_{k=1}^{h} (\theta + a_k) &= \prod_{k=1}^{h} (\theta + b_k) \quad \text{en} \quad \mathbb{F}^{\star}_{p^{h-1}}. \end{aligned} \tag{6}$$

Por otra parte,

$$\prod_{k=1}^{h} (X + t_k) = X^h + \sigma_1(t)X^{h-1} + \sigma_2(t)X^{h-2} + \cdots + \sigma_{h-1}(t)X + \sigma_h(t), \tag{7}$$

donde $\sigma_k(t)$ es la $k-$ésima función simétrica elemental en $t = \{t_1, \ldots, t_h\}$. Por tanto para $a = \{a_1, \ldots, a_h\}$ y $b = \{b_1, \ldots, b_h\}$, de (6) y (7) se sigue

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

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

$$\sigma_k(a) \equiv \sigma_k(b) \quad (\textit{mód}\ p) \quad \text{para} \quad 1 \leq k \leq h. \tag{8}$$

De (8) y la expansión mediante funciones simétricas elementales, dada en (7)

$$\prod_{k=1}^{h} (X + a_k) \; = \prod_{k=1}^{h} (X + b_k) \quad \text{en} \quad \mathbb{Z}_p[X],$$

y puesto que $\mathbb{Z}_p[X]$ es un dominio de factorización única se concluye que $a = b$ y

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

De esta forma, $\mathfrak{R} \in B_h(\mathbb{Z}_p \times \mathbb{Z}_{p^{h-1}-1})$.

Finalmente, del Teorema Chino de los Restos y el Lema 1, se obtiene la nueva construcción de conjuntos B_h módulo $p^h - p$ con p elementos, la cual está dada por el conjunto

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

□

Observación 3. *De la misma forma puede extenderse esta construcción al grupo no cíclico* $\mathbb{F}_q \times \mathbb{Z}_{q^{h-1}-1}$ *de orden* $q^h - q$*, considerando el conjunto*

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

Observación 4. *Nótese que el conjunto dado en* (4) *puede ser expresado de la siguiente forma*

$$R = \{\, (a, \log_g(a + g)) \;:\; a + g \neq 0 \,\} \subseteq \mathbb{Z}_p \times \mathbb{Z}_{p-1},$$

lo que permite ver al conjunto de Sidon tipo Ruzsa como el caso $h = 2$ *del conjunto dado en* (5)*, con un elemento menos.*

A continuación se presentan algunos ejemplos.

Considérese θ una raíz del polinomio primitivo $x^3 + 3x + 2$ sobre $\mathbb{F}_5$; de esta forma los elementos de $\mathbb{F}^{\star}_{5^3}$ pueden ser escritos como potencias de θ. Los siguientes ejemplos están sujetos a estas consideraciones.

Ejemplo 1. *Teniendo en cuenta que*

a	0	1	2	3	4
$\theta + a$	θ	θ^{103}	θ^{119}	θ^{14}	θ^{34}

Del Teorema 2, el conjunto

$$B = \{1, 14, 34, 103, 119\},$$

es un conjunto $B_3(\,mód\ 124\,)$ *tipo Bose-Chowla. Partiendo de* B *y el Teorema 2, se tiene el conjunto*

$$\{0, 1, 3, 10, 14, 26\},$$

que es un conjunto $B_2(\,mód\ 31\,)$ *tipo Singer. Y una vez más, partiendo de* B *y el Teorema 4 se tiene que el conjunto*

$$\{34, 125, 138, 351, 367\},$$

es un conjunto $B_4(\,mód\ 620\,)$.

Finalmente, con los siguientes algoritmos se calculan ejemplo de conjuntos B_h del tipo Bose-Chowla, Singer y como en el Teorema 4, de mayor cardinalidad y módulos más grandes.

Algoritmo 1. Este algoritmo calcula un conjunto B_h tipo Bose-Chowla, creando el cuerpo finito $\mathbb{F}_{q^h}$, con $q = p^r$.

```
boseh:=proc(p,r,h)
begin
K:=Dom::GaloisField(p,h*r); t:=K::randomPrimitive();
s:=(p^(h*r)-1)/(p^r-1); s1:=p^r-1;
K::t1:=t^s; F:={}; A:={1};
for j from 1 to s1 do
F:={op(F),K::t1^j};
end_for;
for i in F do
A:={op(A),K::ln(t+i,t)};
end_for;
end_proc;
```

Algoritmo 2. Este algoritmo calcula un conjunto B_h tipo Singer, utilizando un conjunto B_h mediante el algoritmo `boseh`.

```
singerh:=proc(p,r,h)
begin
s:=(p^ ((h)*r)-1)/(p^r-1);
A:=boseh(p,r,h); A:=A union {0};
map(A,modp,s);
```

```
end_proc;
```

Algoritmo 3. Este algoritmo calcula un conjunto B_h, utilizando un conjunto B_{h-1} tipo Bose-Chowla y una construcción en dos dimensiones.

```
nuevaBh:=proc(p,h)
begin
h1:=h-1;
F:=Dom::GaloisField(p,h1); t:=F::randomPrimitive();
A1:=[[0,1]];
p1:=p-1; p2:=p^h1; p3:=p*(p2 - 1);
for a from 1 to p1 do
A1:=[op(A1),[a,F::ln(t+a,t)]];
end_for;
print(A1);
A2:={ };
for l from 1 to p do
a1:=A1[l]; a2:=a1[1]+(a1[2]-a1[1])*p2 mod p3;
A2:={op(A2),a2};
end_for;
end_proc;
```

Ejemplo 2. *En este ejemplo se considera* $p = 7$ *y* $r = 2$ *, con lo cual se construye un conjunto* B_3 *tipo Bose-Chowla con* 49 *elementos en los enteros módulo* 117648*.*

```
>> boseh(7,2,3);
```

{1, 336, 495, 1917, 5306, 8681, 10043, 14419, 16626, 19595, 25475, 28519, 29611, 31009, 31689, 31760, 32259, 32365, 33319, 36482, 38329, 38462, 43240, 47506, 49174, 53110, 55650, 60154, 60483, 64598, 66503, 69286, 72967, 74673, 76864, 89052, 89089, 89490, 90106, 95708, 97098, 102265, 106757, 109149, 109546, 109996, 100148, 114971, 116877}

Ejemplo 3. *Basado en el ejemplo anterior, se construye un conjunto* B_2 *tipo Singer con* 50 *elementos en los enteros módulo* 2451*.*

```
>> singerh(7,2,2);
```

{0, 1, 119, 154, 199, 239, 326, 336, 396, 404, 495, 502, 658, 816, 853, 872, 883, 937, 965, 1143, 1254, 1305, 1328, 1330, 1364, 1456, 1509, 1558, 1564, 1573, 1597, 1639, 1659, 1680, 1697, 1702, 1728, 1774, 1870, 1888, 1917, 1920, 2108, 2152, 2164, 2168, 2225, 2277, 2348, 2438}

Ejemplo 4. *Finalmente en este ejemplo se considera* $p = 23$*; con lo cual se construye un conjunto* B_4 *con* 23 *elementos en los enteros módulo* 279818*, construyendo primero un conjunto* B_3 *en dos dimensiones en el grupo* $\mathbb{Z}_{23} \times \mathbb{Z}_{23^3-1}$*.*

```
>> nuevaBh(23,3);
```

{ (0, 1), (1, 590), (2, 7401), (3, 9172), (4, 4125), (5, 6610), (6, 2251), (7, 2986), (8, 4555), (9, 5297), (10, 11210), (11, 10623), (12, 6142), (13, 8432), (14, 8671), (15, 3762), (16, 8163), (17, 10322), (18, 10080), (19, 8135), (20, 9014), (21, 4543), (22, 9581)}

{12167, 32080, 47388, 64403, 89659, 94235, 111740, 111917, 112482, 138733, 149424, 182898, 194647, 213729, 216832, 224614, 234012, 240311, 257011, 258373, 262424, 270366, 275463}

3 Problemas abiertos

Comparando los Teoremas 1 y 4 se hace evidente la disminución del módulo necesario para construir un conjunto B_h, $h \geq 3$ entero, con p elementos. Esto sugiere los siguientes interrogantes.

1. ¿Cuál es el mínimo módulo n, para el cual existe un conjunto $B_h(m\acute{o}d\ n)$ con k elementos? Este problema se representa con la siguiente función:

   $$\phi(k,h) := \text{mín}\{n \in \mathbb{N} : \exists A \subseteq \mathbb{Z}_n, \mid A \mid = k \wedge A \in B_h(m\acute{o}d\ n)\}.$$

   Y así por el Teorema 4, $\phi(p,h) \leq p^h - p$.

   Ahora, comparando los siguientes resultados obtenidos computacionalmente, se espera que se puedan construir mejores conjuntos B_h, con relación al orden del grupo.

   La siguiente tabla muestra el menor módulo n, inferior a los dados en las construcciones del presente artículo, con el cual se obtuvo un conjunto B_3 con k elementos por búsqueda computacional.

k	$\phi(k,3) \leq n$	Teorema 4	Tipo Singer
5	65	$5^3 - 5 = 120$	
6	120		$\frac{5^4-1}{5-1} = 156$
7	220	$7^3 - 7 = 336$	
8	330		$\frac{7^4-1}{7-1} = 600$

2. En un sentido más general, se propone el mismo interrogante en un grupo conmutativo G no necesariamente cíclico, lo cual se representa por la función:

   $$\Phi(k,h) := \text{mín}\{\mid G \mid : \exists A \subseteq G, \mid A \mid = k \wedge A \in B_h(G)\}.$$

   Y así por la observación 3, $\Phi(q,h) \leq q^h - q$.

   Esta última función tiene notables consecuencias en la construcción de códigos correctores de errores [8].

4 Agradecimientos

El primer autor agradece a la Universidad del Valle por su sistema de becas para estudios de postgrado (asistencias de docencia), que le permitió la realización de sus estudios de maestría.

Referencias

[1] Singer, J.: A Theorem in Finite Projective Geometry and Some Applications to Number Theory, Trans. Amer. Math. Soc., 43(1938), pp. 377-385.

[2] Bose, R. C.: An affine analogue Singer's theorem, J. Ind. Math. Soc. (new series), 6(1942), pp. 1-15.

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

[4] Ruzsa, I. Z.: Solving a linear equation in a set of integers I, Acta Arithmetica, 65(1993), pp. 259-268.

[5] García, G. Trujillo, C. y Velásquez, J.: Construcción de conjuntos B_h módulo m y particiones, Matemáticas: Enseñanza Universitaria, Revista de la Corporación Escuela Regional de Matemáticas, 14(2006), pp. 65-70.

[6] Halberstam, H. and Roth, K. F.: Sequences(2da edición), Springer Verlag, Mew York, 1983.

[7] Gómez, C. A.: Construcción de conjuntos B_h sobre grupos y Códigos, Tesis de Maestría, Universidad del Valle, Cali, 2008.

[8] Graham, R. L. and Sloane, N. J. A.: Lower bounds for constant weight codes, IEEE Transations on Information Theory, 26(1980), pp. 37-43.

Dirección de los autores

Carlos Alexis Gómez Ruiz — Grupo de investigación: Álgebra, Teoría de Números y Aplicaciones, Departamento de Matemáticas, Universidad del Valle, Cali-Colombia
e-mail: `alegoxz@gmail.com`

Carlos Alberto Trujillo Solarte — Grupo de investigación: Álgebra, Teoría de Números y Aplicaciones, Departamento de Matemáticas, Universidad del Cauca, Popayan-Colombia
e-mail: `trujillo@unicauca.edu.co`