CONJUNTOS B_h MÓDULO N

HERNÁN DARÍO HIDALGO PAREDES
OMAR JOSÉ VALLEJO BARCO

UNIVERSIDAD DEL CAUCA
FACULTAD DE CIENCIAS NATURALES, EXACTAS Y DE LA EDUCACIÓN
DEPARTAMENTO DE MATEMÁTICAS
POPAYÁN
2007

CONJUNTOS B_h MÓDULO N

HERNÁN DARÍO HIDALGO PAREDES
OMAR JOSÉ VALLEJO BARCO

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
2007

CONJUNTOS B_h MÓDULO N

HERNÁN DARÍO HIDALGO PAREDES
OMAR JOSÉ VALLEJO BARCO

DOCUMENTO DEL TRABAJO DE INVESTIGACIÓN, REALIZADO CON EL GRUPO DE INVESTIGACIÓN; ÁLGEBRA, TEORÍA DE NÚMEROS Y APLICACIONES DE LA ESCUELA REGIONAL DE MATEMÁTICAS E.R.M

UNIVERSIDAD DEL CAUCA
FACULTAD DE CIENCIAS NATURALES, EXACTAS Y DE LA EDUCACIÓN
DEPARTAMENTO DE MATEMÁTICAS
POPAYÁN
2007

Nota de aceptación

_____

_____

_____

Director

_____

Doctor Carlos Alberto Trujillo Solarte

Jurados

_____

Magister Jhon Jairo Bravo

_____

Profesor Diego Fernando Ruiz

Fecha de sustentación: Popayán, Noviembre 22 de 2007

AGRADECIMIENTOS

Damos gracias a Dios por permitirnos tener el privilegio de culminar esta etapa en nuestras vidas y los más sinceros agradecimientos al Dr. Carlos Alberto Trujillo Solarte, director de nuestro trabajo de grado, maestro ejemplo para cada uno de los estudiantes de nuestro programa, quien con sus enseñanzas, dedicación y paciencia nos ha motivado a ser unos verdaderos profesionales.

A cada uno de los profesores del departamento de matemáticas, a nuestros compañeros y amigos.

Mil gracias a nuestros padres por ayudarnos y poder ver ese fruto que nos han enseñado a conseguir, también a todos nuestros familiares y demás personas que conviviendo con nosotros, facilitaron la creación de un ambiente propicio para sumergirnos en el fascinante mundo de las matemáticas, los amamos pues con su esfuerzo hicieron que esta meta sea toda una realidad.

Índice general

1. Introducción General

Si X es un conjunto finito, $|X|$ denota su *cardinal*. Sean $A = \{a_1, ..., a_k\}$ un conjunto y $h \geq 2$ un entero; asociados con A y h se tienen los siguientes conjuntos:

$$\begin{aligned} A^h &= \{(a_1, ..., a_h) : a_i \in A,\ i = 1, ..., h\}, \\ A^{\{h\}} &= \{X \subset A : |X| = h\}, \\ A^{(h)} &= \left\{(a_{i_1}, ..., a_{i_h}) \in A^h : 1 \leq i_1 \leq \cdots \leq i_h \leq k\right\}. \end{aligned}$$

Así, A^h es el producto cartesiano de h copias de A y $A^{\{h\}}$ es el conjunto de subconjuntos de A con h elementos. Si $|A| = k$, se sabe que:

$$\begin{aligned} \left|A^h\right| &= k^h, \\ \left|A^{\{h\}}\right| &= \binom{k}{h} = \frac{k!}{(k-h)!h!}, \\ \left|A^{(h)}\right| &= \binom{k+h-1}{h} = \frac{(k+h-1)!}{(k-1)!h!}. \end{aligned}$$

En este trabajo, $(\mathbb{Z}_N, +)$ representa el grupo aditivo de los enteros módulo N. Utilizamos aquí el sistema de representantes de mínimo residuo no negativo, es decir $\mathbb{Z}_N = \{0, 1, 2, ..., N-1\}$.

Definición 1. $A \subseteq \mathbb{Z}_N$ es un **conjunto** B_h **módulo** N si todas las sumas módulo N de h elementos de A, no necesariamente distintos, son diferentes.

Teniendo en cuenta la definición anterior, $A \subseteq \mathbb{Z}_N$ es B_h módulo N, si para todo $x \in \mathbb{Z}_N$, la ecuación

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

sujeta a la restricción

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

tiene a lo sumo una solución en A. En tal caso, también se dice que A **pertenece a la clase** $B_h\,(mód\ N)$.

Con la notación anterior, un conjunto A está en la clase $B_h\,(mód\ N)$, si para todo $X = (a_{i_1}, ..., a_{i_h})$, $Y = (a_{j_1}, ..., a_{j_h}) \in A^{(h)}$ se tiene la implicación

$$a_{i_1} + \cdots + a_{i_h} = a_{j_1} + \cdots + a_{j_h} \Rightarrow (a_{i_1}, ..., a_{i_h}) = (a_{j_1}, ..., a_{j_h}).$$

El **problema fundamental** que se considera en este trabajo, consiste en investigar el máximo cardinal que puede tener un conjunto $B_h\,(mód\ N)$. Se trata entonces de analizar el comportamiento "asintótico" (N tendiendo a infinito) de la función

$$f_h(N) = \text{máx}\,\{|A| : A \in B_h\,(mód\ N)\}.$$

Con un argumento combinatorio se obtiene una cota superior para $f_h(N)$. En efecto, cada $X = (a_{i_1}, ..., a_{i_h}) \in A^{(h)}$ da lugar a una suma

$$\sum_{j=1}^{h} a_{i_j} \in \mathbb{Z}_N,$$

y si $A \in B_h \,(\text{mód } N)$, todas estas sumas son distintas, con lo cual

$$\frac{k^h}{h!} \leq \left|A^{(h)}\right| \leq N,$$

en consecuencia

$$\frac{k^h}{h!} \leq \binom{k+h-1}{h} \leq N.$$

Por lo tanto

$$f_h\,(N) \leq (h!N)^{1/h},$$

de donde

$$\limsup_{\mathbf{N}\to\infty} \frac{f_h(N)}{N^{1/h}} \leq (h!)^{1/h}.$$

Hasta el momento las mejores cotas superiores para $f_h(N)$ han sido obtenidas por Jia [Ji93], para h par y Chen [Ch94], para h general. Recogemos sus resultados en los siguientes teoremas.

Teorema (Jia, 1993). *Para todo $r \geq 1$, la función $f_{2r}(N)$ satisface*

$$f_{2r}(N) \leq (r!)^{1/r} N^{1/2r} + O(N^{1/4r}).$$

Teorema (Chen, 1994). *Para todo $r \geq 1$, la función $f_{2r}(N)$ satisface*

$$f_{2r}\,(N) \leq \left((r!)^2 N\right)^{1/2r} + O(1),$$

y para todo $r \geq 2$, la función $f_{2r-1}(N)$ satisface

$$f_{2r-1}(N) \leq (r!\,(r-1)!N)^{1/(2r-1)} + O(1).$$

Las demostraciones de Jia (Capítulo 2) y Chen (Capítulo 3) utilizan una variante del método de Erdös y Turán [ET41] que optimiza el conteo de "pequeñas" diferencias. En este trabajo mejoramos las cotas presentando valores explícitos de las constantes $O(1)$, implícitas en el Teorema de Chen. Nuestra demostración utiliza sólo argumentos combinatorios elementales y es diferente a las pruebas de Jia y Chen. Además, las pruebas que se presentan son válidas si se extiende el concepto de conjunto B_h a cualquier grupo conmutativo finito de orden N.

Específicamente, en el Capítulo 4 demostramos los siguientes teoremas.

TEOREMA I. *Para todo entero $r \geq 1$, la función $f_{2r}(N)$ satisface*

$$f_{2r}(N) \leq \left((r!)^2 N\right)^{1/2r} + (2r-1).$$

TEOREMA II. *Para todo entero* $r \geq 2$*, la función* $f_{2r-1}(N)$ *satisface*

$$f_{2r-1}(N) \leq (r!\,(r-1)!N)^{1/(2r-1)} + 2\,(r-1)\,.$$

En el Capítulo 2 se presenta una traducción del artículo original de Jia, del cual sólo nos interesa el Teorema 2. El Capítulo 3 corresponde a una traducción similar del artículo original de Chen, del cual nos interesa el Teorema 2. Estas traducciones se exhiben para efectos de comparación con nuestras pruebas; además se presentan las referencias bibliográficas al final de cada uno de estos capítulos. Los demás resultados y problemas mencionados en estos artículos, si bien están relacionados directamente con nuestro trabajo, deben ser objeto de futuros trabajos de grado.

Inicialmente, en el Capítulo 4 se presentan las ideas que condujeron a nuestras pruebas, para este efecto se consideran los casos particulares, $h = 2, 3, 4$, y 5. Aclaramos que las demostraciones de estos casos se realizaron considerando todas las combinaciones posibles de expresiones (sumas y diferencias) asociadas con ciertos subconjuntos de un conjunto $B_h(\textit{mód } N)$, pero debido a la simetría y semejanza de tales combinaciones, sólo se tratan algunas de ellas en detalle.

Finalmente, en el Capítulo 5 se presentan las conclusiones de nuestro trabajo, especialmente un aspecto relacionado con posibles mejoras de las cotas superiores obtenidas en los Teoremas I y II, también se mencionan algunos problemas abiertos relacionados con la temática desarrollada en este trabajo.

2. El Artículo de Jia (1993)

En este capítulo aparece la traducción completa del artículo:

> [Ji93] Xing-De Jia, *On Finite Sidon Sequences*, Journal of Number Theory **44** (1993), 84-92.

2.1. Introducción

Sea $h \geq 2$ un entero. Un conjunto A se llama una sucesión B_h si todas las sumas $a_1 + a_2 + \cdots + a_h$, $a_i \in A$, $i = 1, 2, ..., h$, son distintas excepto por reorganización de los sumandos. Una sucesión B_h también se llama una *sucesión de Sidon* de orden h. Sidon [9] fue quien consideró tales sucesiones en conexión con la teoría de series de Fourier.

Un conjunto finito A es una sucesión B_h para $\mathbb{Z}/(n)$ si todas las sumas de h elementos no necesariamente distintos son distintas módulo n. En este artículo estamos interesados en algunas funciones extremas relacionadas con sucesiones de Sidon finitas, las cuales se definen como sigue.

Con $h \geq 2$ y $k \geq 1$ dados, sea $\phi(h,k)$ el mínimo n tal que existe A sucesión B_h para $\mathbb{Z}/(n)$, con $|A| = k$; sea $\Phi(h,k)$ el mínimo n tal que existe A sucesión B_h contenida en $\{1, ..., n\}$ con $|A| = k$.

Con $h \geq 2$ y n dado, sea $f_h(n)$ *el máximo cardinal de una sucesión* B_h *para* $Z/(n)$; sea $F_h(n)$ el máximo cardinal de una sucesión B_h contenida en $\{1, ..., n\}$.

Con $k \geq 1$ y n dados, sea $h_k(n)$ el máximo h tal que existe A sucesión B_h para $\mathbb{Z}/(n)$, con $|A| = k$; sea $H_k(n)$ el máximo h tal que existe A sucesión B_h contenida en $\{1, ..., n\}$ con $|A| = k$.

Para cualquier $h \geq 2$ fijo, la cota superior para $F_h(n)$ es

$$F_h(n) \leq (h \cdot h!)^{1/h} n^{1/h}.$$

Esto se debe a que si A es una sucesión B_h finita contenida en $\{1, ..., n\}$ con $|A| = k$, entonces

$$hn \geq \binom{k+h-1}{h} \geq \frac{k^h}{h!}. \tag{2.1}$$

Erdös y Turán [4] (ver también [6]) probaron que

$$F_2(n) < \sqrt{n} + O\left(\sqrt[4]{n}\right).$$

Por otro lado, Bose y Chowla [1] demostraron que para todo $h \geq 2$, existe A sucesión B_h para $\mathbb{Z}/\left(m^h - 1\right)$ con $|A| = m$, donde m es una potencia prima. Este teorema implica que

$$F_h(n) \geq (1 + o(1)) n^{1/h}.$$

Por lo tanto,

$$F_2(n) = (1 + o(1))\sqrt{n}. \tag{2.2}$$

$\phi(2,k)$ y $\Phi(2,k)$ fueron estudiadas por Graham y Sloane [5] en conexión con el problema de rotulamiento de grafos en teoría de grafos. En este artículo se prueban algunas estimaciones para esas funciones extremas. Por ejemplo, se prueba que para cualquier $r \geq 1$ fijo cuando $n \to \infty$,

$$\begin{aligned} F_{2r}(n) &\leq r^{1/2r}(r!)^{1/r} n^{1/2r} + O\left(n^{1/4r}\right), \\ f_{2r}(n) &\leq (r!)^{1/r} n^{1/2r} + O\left(n^{1/4r}\right). \end{aligned}$$

En particular, se obtiene que

$$\begin{aligned} F_4(n) &\leq 8^{1/4} n^{1/4} + O\left(n^{1/8}\right) \approx 1{,}6818 n^{1/4} + O\left(n^{1/8}\right), \\ f_4(n) &\leq \sqrt{2} n^{1/4} + O\left(n^{1/8}\right) \approx 1{,}4142 n^{1/4} + O\left(n^{1/8}\right). \end{aligned}$$

Al final de este artículo también se discuten algunos problemas abiertos relacionados con sucesiones de Sidon.

2.2. Resultados Principales.

Partiendo de la definición se tiene que

$$\begin{aligned} \Phi(h,k) &\leq \phi(h,k) \text{ para } h \geq 2,\ k \geq 1, \\ F_h(n) &\geq f_h(n) \text{ para } h \geq 2,\ n \geq 2, \\ H_k(n) &\geq h_k(n) \text{ para } h \geq 2,\ n \geq 2. \end{aligned}$$

Teorema 1. *Se tienen las siguientes estimaciones:*

(i) *Para cualquier $h \geq 2$ fijo,*

$$\frac{1}{h!} \leq \lim_{k\to\infty} \inf \frac{\phi(h,k)}{k^h} \leq 1.$$

(ii) *Para cualquier $h \geq 2$ fijo cuando $k \to \infty$,*

$$\frac{k^h}{h \cdot h!} \leq \Phi(h,k) \leq (1 + o(1))\, k^h.$$

(iii) *Para cualquier $h \geq 2$ fijo,*

$$1 \leq \lim_{n\to\infty} \sup \frac{f_h(n)}{n^{1/h}} \leq (h!)^{1/h}.$$

(iv) *Para cualquier* $h \geq 2$ *fijo cuando* $n \to \infty$,

$$(1 + o(1))\, n^{1/h} \leq F_h(n) \leq (h \cdot h!)^{1/h}\, n^{1/h};$$

(v) *para cualquier* $k \geq 2$ *fijo cuando* $n \to \infty$,

$$n^{1/(k-1)} - 2 < h_k(n) \leq ((k-1)!)^{1/(k-1)}\, n^{1/(k-1)}.$$

(vi) *Para cualquier* $k \geq 3$ *fijo cuando* $n \to \infty$,

$$(n-1)^{1/(k-2)} - 2 < H_k(n) \leq ((k-1)!)^{1/(k-2)}\, n^{1/(k-2)}.$$

Prueba. Sea A una sucesión B_h para $\mathbb{Z}/(n)$ con $|A| = k$. Entonces

$$n \geq \binom{k+h-1}{h}. \tag{2.3}$$

Luego, para cualquier $h \geq 2$ fijo, $n \geq k^h/h!$ implica la cota inferior en (i) y la cota superior en (iii). Se sigue del teorema de Bose-Chowla que $\phi(h,k) \leq k^h - 1$ si k es una potencia prima. Esto implica la cota superior en (ii) y la cota inferior en (iii).

Sea A una sucesión B_h contenida en $\{1, ..., n\}$ con $|A| = k$. Entonces (2.1) implica la cota inferior en (ii) y la cota superior en (iv). La cota superior en (ii) y la cota inferior en (iv) se sigue inmediatamente del Teorema de Bose-Chowla y el hecho que $p - p' = o(p)$ si p, p' son primos consecutivos. Sea A una sucesión B_h para $\mathbb{Z}/(n)$ con $|A| = k$. Entonces se sigue de (2.3) que para todo $k \geq 2$ fijo,

$$h \leq ((k-1)!)^{1/(k-1)}\, n^{1/(k-1)},$$

que implica la cota superior en (v). Para probar la cota inferior en (v), sea

$$A = \left\{0, 1, h+1, (h+1)^2, ..., (h+1)^{k-2}\right\},$$

donde $h = \left\lfloor n^{1/(k-1)} \right\rfloor - 1$. Entonces A es una sucesión B_h. Como

$$n \geq (h+1)^{k-1} > h\,(h+1)^{k-2},$$

se ve que A es una sucesión B_h para $\mathbb{Z}/(n)$ y de aquí

$$n^{1/(k-1)} - 2 < h_k(n).$$

Sea A una sucesión B_h contenida en $\{1, 2, ..., n\}$ con $|A| = k$. La cota superior de $H_k(n)$ en (vi) se sigue inmediatamente de (2.1). Para ver la cota inferior de $H_k(n)$, se define $h = \left\lfloor (n-1)^{1/(k-2)} \right\rfloor - 1$ y

$$A_1 = \left\{1, 2, h+2, (h+1)^2 + 1, ..., (h+1)^{k-2} + 1\right\}.$$

Como A_1 es sólo una traslación de A, A_1 es también una sucesión B_h. Notando

$$(h+1)^{k-2}+1 \leq \left((n-1)^{1/(k-2)}-1+1\right)^{k-2}+1=n,$$

se ve que $(n-1)^{1/(k-2)}-2<H_k(n)$.

La prueba del Teorema 1 está completa. □

Teorema 2. $f_{2r}(n) \leq (r!)^{1/r} n^{1/2r} + O\left(n^{1/4r}\right)$.

Prueba. Sea $k=f_{2r}(n)$. Sea A una sucesión B_{2r} para $\mathbb{Z}/(n)$ con $|A|=k$. Sea $B=rA$, donde rA denota el conjunto de todas las sumas de r elementos no necesariamente distintos de A. Aunque rA no es necesariamente una sucesión B_2 para $\mathbb{Z}/(n)$, está suficientemente cercana a una para que el argumento de Erdös y Turán [4] (ver también [6, Teorema 4. p. 86]) pueda aplicarse.

Como A es una sucesión B_{2r} para $\mathbb{Z}/(n)$, se puede asumir sin pérdida de generalidad que B es un subconjunto de $[1,n]$. Si $|B|=t$, entonces

$$t=\binom{k+r-1}{r} \geq \frac{k^r}{r!}. \tag{2.4}$$

Sea u un entero positivo menor que n (a ser escogido más tarde) e $I_m=[-u+m,-1+m]$ para $m=1,2,...,n+u$. Cada entero $c\in[0,n]$ está precisamente en u intervalos I_m y por lo tanto, si B_m denota el número de elementos de B en el intervalo I_m, entonces

$$\sum_{m=1}^{n+u} B_m = tu,$$

luego, por el argumento de Erdös y Turán,

$$\frac{1}{2}tu\left(\frac{tu}{n+u}-1\right) \leq \sum_{m=1}^{n+u}\frac{1}{2}B_m\left(B_m-1\right). \tag{2.5}$$

Así, de (2.4), (2.5) y el hecho que $n>u$,

$$\frac{k^r}{r!} \leq t \leq \frac{n}{u}+\left\{\frac{2\left(n+u\right)}{u^2}\sum_{m=1}^{n+u}\frac{1}{2}B_m\left(B_m-1\right)+\frac{n^2}{u^2}\right\}^{1/2}. \tag{2.6}$$

Por otro lado, la suma en el lado derecho de (2.5) cuenta el número de todos los pares b,b' de B que satisfacen $b'-b=d$, $1\leq d\leq u-1$. El par que corresponde a un d particular, $1\leq d\leq u-1$, ocurre en exactamente $u-d$ de los intervalos I_m. Si B fuese una sucesión B_2, debería corresponder a cada d a lo sumo un par b,b' y sería posible concluir que la suma en el lado derecho de (2.5) es a lo sumo

$$\sum_{d=1}^{n-1}\left(u-d\right)=\frac{1}{2}u\left(u-1\right).$$

Ahora se prueba que aunque B no es una sucesión B_2, está cerca de serlo.

Sea

$$V = \{(b, b') : 0 < b' - b < u; b, b' \in B\},$$

y sean

$$b = a_1 + \cdots + a_r, \tag{2.7}$$
$$b' = a'_1 + \cdots + a'_r, \tag{2.8}$$

las representaciones esencialmente únicas de b y b' respectivamente como sumas de r elementos de A. Considere

$$V = V_0 \cup V_1$$

como la partición de V, en la cual (b, b') está en V_0 sí y sólo si las representaciones (2.7) y (2.8) no tienen sumandos comunes, y de otra forma está en V_1.

Se sigue de (2.3) con $h = 2r$ que

$$k \ll n^{1/2r}.$$

Por lo tanto,

$$|V_1| \leq k^{2r-1} \ll n^{(2r-1)/2r},$$

y así los pares $(b, b') \in V_1$ contribuyen en una cantidad $\ll (u-1)\, n^{(2r-1)/2r}$ a la suma en el lado derecho de (2.5).

Volviendo a V_0, sea $\mu : V_0 \to [1, u-1]$ la aplicación dada por

$$\mu(b, b') = b' - b.$$

Si cada uno de los pares

$$(b, b') = (a_1 + \cdots + a_r, a'_1 + \cdots + a'_r)$$
$$(b'', b''') = (a''_1 + \cdots + a''_r, a'''_1 + \cdots + a'''_r)$$

está en V_0 y $\mu(b, b') = \mu(b'', b''')$, entonces

$$a_1 + \cdots + a_r + a'''_1 + \cdots + a'''_r = a'_1 + \cdots + a'_r + a''_1 + \cdots + a''_r.$$

Como A es una sucesión B_{2r}, esto ocurre si

$$\{a_1, ..., a_r\} = \{a''_1, ..., a''_r\}$$

y

$$\{a'_1, ..., a'_r\} = \{a'''_1, ..., a'''_r\},$$

lo cual implica que $(b, b') = (b'', b''')$. Luego, para cada $d \in \{1, 2, ..., u-1\}$ hay a lo sumo un $(b, b') \in V_0$ tal que $\mu(b, b') = d$, por lo tanto

$$\sum_{m=1}^{n+u} \frac{1}{2} B_m (B_m - 1) \leq \frac{1}{2} u (u-1) + O\left(u n^{(2r-1)/2r}\right).$$

Sea n suficientemente grande y

$$u = \left\lfloor n^{1-1/(4r)} \right\rfloor .$$

Entonces de (2.6),

$$\begin{aligned} \frac{k^r}{r!} &\leq \frac{n}{u}\left\{ n + u + O\left(u^{-1}n^{2-1/2r}\right) + \frac{n^2}{u^2} \right\}^{1/2} \\ &= \frac{n}{u} + n^{1/2}\left\{ 1 + \frac{u}{n} + O\left(u^{-1}n^{1-1/2r}\right) + \frac{n}{u^{-2}} \right\}^{1/2} \\ &= n^{1/2}\left\{ 1 + O\left(n^{-1/4r}\right) \right\}. \end{aligned}$$

Luego

$$k \leq (r!)^{1/r} n^{1/2r}\left(1 + O\left(n^{-1/4r}\right)\right).$$

La prueba del Teorema 2 está completa. □

Corolario 1. *Para todo r fijo cuando* $k \to \infty$,

$$\phi(2r, k) \geq \frac{k^{2r}}{r!} + o\left(k^{2r}\right).$$

Corolario 2. *Tenemos*

$$\lim\sup_{n\to\infty} \frac{f_2(n)}{\sqrt{n}} = 1.$$

Un argumento similar a la prueba del Teorema 2 conduce al siguiente teorema. Note que si A está contenido en $\{1, 2, ..., n\}$ entonces rA está contenido en $\{1, 2, ..., rn\}$.

Teorema 3. *Para todo r fijo, cuando* $n \to \infty$,

$$F_{2r}(n) \leq r^{1/2r} r! n^{1/2r} + O\left(n^{1/4r}\right).$$

En particular se obtiene (2.2). Junto con (iv) en el Teorema 1, también tenemos

$$(1 + o(1))\, n^{1/4} \leq F_4(n) \leq 8^{1/4} n^{1/4} + O\left(n^{1/8}\right) \approx 1{,}6818 n^{1/4} + O\left(n^{1/4}\right).$$

El siguiente corolario se obtiene del Teorema 3.

Corolario 3. *Para todo r fijo, cuando* $k \to \infty$,

$$\Phi(2r, k) \geq \frac{k^{2r}}{r \cdot (r!)^2} + O\left(k^{(2r-1)/2}\right).$$

2.3. Problemas y Observaciones

Sea $n = k^h - 1$, donde k es una potencia prima. Bose y Chowla probaron que existe A sucesión B_h para $\mathbb{Z}/(n)$ con $|A| = k$. Esto sugiere la siguiente pregunta: ¿Es verdad que para todo $h \geq 2$ y todo n grande, existe A sucesión B_h para $\mathbb{Z}/(n)$ con $|A| = (1 + o(1)) n^{1/h}$? En otras palabras, ¿es verdad que

$$f_h(n) \geq (1 + o(1)) n^{1/h}$$

para todo $h \geq 2$ fijo cuando $n \to \infty$? No se ha podido probar o refutar aún en el caso inicial cuando $h = 2$.

Del Teorema 3 y el teorema de Bose y Chowla, se tiene

$$(1 + o(1)) n^{1/2r} \leq F_{2r}(n) \leq r^{1/2r} (r!)^{1/r} n^{1/2r} + O\left(n^{1/4r}\right).$$

¿Es verdad que, para todo $h \geq 2$ fijo cuando $n \to \infty$,

$$F_h(n) = (1 + o(1)) n^{1/h}?$$

Si se restringe a considerar únicamente sumas de elementos *distintos*, es posible definir algunas funciones análogas. Por ejemplo, $F_h^*(n)$ es el cardinal de un conjunto máximo $A \subseteq [1, n]$ con la propiedad que todas las sumas de h elementos distintos de A son diferentes (un conjunto A con esta propiedad no es necesariamente una sucesión B_h, podría llamarse una *semisucesión* B_h). Algunas de estas funciones extremas están relacionadas con rotulamiento de grafos (ver [5]). Graham y Sloane [5] probaron que

$$F_2^*(n) = (1 + o(1)) n^{1/2}.$$

Erdös [2] conjeturó que

$$F_h^*(n) = (1 + o(1)) n^{1/h}.$$

En general, ¿existe una constante $c = c(h) > 0$ tal que todo grupo finito G de orden n contiene A sucesión B_h (o *semisucesión* B_h) con $|A| > cn^{1/h}$? ¿Cuál es la menor constante? ¿Es igual a 1? Ciertamente se pueden definir funciones análogas a las que se han definido para $\mathbb{Z}/(n)$.

Sea $A(n)$ la función contadora del conjunto A. Un problema abierto en teoría de números aditiva es probar o refutar lo siguiente:

$$\liminf_{n\to\infty} A(n) \left(\frac{\log n}{n}\right)^{1/h} < \infty \text{ para toda } A \text{ sucesión } B_h. \tag{2.9}$$

Erdös [2] probó (2.9) en el caso $h = 2$, y Nash [8] probó el caso $h = 4$. Recientemente, Jia [7] probó (2.9) en el caso cuando h es un número par suponiendo que $A\left(n^2\right) \ll A(n)^2$ para todo n suficientemente grande. Se puede ver que la condición $A\left(n^2\right) \ll A(n)^2$ no es necesariamente cierta para A sucesión B_h. Sin embargo, se piensa que (2.9) es verdad para toda sucesión B_h.

REFERENCIAS

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

2. P. Erdös, *Some problems and results on combinatorial number theory*, preprint.

3. P. Erdös an R. Freud, *On sums of a Sidon-sequence*, J. Number Theory **38** (1991), 191-205.

4. P. Erdös and P. Turán, *On a problem in additive number theory, and some related problems*, J. Lond. Math. Soc. (2) **16** (1941), 212-215; addendum (by P. Erdös), J. London Math. Soc. (2) **19** (1944), 208.

5. R. L. Graham and N. J. A. Sloane, *On additive bases and harmonious graphs*, SIAM J. Alg. Disc. Meth. **1** (1980), 382-404.

6. H. Halberstam and K. F. Roth, "Sequences", Springer-Verlag, New York, 1983.

7. X.-D. Jia, *On B_{2k}-sequences*, J. Number Theory, to appear.

8. J. C. M. Nash, *On B_4-sequences*, Canad. Math. Bull. **32** (1989), 446-449.

9. S. Sidon, *Ein Satz über trigonometrische Polynome und seine Anwendungen in der Theorie der Fourier-Reihen*, Math. Ann. **106** (1932), 536.539.

3. El Artículo de Chen (1994)

En este capítulo aparece la traducción completa del artículo:

> [Ch94] Sheng Chen, *On the size of finite Sidon sequences*, Proceedings of the American Mathematical Society, **121** (1994), 353-356.

Sea $h \geq 2$ un entero. Un conjunto de enteros positivos B se llama una sucesión B_h si todas las sumas $a_1 + a_2 + \cdots + a_h$, $a_i \in B$, $i = 1, 2, ..., h$, son distintas excepto por reorganización de los sumandos.

Una sucesión B_h también se llama una sucesión de Sidon de orden h, ver [6]. Decimos que B es una sucesión B_h para $\mathbb{Z}/(n)$ si B es una sucesión B_h finita y todas las sumas son distintas módulo n.

Sean $F_h(n)$ el cardinal de una sucesión B_h máxima contenida en el conjunto $\{1, 2, ..., n\}$ y $f_h(n)$ el cardinal de una sucesión B_h para $\mathbb{Z}/(n)$.

Entonces se sigue de un argumento combinatorio que

$$F_h(n) \leq (h \cdot h!)^{1/h} n^{1/h} \quad \text{y} \quad f_h(n) \leq (h!)^{1/h} n^{1/h}.$$

Erdös y Turán [2] probaron que $F_2(n) < \sqrt{n} + O\left(n^{1/4}\right)$. Por otro lado, Bose y Chowla [1] demostraron que para todo $h \geq 2$, existe B sucesión B_h para $\mathbb{Z}/\left(m^h - 1\right)$ con $|B| = m$, donde m es una potencia prima. Esto implica que

$$F_h(n) \geq (1 + o(1)) n^{1/h}.$$

Por lo tanto, $F_2(n) = (1 + o(1)) \sqrt{n}$.

Erdös conjeturó que $F_2(n) = \sqrt{n} + O(1)$. Para $h = 3$, Lee [4] obtuvo que

$$F_3(n) \leq \left(\left(1 - \frac{1}{6 \log_2^2 n}\right) 4n\right)^{1/3}.$$

Para $h = 4$, Lindström [5] probó que

$$F_4(n) \leq (8n)^{1/4} + O(n^{1/8}).$$

Cuando $h = 2r$ $(r \geq 1)$, Jia [3] demostró que

$$F_{2r}(n) \leq \left((r!)^2 rn\right)^{1/2r} + O(n^{1/4r})$$

y

$$f_{2r}(n) \leq \left((r!)^2 n\right)^{1/2r} + O(n^{1/4r}).$$

En este artículo, se obtiene una cota superior similar para $F_{2r-1}(n)$ como también para $f_h(n)$.

Teorema 1. *Para todo* $r \geq 1$,

$$F_{2r-1}(n) \leq \left((r!)^2 n\right)^{1/(2r-1)} + O\left(n^{1/(4r-2)}\right).$$

Teorema 2. *Para todo* $r \geq 1$,

$$f_{2r}(n) \leq \left((r!)^2 n\right)^{1/2r} + O(1)$$

y

$$f_{2r-1}(n) \leq (r!\,(r-1)!n)^{1/(2r-1)} + O(1).$$

Sea B una sucesión B_{2r-1} con $|B| = k$. Sea $A = rB$ donde rB denota el conjunto de todas las sumas de r elementos no necesariamente distintos en B. Se tiene

$$t = |A| = \binom{k+r-1}{r} \geq \frac{k^r}{r!}.$$

Sea

$$V = \{(a,b) : a, b \in rB\} = V_0 \cup V_1,$$

donde $V_1 = V \setminus V_0$ y V_0 consiste de todos los elementos (a,b) tales que

$$a = \sum_{i=1}^{r} a_i \quad y \quad b = \sum_{i=1}^{r} b_i,$$

con $a_i, b_j \in B$ y $a_i \neq b_j$ para todo $1 \leq i, j \leq r$.

Lema. *Para todo entero* d*, hay a lo sumo* k/r *elementos* (a,b) *en* V_0 *tales que* $a - b = d$.

Prueba. Sean (a_i, b_i) elementos en V_0, $i = 1, 2, ..., s$, tales que $a_i - b_i = d$ para todo $1 \leq i \leq s$. Es suficiente probar que si $s > k/r$, al menos dos de los (a_i, b_i) son los mismos.

Ahora tomando $s > k/r$. Sea $a_i = \sum_{j=1}^{r} a_{ij}$ y $b_i = \sum_{j=1}^{r} b_{ij}$ donde $a_{ij}, b_{ij} \in B$. Como $|B| = k$ y $sr > k$, hay al menos dos pares (i,j) e (i',j') $(1 \leq i, i' \leq s$ y $1 \leq j, j' \leq r)$ tales que $a_{ij} = a_{i'j'}$. Por la definición de V_0, $i \neq i'$. Pero entonces se tiene $a_i - a_{ij} - b_i = a_{i'} - a_{i'j'} - b_{i'}$. Luego

$$a_i - a_{ij} + b_{i'} = a_{i'} - a_{i'j'} + b_i.$$

Como B es una sucesión B_{2r-1} y los a_{ij} y b_{ij} son mútuamente distintos, se tiene

$$\{a_{i1}, a_{i2}, ..., a_{ir}\} = \{a_{i'1}, a_{i'2}, ..., a_{i'r}\}$$

y

$$\{b_{i1}, b_{i2}, ..., b_{ir}\} = \{b_{i'1}, b_{i'2}, ..., b_{i'r}\}.$$

Por lo tanto, $(a_i, b_i) = (a_{i'}, b_{i'})$. Esto completa la prueba del lema.

Prueba del Teorema 1. Sean $u = \left\lfloor n^{(4r-3)/(4r-2)} \right\rfloor$ e $I_m = [-u+m, -1+m]$, $m = 1, 2, ..., rn+u$, $C_m = I_m \cap A$, y $c_m = |C_m|$. Entonces

$$(tu)^2 = \left(\sum_{m=1}^{rn+u} c_m \right)^2 \leq (rn+u) \sum_{m=1}^{rn+u} c_m^2.$$

Note que c_m^2 es el número de elementos $(a,b) \in V$ tales que $a, b \in C_m$. Luego $-u > a - b > u$.

Para todo entero d, $-u < d < u$, por el Lema, hay a lo sumo k/r elementos (a,b) en V_0 tales que $a - b = d$. Y cada par de estos se cuenta $u - |d|$ veces en la suma $\sum_{m=1}^{rn+u} c_m^2$.Como $|V_1| \leq O\left(k^{2r-1}\right)$ y $k \leq O\left(n^{1/(2r-1)}\right)$, se tiene

$$\begin{aligned} (tu)^2 &\leq (rn+u)\left(\left(\sum_{-u<d<u} \frac{k}{r}(u-|d|) \right) + O\left(k^{2r-1}\right) \right) \\ &= (rn+u)\left(\frac{k}{r}u^2 + O\left(k^{2r-1}\right) \right). \end{aligned}$$

Así,

$$t^2 \leq nk\left(1 + O\left(n^{-1/(4r-2)}\right)\right).$$

Luego,

$$k \leq \left((r!)^2 n \left(1 + O\left(n^{-1/(4r-2)}\right)\right)\right)^{1/(2r-1)} \leq \left((r!)^2 n\right)^{1/(2r-1)} + O\left(n^{1/(4r-2)}\right).$$

Esto prueba el Teorema 1. □

Prueba del Teorema 2. En el caso $h = 2r-1$, se utilizan los mismos A y V. Como, para cualquier $d \in \mathbb{Z}/(n)$, existen a lo sumo k/r elementos $(a,b) \in V_0$ tales que $a - b = d$, se tiene

$$t^2 = |V| = |V_0| + |V_1| \leq \frac{k}{r}n + O\left(k^{2r-1}\right).$$

Luego,

$$\frac{k^{2r}}{(r!)^2} \leq \frac{k}{r}n + O\left(k^{2r-1}\right) = \frac{k}{r}n\left(1 + O\left(n^{-1/(2r-1)}\right)\right),$$

y

$$\begin{aligned} k &\leq (r!\,(r-1)!n)^{1/(2r-1)}\left(1 + O\left(n^{-1/(2r-1)}\right)\right)^{1/(2r-1)} \\ &= (r!\,(r-1)!n)^{1/(2r-1)} + O(1). \end{aligned}$$

Esto demuestra que $f_{2r-1}(n) \leq (r!\,(r-1)!n)^{1/(2r-1)} + O(1)$. Similarmente, se obtiene $f_{2r}(n) \leq \left((r!)^2 n\right)^{1/2r} + O(1)$, que completa la prueba del Teorema 2. □

REFERENCIAS

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

2. P. Erdös an P. Turán, *On a problem in additive number theory and some related problems*, J. Number Theory **38** (1941), 191-205.

3. X.-D. Jia, *On finite Sidon sequences*, J. Number Theory **44** (1993), 84-92.

4. M. A. Lee, *On B_3 sequences*, Acta Math. Sinica **34** (1991), 67-71.

5. B. Lindström, *A remark on B_4-sequences*, J. Combin. Theory **7** (1969), 276-277.

6. S. Sidon, *Ein Satz uber trigonomietrische Polynome und seine Anwendun gen in der Theorie de Fourier-Reihen*, Math. Ann. **106** (1932), 536-539.

4. Resultados de Nuestro Trabajo

En este capítulo aparecen los resultados obtenidos durante el desarrollo de nuestro trabajo de grado.

4.1. Algunos Casos Particulares

Iniciemos aclarando que todas las operaciones se realizan en los enteros módulo N. Nuestro método general consiste en contar en el conjunto $A^{\{h\}}$, ciertas expresiones que mezclan sumas y diferencias; no solamente sumas como se hace en los trabajos de Jia y Chen.

Para la prueba de algunas afirmaciones se toman casos particulares, en los demás se procede de forma similar.

Consideramos los casos h par y h impar separadamente. En esta sección analizamos los casos particulares $h = 2$, 4 y $h = 3$, 5.

4.1.1. El caso $h = 2$

Sea A un conjunto $B_2(m\acute{o}d\ N)$. Consideremos el conjunto

$$A^{\{2\}} = \{X \subset A : |X| = 2\}.$$

Para cada $\{a, b\} \in A^{\{2\}}$ asociamos dos elementos de $\mathbb{Z}_N$ no nulos, a saber

$$a - b,$$

y su inverso aditivo

$$-a + b.$$

Estos elementos son distintos, porque si suponemos que

$$a - b = -a + b,$$

entonces

$$a + a = b + b,$$

y como A es un conjunto $B_2(m\acute{o}d\ N)$ se sigue que $a = b$, lo cual no es posible.

Por otro lado, con dos conjuntos diferentes $\{a, b\}, \{c, d\} \in A^{\{2\}}$ asociamos cuatro elementos

$$a - b, -a + b, \quad c - d, -c + d,$$

los cuales son todos distintos, porque si por ejemplo

$$a - b = c - d,$$

entonces

$$a + d = c + b,$$

y como A es un conjunto $B_2(\textit{mód } N)$, $a \neq b$ y $c \neq d$, con lo que $a = c$ y $b = d$, contrario a la suposición de que $\{a, b\}$ y $\{c, d\}$ son distintos. Los demás casos se prueban en forma similar.

Luego, si $|A| = k$ tenemos

$$2\left|A^{\{2\}}\right| = 2\binom{k}{2} = k\,(k-1)\,,$$

valores distintos en $\mathbb{Z}_N$, ninguno de los cuales es cero. Con lo anterior hemos probado la siguiente proposición.

Proposición 1. *Si A es un conjunto $B_2(\textit{mód } N)$ con k elementos, entonces*

$$k\,(k-1) \leq N-1.$$

Por ejemplo, con $N = 100$ la Proposición 1 nos dice que no hay conjuntos $B_2(\textit{mód } 100)$ con más de 10 elementos.

Una propiedad de los conjuntos $B_h(\textit{mód } N)$ que usaremos repetidamente es la siguiente.

Lema 1. *Para todo $h \geq 3$, si A es un conjunto $B_h(\textit{mód } N)$, entonces A es un conjunto $B_{h-1}(\textit{mód } N)$.*

Prueba. Se sigue inmediatamente de la definición. □

4.1.2. El caso $h = 4$

Sea A un conjunto $B_4(\textit{mód } N)$. Sabemos que

$$A^{\{4\}} = \{X \subset A : |X| = 4\}\,.$$

Para cada $\{a, b, c, d\} \in A^{\{4\}}$ asociamos seis elementos de $\mathbb{Z}_N$, a saber

$$a+b-c-d, \quad a-b+c-d, \quad -a+b+c-d,$$

y sus inversos aditivos

$$-a-b+c+d, \quad -a+b-c+d, \quad a-b-c+d.$$

Estos seis elementos son todos distintos porque, si igualamos una de estas expresiones con otra que no sea su inverso aditivo, por ejemplo

$$a+b-c-d = a-b-c+d,$$

entonces

$$b+b = d+d.$$

Como A es un conjunto $B_4(\textit{mód } N)$, también es un conjunto $B_2(\textit{mód } N)$, así se tendría que $b = d$, lo cual no es posible.

Similarmente, si igualamos una de las expresiones con su inverso aditivo, por ejemplo

$$a+b-c-d=-a-b+c+d,$$

entonces

$$a+a+b+b=c+d+c+d,$$

y como A es un conjunto $B_4(módN)$ y $\{a,b\}\cap\{c,d\}=\Phi$, lo anterior no puede ser.

Los demás casos se tratan en forma similar.

Además, ninguna de esas expresiones es igual a una diferencia de dos elementos de A, porque si existe $e,f\in A$ tal que, por ejemplo

$$a+b-c-d=e-f,$$

entonces

$$a+b+f=e+c+d,$$

que no es posible, ya que A es también un conjunto $B_3(mód\ N)$ y $\{a,b\}\cap\{c,d\}=\Phi$.

Por otro lado, para dos conjuntos diferentes $\{a,b,c,d\}$, $\{e,f,g,h\}\in A^{\{4\}}$ asociamos doce elementos, los seis correspondientes a $\{a,b,c,d\}$

$$\begin{gathered}a+b-c-d,\quad a-b+c-d,\quad -a+b+c-d,\\ -a-b+c+d,\quad -a+b-c+d,\quad a-b-c+d,\end{gathered}$$

y los seis correspondientes a $\{e,f,g,h\}$

$$\begin{gathered}e+f-g-h,\quad e-f+g-h,\quad -e+f+g-h,\\ -e-f+g+h,\quad -e+f-g+h,\quad e-f-g+h,\end{gathered}$$

los cuales son distintos porque, si por ejemplo

$$a+b-c-d=e+f-g-h,$$

entonces

$$a+b+g+h=e+f+c+d$$

y como A es un conjunto $B_4(mód\ N)$, $\{a,b\}\cap\{c,d\}=\{g,h\}\cap\{e,f\}=\Phi$, debemos tener $\{a,b\}=\{e,f\}$ y $\{c,d\}=\{g,h\}$, de donde $\{a,b,c,d\}=\{e,f,g,h\}$ contrario a la suposición que son distintos. Los demás casos se tratan en forma similar.

Luego, si $|A|=k$ tenemos

$$6\left|A^{\{4\}}\right|=6\binom{k}{4}=\frac{1}{4}k\left(k-1\right)\left(k-2\right)\left(k-3\right),$$

valores distintos en $\mathbb{Z}_N$, ninguno de los cuales es igual a una diferencia de dos elementos de A. Como hay $2\binom{k}{2}+1\ =\ k(k-1)+1$ diferencias distintas de dos elementos de A, con lo anterior se ha probado la siguiente proposición.

Proposición 2. *Si A es un conjunto $B_4(mód\ N)$ con k elementos, entonces*

$$k\left(k-1\right)\left(k-2\right)\left(k-3\right)\leq 4\left(N-k^2+k-1\right).$$

4.1.3. El caso $h = 3$

Sea A un conjunto $B_3(mód\ N)$. Consideremos el conjunto

$$A^{\{3\}} = \{X \subset A : |X| = 3\}.$$

Para cada $\{a, b, c\} \in A^{\{3\}}$ asociamos tres elementos de $\mathbb{Z}_N$, a saber

$$a + b - c, \quad a - b + c, \quad -a + b + c,$$

estos tres elementos son todos distintos porque, si se supone que

$$a + b - c = a - b + c,$$

entonces

$$b + b = c + c,$$

como A es un conjunto $B_3(mód\ N)$, también es un conjunto $B_2(mód\ N)$, así se tendría que $b = c$, lo cual no es posible. Los demás casos se prueban en forma similar.

Además, ninguna de esas expresiones es igual a un elemento de A, pues si existe $e \in A$ tal que, por ejemplo

$$a + b - c = e,$$

entonces

$$a + b = c + e,$$

y como A es un conjunto $B_2(mód\ N)$, c debe ser igual a a o a b, que no puede ser.

Por otro lado, con dos conjuntos diferentes $\{a, b, c\}$, $\{d, e, f\} \in A^{\{3\}}$ asociamos seis elementos, los tres correspondientes a $\{a, b, c\}$

$$a + b - c, \quad a - b + c, \quad -a + b + c,$$

y los tres correspondientes a $\{d, e, f\}$

$$d + e - f, \quad d - e + f, \quad -d + e + f.$$

Todos éstos elementos son distintos porque, si por ejemplo

$$a + b - c = -d + e + f,$$

entonces

$$a + b + d = e + f + c,$$

y como A es un conjunto $B_3(mód\ N)$, $a, b \neq c$ y $e, f \neq d$, debemos tener $\{a, b, c\} = \{d, e, f\}$, contrario a la suposición que son distintos. Los demás casos se tratan en forma similar.

Luego, si $|A| = k$ tenemos

$$3\left|A^{\{3\}}\right| = 3\binom{k}{3} = \frac{1}{2}k\,(k-1)\,(k-2)\,,$$

valores distintos en $\mathbb{Z}_N$, ninguno de los cuales es un elemento de A. Con lo anterior hemos probado la siguiente proposición.

Proposición 3. *Si A es un conjunto $B_3(\text{mód } N)$ con k elementos, entonces*

$$k\,(k-1)\,(k-2) \leq 2\,(N-k)\,.$$

4.1.4. El caso $h = 5$

Sea A un conjunto $B_5(\text{mód } N)$. Sabemos que

$$A^{\{5\}} = \{X \subset A : |X| = 5\}\,.$$

Para cada $\{a, b, c, d, e\} \in A^{\{5\}}$ asociamos diez elementos de $\mathbb{Z}_N$, a saber

$$\begin{array}{l} a+b+c-d-e, \quad a+b-c+d-e, \quad a-b+c+d-e, \\ -a+b+c+d-e, \quad a+b-c-d+e, \\ a-b+c-d+e, \quad -a+b+c-d+e, \quad a-b-c+d+e, \\ -a+b-c+d+e, \quad -a-b+c+d+e, \end{array}$$

los cuales son todos distintos porque, si por ejemplo

$$a+b+c-d-e = -a+b+c-d+e,$$

entonces

$$a+a = e+e,$$

como A es un conjunto $B_5(\text{mód } N)$, también es un conjunto $B_2(\text{mód } N)$, así se tendría que $a = e$, que no puede ser.

Similarmente, si por ejemplo

$$a+b+c-d-e = -a-b+c+d+e,$$

entonces

$$a+a+b+b = d+d+e+e,$$

y como A es un conjunto $B_5(\text{mód } N)$, también es un conjunto $B_4(\text{mód } N)$, así que $\{a, b\} = \{d, e\}$, lo cual no es posible.

Los demás casos se tratan en forma similar.

Además, ninguna de esas expresiones es igual a una expresión $f+g-h$, obtenida a partir de $\{f, g, h\} \in A^{\{3\}}$, con dos signos $+$ y un signo $-$, porque, si por ejemplo

$$a+b+c-d-e = f+g-h,$$

entonces

$$a+b+c+h=f+g+d+e,$$

y como A es un conjunto $B_4(m\acute{o}d\ N)$, esto no es posible, ya que $\{a,b,c\}\cap\{d,e\}=\emptyset$.

Por otro lado, con dos conjuntos diferentes $\{a,b,c,d,e\}, \{f,g,h,i,j\} \in A^{\{5\}}$ asociamos veinte elementos, los diez correspondientes a $\{a,b,c,d,e\}$

$$\begin{aligned}
&a+b+c-d-e, \quad a+b-c+d-e, \quad a-b+c+d-e,\\
&-a+b+c+d-e, \quad a+b-c-d+e,\\
&a-b+c-d+e, \quad -a+b+c-d+e, \quad a-b-c+d+e,\\
&-a+b-c+d+e, \quad -a-b+c+d+e,
\end{aligned}$$

y los diez correspondietes a $\{f,g,h,i,j\}$

$$\begin{aligned}
&f+g+h-i-j, \quad f+g-h+i-j, \quad f-g+h+i-j,\\
&-f+g+h+i-j, \quad f+g-h-i+j,\\
&f-g+h-i+j, \quad -f+g+h-i+j, \quad f-g-h+i+j,\\
&-f+g-h+i+j, \quad -f-g+h+i+j,
\end{aligned}$$

todos éstos elementos son distintos porque, si por ejemplo

$$a+b+c-d-e=f-g-h+i+j,$$

entonces

$$a+b+c+g+h=f+i+j+d+e,$$

y como A es un conjunto $B_5(m\acute{o}d\ N)$, $\{a,b,c\}\cap\{d,e\}=\emptyset$, $\{f,i,j\}\cap\{g,h\}=\emptyset$, debemos tener $\{a,b,c,d,e\}=\{f,g,h,i,j\}$, contrario a la suposición que son distintos. Los demás casos se tratan en forma similar.

Luego, si $|A|=k$ tenemos

$$10\left|A^{\{5\}}\right|=10\binom{k}{5}=\frac{1}{12}k\,(k-1)\,(k-2)\,(k-3)\,(k-4)\,,$$

valores distintos en $\mathbb{Z}_N$, ninguno de los cuales es igual a una expresión de la forma $f+g-h$, obtenida a partir de $\{f,g,h\}\in A^{\{3\}}$, éstas últimas producen $3\binom{k}{3}$ elementos distintos de $\mathbb{Z}_N$ (porque A también es un conjunto $B_3(m\acute{o}d\ N)$). Con lo anterior hemos probado la siguiente proposición.

Proposición 5. *Si A es un conjunto $B_5(m\acute{o}d\ N)$ con k elementos, entonces*

$$k\,(k-1)\,(k-2)\,(k-3)\,(k-4)\leq 12\left(N-3\binom{k}{3}\right).$$

4.2. Prueba del Teorema I (h par)

En los casos iniciales $h = 2$ y $h = 4$, consideramos expresiones de la forma $a-b$ (un + y un $-$) y $a+b-c-d$ (dos + y dos $-$), por lo tanto para generalizar debemos considerar expresiones con $h = 2r$ elementos de los cuales r llevan signo + y r llevan signo $-$, luego contamos el número total de tales expresiones que resultan ser distintas. Esta idea la generalizamos como sigue.

Sean $h = 2r$, con $r \geq 1$ y A un conjunto $B_h(m\acute{o}d\ N)$. Sabemos que

$$A^{\{h\}} = \{X \subset A : |X| = h\}.$$

Se define

$$\begin{aligned} I &= \{1, 2, ..., 2r\}, \\ P(I) &= \{\{I_0, I_1\} : I_0, I_1 \subset I,\ |I_0| = |I_1| = r,\ I_0 \cap I_1 = \Phi\}. \end{aligned}$$

Observe que $P(I)$ no es más que una partición del conjunto I en dos clases de igual cardinal.

El siguiente lema establece el número de elementos distintos de $\mathbb{Z}_N$ que podemos asociar a un subconjunto de A con h elementos.

Lema 2. *Si A es un conjunto $B_h(m\acute{o}d\ N)$ y $\{a_1, ..., a_h\} \in A^{\{h\}}$, entonces para cada par de particiones diferentes $\{I_0, I_1\}, \{J_0, J_1\} \in P(I)$, entonces*

$$\left(\sum_{i\in I_0} a_i\right) - \left(\sum_{i\in I_1} a_i\right), \quad \left(\sum_{i\in J_0} a_i\right) - \left(\sum_{i\in J_1} a_i\right),$$

son distintos.

Prueba. Si

$$\left(\sum_{i\in I_0} a_i\right) - \left(\sum_{i\in I_1} a_i\right) = \left(\sum_{i\in J_0} a_i\right) - \left(\sum_{i\in J_1} a_i\right),$$

entonces

$$\left(\sum_{i\in I_0} a_i\right) + \left(\sum_{i\in J_1} a_i\right) = \left(\sum_{i\in J_0} a_i\right) + \left(\sum_{i\in I_1} a_i\right).$$

Como A es un conjunto $B_h(m\acute{o}d\ N)$, se sigue que

$$\{a_i\}_{i\in I_0} \cup \{a_i\}_{i\in J_1} = \{a_i\}_{i\in J_0} \cup \{a_i\}_{i\in I_1},$$

y como

$$\{a_i\}_{i\in I_0} \cap \{a_i\}_{i\in I_1} = \{a_i\}_{i\in J_0} \cap \{a_i\}_{i\in J_1} = \emptyset,$$

debemos tener que

$$\{a_i\}_{i\in I_0} = \{a_i\}_{i\in J_0} \quad y\ \{a_i\}_{i\in I_1} = \{a_i\}_{i\in J_1},$$

de donde $I_0 = J_0$ e $I_1 = J_1$, luego $\{I_0, I_1\} = \{J_0, J_1\}$, lo cual no es posible porque se asumen diferentes. $\square$

El siguiente lema establece que a subconjuntos diferentes en $A^{\{h\}}$ corresponden valores distintos.

Lema 3. Sean A *un conjunto* $B_h(m\acute{o}d\ N)$,

$$X = \{a_1, ..., a_h\}, Y = \{b_1, ..., b_h\} \in A^{\{h\}},$$

con $X \neq Y$. Si $\{I_0, I_1\}, \{J_0, J_1\} \in P(I)$, *entonces*

$$\left(\sum_{i\in I_0} a_i\right) - \left(\sum_{i\in I_1} a_i\right), \quad \left(\sum_{i\in J_0} b_i\right) - \left(\sum_{i\in J_1} b_i\right),$$

son distintos.

Prueba. Si

$$\left(\sum_{i\in I_0} a_i\right) - \left(\sum_{i\in I_1} a_i\right) = \left(\sum_{i\in J_0} b_i\right) - \left(\sum_{i\in J_1} b_i\right),$$

entonces

$$\left(\sum_{i\in I_0} a_i\right) + \left(\sum_{i\in J_1} b_i\right) = \left(\sum_{i\in J_0} b_i\right) + \left(\sum_{i\in I_1} a_i\right).$$

Como A es un conjunto $B_h(m\acute{o}d\ N)$, debemos tener que

$$\{a_i\}_{i\in I_0} \cup \{b_i\}_{i\in J_1} = \{b_i\}_{i\in J_0} \cup \{a_i\}_{i\in I_1},$$

además,

$$\{a_i\}_{i\in I_0} \cap \{a_i\}_{i\in I_1} = \{b_i\}_{i\in J_0} \cap \{b_i\}_{i\in J_1} = \emptyset,$$

así que

$$\{a_i\}_{i\in I_0} = \{b_i\}_{i\in J_0}, \quad \{a_i\}_{i\in I_1} = \{b_i\}_{i\in J_1},$$

de donde $\{a_i\}_{i\in I_0} \cup \{a_i\}_{i\in I_1} = \{b_i\}_{i\in J_0} \cup \{b_i\}_{i\in J_1}$, es decir $X = Y$, lo cual no es posible pues $X \neq Y$. $\square$

De los Lemas 2 y 3, se sigue que para $h = 2r$ y $|A| = k$ se tiene

$$\begin{aligned}
\binom{2r}{r}\left|A^{\{2r\}}\right| &= \binom{2r}{r}\binom{k}{2r} \\
&= \frac{(2r)!}{(r!)^2}\frac{k\,(k-1)\cdots(k-(2r-1))}{(2r)!} \\
&= \frac{k\,(k-1)\cdots(k-(2r-1))}{(r!)^2},
\end{aligned}$$

valores distintos en $\mathbb{Z}_N$. Si utilizamos la desigualdad trivial

$$\frac{(k-(2r-1))^{2r}}{(r!)^2} \leq \frac{k\,(k-1)\cdots(k-(2r-1))}{(r!)^2},$$

obtenemos el Teorema I.

TEOREMA I. *Para todo entero $r \geq 1$, la función $f_{2r}(N)$ satisface*

$$f_{2r}(N) \leq \left((r!)^2 N\right)^{1/2r} + (2r-1).$$

4.3. Prueba del Teorema II (h impar)

En los casos iniciales $h = 3$ y $h = 5$, consideramos expresiones de la forma $a+b-c$ (dos + y un −) y $a+b+c-d-e$ (tres + y dos −), por lo tanto para generalizar debemos considerar expresiones con $h = 2r-1$, $r \geq 2$, elementos de los cuales r llevan signo + y $r-1$ llevan signo −, luego contamos el número total de tales expresiones que resultan ser distintas. Esta idea la generalizamos como sigue.

Sean $h = 2r-1$, con $r \geq 2$ y A un conjunto $B_h(mód\ N)$. Recordemos que

$$A^{\{h\}} = \{X \subset A : |X| = h\}.$$

se define

$$\begin{aligned} I &= \{1, 2, ..., 2r-1\}, \\ P(I) &= \{\{I_0, I_1\} : I_0, I_1 \subset I,\ |I_0| = r,\ |I_1| = r-1,\ I_0 \cap I_1 = \Phi\}. \end{aligned}$$

El siguiente lema establece el número de elementos distintos de $\mathbb{Z}_N$ que podemos asociar a un subconjunto de A con h elementos.

Lema 4. *Si A es un conjunto $B_h(mód\ N)$ y $\{a_1, ..., a_h\} \in A^{\{h\}}$, entonces para cada par de particiones diferentes $\{I_0, I_1\}, \{J_0, J_1\} \in P(I)$, los elementos*

$$\left(\sum_{i\in I_0} a_i\right) - \left(\sum_{i\in I_1} a_i\right), \quad \left(\sum_{i\in J_0} a_i\right) - \left(\sum_{i\in J_1} a_i\right),$$

son distintos.

Prueba. Si

$$\left(\sum_{i\in I_0} a_i\right) - \left(\sum_{i\in I_1} a_i\right) = \left(\sum_{i\in J_0} a_i\right) - \left(\sum_{i\in J_1} a_i\right),$$

entonces

$$\left(\sum_{i\in I_0} a_i\right) + \left(\sum_{i\in J_1} a_i\right) = \left(\sum_{i\in J_0} a_i\right) + \left(\sum_{i\in I_1} a_i\right).$$

Como A es un conjunto $B_h(mód\ N)$, debemos tener que

$$\{a_i\}_{i\in I_0} \cup \{a_i\}_{i\in J_1} = \{a_i\}_{i\in J_0} \cup \{a_i\}_{i\in I_1},$$

pero como

$$\{a_i\}_{i\in I_0} \cap \{a_i\}_{i\in I_1} = \{a_i\}_{i\in J_0} \cap \{a_i\}_{i\in J_1} = \emptyset,$$

se sigue que

$$\{a_i\}_{i\in I_0} = \{a_i\}_{i\in J_0} \quad y \quad \{a_i\}_{i\in I_1} = \{a_i\}_{i\in J_1},$$

de donde $I_0 = J_0$ e $I_1 = J_1$, luego $\{I_0, I_1\} = \{J_0, J_1\}$, que no es posible porque se asumen diferentes. □

El siguiente lema establece que a subconjuntos diferentes en $A^{\{h\}}$ corresponden valores distintos.

Lema 5. Sean A *un conjunto* $B_h(m\acute{o}d\ N)$,

$$X = \{a_1, ..., a_h\}, Y = \{b_1, ..., b_h\} \in A^{\{h\}},$$

con $X \neq Y$. *Si* $\{I_0, I_1\}, \{J_0, J_1\} \in P(I)$, *entonces*

$$\left(\sum_{i\in I_0} a_i\right) - \left(\sum_{i\in I_1} a_i\right), \quad \left(\sum_{i\in J_0} b_i\right) - \left(\sum_{i\in J_1} b_i\right),$$

son distintos.

Prueba. Si

$$\left(\sum_{i\in I_0} a_i\right) - \left(\sum_{i\in I_1} a_i\right) = \left(\sum_{i\in J_0} b_i\right) - \left(\sum_{i\in J_1} b_i\right),$$

entonces

$$\left(\sum_{i\in I_0} a_i\right) + \left(\sum_{i\in J_1} b_i\right) = \left(\sum_{i\in J_0} b_i\right) + \left(\sum_{i\in I_1} a_i\right).$$

Como A es un conjunto $B_h(m\acute{o}d\ N)$, debemos tener que

$$\{a_i\}_{i\in I_0} \cup \{b_i\}_{i\in J_1} = \{b_i\}_{i\in J_0} \cup \{a_i\}_{i\in I_1},$$

además,

$$\{a_i\}_{i\in I_0} \cap \{a_i\}_{i\in I_1} = \{b_i\}_{i\in J_0} \cap \{b_i\}_{i\in J_1} = \emptyset,$$

así que

$$\{a_i\}_{i\in I_0} = \{b_i\}_{i\in J_0}, \quad \{a_i\}_{i\in I_1} = \{b_i\}_{i\in J_1},$$

de donde $\{a_i\}_{i\in I_0} \cup \{a_i\}_{i\in I_1} = \{b_i\}_{i\in J_0} \cup \{b_i\}_{i\in J_1}$, es decir $X = Y$, que no es posible porque $X \neq Y$. □

De los Lemas 4 y 5, se sigue que para $h = 2r-1$, $r \geq 2$, y $|A| = k$ tenemos

$$\begin{aligned}
\binom{2r-1}{r}\left|A^{\{2r-1\}}\right| &= \binom{2r-1}{r}\binom{k}{2r-1} \\
&= \frac{(2r-1)!}{(r-1)!r!}\frac{k\,(k-1)\cdots(k-2\,(r-1))}{(2r-1)!} \\
&= \frac{k\,(k-1)\cdots(k-2\,(r-1))}{(r-1)!r!},
\end{aligned}$$

valores distintos en $\mathbb{Z}_N$. Si utilizamos la desigualdad trivial

$$\frac{(k-2(r-1))^{2r-1}}{(r-1)!r!} \leq \frac{k\,(k-1)\cdots(k-2(r-1))}{(r-1)!r!},$$

obtenemos el Teorema II.

TEOREMA II. *Para todo entero $r \geq 2$, la función $f_{2r-1}(N)$ satisface*

$$f_{2r-1}(N) \leq ((r-1)!r!N)^{1/(2r-1)} + 2(r-1).$$

5. Conclusiones

Las conclusiones que mencionamos a continuación están relacionadas con algunas observaciones obtenidas a partir de nuestro trabajo, de la información sobre las mejores construcciones conocidas y de las tablas que hemos calculado sobre la función $f_h(N)$. Además planteamos algunos interrogantes, un problema abierto, y posibles mejoras de nuestros teoremas, como también algunas sugerencias para futuros trabajos de grado.

5.1. Conjuntos B_2 (**mód** N)

No es posible mejorar la cota inferior de la Proposición 1

$$k\,(k-1) \leq N-1,$$

debido a la cota inferior obtenida por las construcciones.

En efecto, un resultado de S. Singer (ver [BCh62]) establece que: "para toda potencia prima q, existe un conjunto $B_2(mód\ q^2+q+1)$ con $q+1$ elementos". En este caso tenemos

$$k\,(k-1) = (q+1)\,q = q^2+q = N-1.$$

Es decir, para infinitos valores del módulo la cota de la Proposición 1 es la mejor posible.

Sin embargo, en este caso inicial hay todavía un problema abierto.

Problema abierto 1. ¿El límite

$$\lim_{N\to\infty} \frac{f_2(N)}{\sqrt{N}},$$

existe? Lo único que conocemos es que si existe debe ser 1. (Ver [ACT04]).

La mayor dificultad que se presenta para responder a este problema radica en que la función $f_2(N)$ no es necesariamente creciente. (Ver Tabla 1 del Apéndice).

5.2. Conjuntos B_3, B_4 (**mód** N)

Teniendo en cuenta los valores conocidos para la función $f_3(N)$, parece que la cota superior de la Proposición 3

$$\binom{1}{1}k + \binom{3}{2}\binom{k}{3} = \frac{k^3-3k^2+4k}{2} \leq N,$$

no es la mejor posible. (Ver Tabla 2 del Apéndice).

Algo similar sucede con la función $f_4(N)$, la cota superior de la Proposición 2

$$1 + \binom{2}{1}\binom{k}{2} + \binom{4}{2}\binom{k}{4} \leq N,$$

no es la mejor posible.

Pensamos que se puede mejorar un poco estas cotas superiores si se analizan otras expresiones (sumas y restas) asociadas con subconjuntos de elementos de A.

En cuanto a construcciones, Bose & Chowla (ver [BCh62]) demuestran, entre otros resultados que: "para toda potencia prima q y todo $h \geq 2$, existe un conjunto $B_h(\textit{mód } q^h - 1)$ con q elementos".

Un problema interesante consiste en obtener mejores construcciones de conjuntos $B_h(\textit{mód } N)$ para $h = 3, 4$. Este problema deberá ser objeto de un futuro trabajo de grado.

5.3. Caso General

Teniendo en cuenta el análisis detallado de cada uno de los casos particulares, consideramos que es posible mejorar un poco más el resultado de los Teoremas I y II. Creemos que con algo más de cuidado se pueden demostrar los siguientes dos teoremas.

TEOREMA I'. *Para todo $r \geq 1$, si A es un conjunto $B_{2r}(\textit{mód } N)$ con k elementos, entonces:*

$$1 + \sum_{i=1}^{r} \binom{2i}{i}\binom{k}{2i} \leq N.$$

TEOREMA II'. *Para todo $r \geq 2$, si A es un conjunto $B_{2r-1}(\textit{mód } N)$ con k elementos, entonces:*

$$\sum_{i=1}^{r} \binom{2i-1}{i}\binom{k}{2i-1} \leq N.$$

Estos teoremas son muy generales, en el sentido que funcionan sobre cualquier grupo conmutativo de orden N, si generalizamos el concepto de conjuntos B_h sobre grupos conmutativos.

Estos resultados aparecerán en el artículo "Conjuntos B_h sobre grupos conmutativos finitos", el cual se encuentra en preparación y será sometido a publicación en la revista "Matemáticas: Enseñanza Universitaria" ([HTV07]).

También como futuro trabajo hay que investigar una mejora substancial en las cotas superiores, puede ser necesario considerar otras expresiones adicionales. Por ejemplo, en el caso h impar ¿qué ocurre con los inversos aditivos de las expresiones que hemos considerado? y en el caso par ¿qué ocurre con las otras expresiones?

6. Apéndice

6.1. Algunos valores iniciales de $f_2(N)$

Sea $f_2(N) = \max\{|A| : A \in B_2(\textit{mód } N)\}$. La Tabla 1 muestra los valores de $f_2(N)$ para los primeros pocos valores de N.

Fuente, *http://www.tcs.hut.fi/~haha/Zn/*

Tabla 1: Primeros valores de $f_2(N)$

N	$f(N)$	Primer conjunto lexicográficamente
1,2	1	$\{0\}$
3,6	2	$\{0, 1\}$
7,12	3	$\{0, 1, 3\}$
13	4	$\{0, 1, 3, 9\}$
14	4	$\{0, 1, 4, 6\}$
15,20	4	$\{0, 1, 3, 7\}$
21	5	$\{0, 1, 4, 14, 16\}$
22	4	$\{0, 1, 3, 7\}$
23	5	$\{0, 1, 3, 8, 14\}$
24	5	$\{0, 1, 3, 9, 20\}$
25,30	5	$\{0, 1, 3, 7, 12\}$
31	6	$\{0, 1, 3, 8, 12, 18\}$
32,34	5	$\{0, 1, 3, 7, 12\}$
35	6	$\{0, 1, 3, 7, 12, 20\}$
36	6	$\{0, 1, 3, 8, 23, 27\}$
37	6	$\{0, 1, 3, 7, 16, 26\}$
38	6	$\{0, 1, 3, 7, 17, 30\}$
39	6	$\{0, 1, 3, 7, 12, 22\}$
40	6	$\{0, 1, 3, 7, 17, 28\}$
41,47	6	$\{0, 1, 3, 7, 12, 20\}$
48	7	$\{0, 1, 3, 15, 20, 38, 42\}$
49	7	$\{0, 1, 3, 7, 27, 35, 40\}$
50	7	$\{0, 1, 3, 8, 14, 18, 30\}$
51	7	$\{0, 1, 3, 8, 12, 20, 30\}$
52	7	$\{0, 1, 3, 7, 12, 22, 35\}$
53	7	$\{0, 1, 3, 7, 12, 22, 40\}$
54	7	$\{0, 1, 3, 7, 16, 26, 37\}$
55	7	$\{0, 1, 3, 7, 12, 20, 30\}$
56	7	$\{0, 1, 3, 7, 12, 20, 41\}$

N	$f_2(N)$	Primer conjunto lexicográficamente
57	8	$\{0, 1, 3, 13, 32, 36, 43, 52\}$
58	7	$\{0, 1, 3, 7, 12, 20, 43\}$
59	7	$\{0, 1, 3, 7, 12, 20, 34\}$
60	7	$\{0, 1, 3, 7, 12, 20, 38\}$
61,62	7	$\{0, 1, 3, 7, 12, 20, 30\}$
63	8	$\{0, 1, 3, 7, 15, 20, 31, 41\}$
64	8	$\{0, 1, 3, 8, 19, 25, 29, 52\}$
65	8	$\{0, 1, 3, 11, 15, 20, 36, 42\}$
66	8	$\{0, 1, 3, 7, 12, 20, 41, 51\}$
67	8	$\{0, 1, 3, 7, 12, 20, 30, 46\}$
68	8	$\{0, 1, 3, 7, 12, 20, 43, 53\}$
69	8	$\{0, 1, 3, 7, 12, 22, 30, 56\}$
70	8	$\{0, 1, 3, 7, 12, 22, 45, 53\}$
71	8	$\{0, 1, 3, 7, 12, 22, 30, 46\}$
72	8	$\{0, 1, 3, 7, 12, 20, 34, 49\}$
73	9	$\{0, 1, 3, 7, 15, 31, 36, 54, 63\}$
74	8	$\{0, 1, 3, 7, 12, 20, 45, 59\}$
75	8	$\{0, 1, 3, 7, 12, 20, 34, 50\}$
76	8	$\{0, 1, 3, 7, 12, 20, 30, 51\}$
77	8	$\{0, 1, 3, 7, 12, 20, 30, 44\}$
78	8	$\{0, 1, 3, 7, 12, 20, 47, 57\}$
79	8	$\{0, 1, 3, 7, 12, 20, 30, 44\}$
80	9	$\{0, 1, 3, 9, 22, 27, 34, 38, 66\}$
81	8	$\{0, 1, 3, 7, 12, 20, 30, 45\}$
82	8	$\{0, 1, 3, 7, 12, 20, 34, 59\}$
83	8	$\{0, 1, 3, 7, 12, 20, 30, 44\}$
84	8	$\{0, 1, 3, 7, 12, 20, 30, 51\}$
85	9	$\{0, 1, 3, 8, 14, 29, 33, 49, 76\}$
86	9	$\{0, 1, 3, 7, 8, 17, 36, 42, 63, 74\}$

N	$f_2(N)$	Primer conjunto lexicográficamente
87	9	$\{0, 1, 3, 7, 17, 36, 49, 67, 79\}$
88	9	$\{0, 1, 3, 7, 27, 41, 52, 60, 73\}$
89	9	$\{0, 1, 3, 7, 12, 20, 35, 49, 65\}$
90	9	$\{0, 1, 3, 7, 20, 28, 51, 61, 75\}$
91	10	$\{0, 1, 3, 9, 27, 49, 56, 61, 77, 81\}$
92	9	$\{0, 1, 3, 7, 12, 20, 43, 67, 77\}$
93	9	$\{0, 1, 3, 7, 12, 20, 34, 49, 70\}$
94	9	$\{0, 1, 3, 7, 15, 24, 35, 40, 53\}$
95	9	$\{0, 1, 3, 7, 12, 20, 34, 44, 60\}$
96	9	$\{0, 1, 3, 7, 12, 20, 30, 46, 61\}$
97	9	$\{0, 1, 3, 7, 12, 20, 30, 45, 61\}$
98	9	$\{0, 1, 3, 7, 12, 20, 30, 46, 77\}$
99	9	$\{0, 1, 3, 7, 12, 20, 30, 46, 78\}$
100	9	$\{0, 1, 3, 7, 12, 20, 30, 64, 79\}$
101	9	$\{0, 1, 3, 7, 12, 20, 30, 56, 70\}$
102	9	$\{0, 1, 3, 7, 12, 20, 30, 44, 69\}$
103	9	$\{0, 1, 3, 7, 12, 20, 30, 45, 69\}$
104	9	$\{0, 1, 3, 7, 12, 20, 30, 44, 65\}$
105	9	$\{0, 1, 3, 7, 12, 20, 30, 44, 70\}$
106	9	$\{0, 1, 3, 7, 12, 20, 30, 45, 66\}$
107	10	$\{0, 1, 3, 8, 20, 46, 68, 74, 83, 97\}$
108	10	$\{0, 1, 3, 12, 26, 39, 46, 61, 79, 103\}$
109	10	$\{0, 1, 3, 7, 12, 42, 59, 78, 88, 96\}$
110	10	$\{0, 1, 3, 7, 17, 37, 49, 84, 89, 102\}$
111	10	$\{0, 1, 3, 7, 12, 20, 35, 45, 61, 75\}$
112	10	$\{0, 1, 3, 7, 16, 24, 46, 65, 75, 101\}$
113	10	$\{0, 1, 3, 7, 12, 22, 39, 59, 72, 90\}$
114	10	$\{0, 1, 3, 7, 12, 36, 55, 68, 76, 99\}$
115	10	$\{0, 1, 3, 7, 12, 27, 52, 60, 81, 99\}$

N	$f_2(N)$	Primer conjunto lexicográficamente
116	10	$\{0, 1, 3, 7, 12, 20, 36, 57, 75, 85\}$
117	10	$\{0, 1, 3, 7, 12, 20, 36, 58, 76, 90\}$
118	10	$\{0, 1, 3, 7, 12, 22, 36, 52, 75, 93\}$
119	10	$\{0, 1, 3, 7, 12, 20, 30, 44, 65, 80\}$
120	11	$\{0, 1, 3, 20, 31, 35, 45, 53, 58, 74, 114\}$
121	10	$\{0, 1, 3, 7, 12, 20, 30, 46, 86, 100\}$
122	10	$\{0, 1, 3, 7, 12, 20, 34, 49, 59, 99\}$
123	10	$\{0, 1, 3, 7, 12, 20, 30, 46, 67, 82\}$
124	10	$\{0, 1, 3, 7, 12, 20, 34, 55, 80, 95\}$
125	10	$\{0, 1, 3, 7, 12, 20, 30, 46, 90, 104\}$
126	10	$\{0, 1, 3, 7, 12, 20, 30, 55, 89, 105\}$
127	10	$\{0, 1, 3, 7, 12, 20, 30, 44, 72, 94\}$
128	10	$\{0, 1, 3, 7, 12, 20, 30, 44, 78, 93\}$
129	10	$\{0, 1, 3, 12, 20, 30, 45, 69, 95\}$
130	10	$\{0, 1, 3, 7, 12, 20, 30, 46, 78, 93\}$
131	10	$\{0, 1, 3, 7, 12, 20, 30, 44, 65, 93\}$
133	12	$\{0, 1, 3, 12, 20, 34, 38, 81, 88, 94, 104, 109\}$
134	10	$\{0, 1, 3, 7, 12, 20, 30, 44, 65, 80\}$
135	11	$\{0, 1, 3, 7, 23, 35, 49, 73, 117, 125\}$
136	11	$\{0, 1, 3, 7, 26, 35, 43, 55, 65, 76, 92\}$
137	11	$\{0, 1, 3, 7, 12, 43, 60, 73, 93, 112, 122\}$
138	11	$\{0, 1, 3, 7, 19, 65, 86, 91, 106, 114, 128\}$
139	11	$\{0, 1, 3, 7, 12, 29, 39, 62, 86, 105, 126\}$
140	11	$\{0, 1, 3, 7, 12, 27, 44, 58, 80, 93, 122\}$
141	11	$\{0, 1, 3, 7, 15, 20, 52, 61, 79, 108, 118\}$
142	11	$\{0, 1, 3, 7, 12, 27, 45, 67, 92, 113, 126\}$
143	11	$\{0, 1, 3, 7, 12, 20, 55, 70, 84, 106, 116\}$
144	11	$\{0, 1, 3, 7, 12, 22, 40, 69, 96, 113, 121\}$
145	11	$\{0, 1, 3, 7, 12, 20, 48, 69, 92, 106, 130\}$

N	$f_2(N)$	Primer conjunto lexicográficamente
146	11	$\{0, 1, 3, 7, 12, 20, 43, 58, 72, 99, 121\}$
147	11	$\{0, 1, 3, 7, 12, 20, 30, 65, 79, 111, 126\}$
148	11	$\{0, 1, 3, 7, 12, 20, 35, 45, 61, 85, 112\}$
149	11	$\{0, 1, 3, 7, 12, 20, 30, 65, 80, 112, 128\}$
150	11	$\{0, 1, 3, 7, 12, 20, 30, 44, 86, 102, 117\}$
151	11	$\{0, 1, 3, 7, 12, 20, 34, 66, 103, 113, 128\}$
152	11	$\{0, 1, 3, 7, 12, 20, 30, 74, 100, 116, 131\}$
153	11	$\{0, 1, 3, 7, 12, 20, 30, 44, 72, 98, 120\}$
154	11	$\{0, 1, 3, 7, 12, 20, 30, 44, 69, 103, 119\}$
155	11	$\{0, 1, 3, 7, 12, 20, 30, 54, 75, 97, 123\}$
156	12	$\{0, 1, 3, 10, 18, 32, 38, 43, 59, 89, 99, 112\}$
157	11	$\{0, 1, 3, 7, 12, 20, 30, 46, 84, 99, 136\}$
158	12	$\{0, 1, 3, 7, 22, 57, 89, 97, 117, 122, 135\}$
159	12	$\{0, 1, 3, 7, 30, 35, 44, 68, 90, 110, 141, 149\}$
160	11	$\{0, 1, 3, 7, 12, 20, 30, 51, 79, 103, 125\}$
161	12	$\{0, 1, 3, 8, 38, 51, 77, 108, 117, 140, 144, 150\}$
162	12	$\{0, 1, 3, 7, 12, 37, 56, 76, 91, 104, 122, 136\}$
163	12	$\{0, 1, 3, 7, 16, 41, 67, 72, 89, 109, 117, 152\}$
164	12	$\{0, 1, 3, 8, 17, 30, 49, 87, 105, 120, 130, 141\}$
165	12	$\{0, 1, 3, 7, 12, 23, 38, 51, 59, 68, 93, 125, 139\}$
166	12	$\{0, 1, 3, 8, 27, 31, 42, 64, 74, 80, 109, 149\}$
167	12	$\{0, 1, 3, 7, 16, 35, 49, 102, 113, 123, 131, 143\}$
168	13	$\{0, 1, 3, 11, 30, 34, 46, 83, 103, 108, 121, 147, 162\}$
183	14	$\{0, 1, 3, 16, 23, 28, 42, 76, 82, 86, 119, 137, 154, 175\}$

Parece conveniente investigar la siguiente función asociada con $f_2(N)$:

$$v_2(k) = \min \{N \in \mathbb{N} : \exists A \in B_2(m\acute{o}d\ N) \text{ con } |A| = k\}.$$

La siguiente tabla da los primeros valores de esta función (ver [ACT04]).

k	$v_2(k)$	Ejemplo
2	$3 = 2^2 - 1$	$\{0, 1\}$
3	$7 = 2^2 + 2 + 1$	$\{0, 1, 3\}$
4	$13 = 3^2 + 3 + 1$	$\{0, 1, 3, 9\}$
5	$21 = 2^4 + 2^2 + 1$	$\{0, 1, 4, 14, 16\}$
6	$31 = 5^2 + 5 + 1$	$\{0, 1, 3, 8, 12, 18\}$
7	$48 = 7^2 - 1$	$\{0, 1, 3, 15, 20, 38, 42\}$
8	$57 = 7^2 + 7 + 1$	$\{0, 1, 3, 13, 32, 36, 43, 52\}$
9	$73 = 2^6 + 2^3 + 1$	$\{0, 1, 3, 7, 15, 31, 36, 54, 63\}$
10	$91 = 3^4 + 3^2 + 1$	$\{0, 1, 3, 9, 27, 49, 56, 61, 77, 81\}$
11	$120 = 11^2 - 1$	$\{0, 1, 3, 20, 31, 35, 45, 53, 58, 74, 114\}$
12	$133 = 11^2 + 11 + 1$	$\{0, 1, 3, 12, 20, 34, 38, 81, 88, 94, 104, 109\}$
13	$168 = 13^2 - 1$	$\{0, 1, 3, 11, 30, 34, 46, 83, 103, 108, 121, 147, 162\}$
14	$183 = 13^2 + 13 + 1$	$\{0, 1, 3, 16, 23, 28, 42, 76, 82, 86, 119, 137, 154, 175\}$

Por las construcciones de Singer, Bose & Chowla, sabemos que (ver [ACT]):

$$\begin{aligned} f_2\left(q^2 - 1\right) &= q, \\ f_2(q^2 + q + 1) &= q + 1, \end{aligned}$$

para toda potencia prima q.

6.2. Algunos valores iniciales de $f_3(N)$

Sea $f_3(N) = \max\{|A| : A \in B_3(\textit{mód } N)\}$. La Tabla 2 muestra los valores de $f_3(N)$ para los primeros pocos valores de N.

Tabla 2: Algunos valores iniciales de $f_3(N)$

N	$f_3(N)$	Conjunto ejemplo
4,12	2	$\{0, 1\}$
13	3	$\{0, 5, 11\}$
14,29	3	
30	4	$\{0, 17, 23, 25\}$
31	3	$\{0, 22, 23\}$
32	4	$\{0, 19, 20, 23\}$
33	3	$\{0, 21, 23\}$
34	4	$\{0, 21, 23, 28\}$
35,64	4	
65	5	$\{0, 5, 8, 22, 23\}$
66,68	4	
69	5	$\{1, 9, 22, 23, 60\}$
120	≥ 6	$\{1, 60, 89, 95, 106, 114\}$
130	≥ 6	$\{23, 60, 93, 96, 101, 110\}$
140	≥ 6	$\{1, 33, 60, 86, 96, 134\}$
156	≥ 6	$\{21, 60, 87, 96, 109, 134\}$

BIBLIOGRAFÍA

1. [ACT04] Astudillo Pilar, Collazos Idaly, Trujillo Carlos, *Conjuntos de Sidon sobre* $\mathbb{Z}_N$, Escuela Regional de Matemáticas, XI Encuentro, Universidad del Valle, Cali, 27 de junio al 1 de julio de 2005.

2. [BCh61] R. C. Bose and S. Chowla, *Theorems in the additive theory of numbers*, Comment. Math. Helv. **37** (1962/1963), 141-147.

3. [Ch94] Sheng Chen, *On the size of finite Sidon sequences*, Proceedings of the American Mathematical Society, **121** (1994), 353-356.

4. [ET41] P. Erdös and P. Turán, *On a problem of Sidon in additive number theory and some related problems*, J. Lond. Math. Soc. (1941), 212-215.

5. [HH06] Harri Haanpää, Página Web, http://www.tes.hut.fi/~haha/Zn/

6. [HR83] H. Halberstam and K. F. Roth, *"Sequences"*, Springer Verlag, New York, 1983.

7. [HTV07] Hernán Hidalgo, Carlos Trujillo, Omar Vallejo, *Conjuntos* B_h *sobre grupos conmutativos finitos*. Preprint.

8. [Ji93] Xing-De Jia, *On Finite Sidon Sequences*, Journal of Number Theory **44** (1993), 84-92.