Vol. XVI, Nº 2, Diciembre (2008)
Notas: 103–106

Matemáticas:
Enseñanza Universitaria

Transformada de Fourier sobre $\mathbb{Z}_N$ y conjuntos $B_2^-[g]$

Jhon Jairo Bravo G.
Universidad del Cauca

Recibido Nov. 19, 2007 Aceptado Abr. 1, 2008

Abstract

A set $\{a_1, a_2, \ldots, a_n, \ldots\}$ of positive integers is called a $B_2^-[g]-$set, if the number of representations of any x as $a_i - a_j$, $a_i \neq a_j$, is at most g. In this paper we use basic properties from Fourier analysis on $\mathbb{Z}_N$ and we follow the Ben Green style [1], to show with a different method, the best upper bound known so far for the maximum cardinal of a $B_2^-[g]-$set contained in $\{1, 2, \ldots, N\}$.

Keywords: $B_2^-[g]-$sets, Fourier transform on $\mathbb{Z}_N$.

MSC(2000): Primary: 11B50, Secondary: 11B75, 05B10.

Resumen

Un conjunto A de enteros positivos se llama un conjunto $B_2^-[g]$, si todo entero puede representarse como diferencia de dos elementos distintos de A, a lo sumo en g formas. En este artículo usamos propiedades básicas del análisis de Fourier sobre $\mathbb{Z}_N$ y seguimos el estilo de Ben Green [1] para mostrar con un método diferente, la mejor cota superior, conocida hasta el momento, para el máximo cardinal de un conjunto $B_2^-[g]$ contenido en $\{1, 2, \ldots, N\}$.

Palabras y frases claves: Conjuntos $B_2^-[g]$, transformada de Fourier sobre $\mathbb{Z}_N$.

1 Introducción

Un conjunto A de enteros positivos es un conjunto $B_2^-[g]$, o un conjunto en la clase $B_2^-[g]$, si para cada entero d, la ecuación $d = a_1 - a_2$, $a_1, a_2 \in A$, $a_1 \neq a_2$, tiene a lo sumo g soluciones.

Si A es un subconjunto finito de $\mathbb{N} = \{1, 2, \ldots\}$ y d es un entero, el número de soluciones de la ecuación $d = a_1 - a_2$, $a_1, a_2 \in A$, se denota por $\delta_A(d)$. De esta manera A es un conjunto $B_2^-[g]$ si para todo entero $d \neq 0$, $\delta_A(d) \leq g$.

El problema general a considerar en este trabajo es determinar el máximo cardinal de un conjunto, seleccionado de los primeros N enteros positivos, que esté en la clase $B_2^-[g]$. El camino natural a seguir es estudiar el comportamiento asintótico de la función

$$F_{2,g}^-(N) = \text{máx}\{|A| : A \subseteq \{1, 2, \ldots, N\}, A \in B_2^-[g]\}.$$

Respecto a esta función, Trujillo, García y Velásquez demuestran en [2] el siguiente teorema.

Teorema 1.1. *Sean $g \in \mathbb{N}$ y $A \subseteq \{1, 2, \ldots, N\}$, $A \in B_2^-[g]$. Entonces*

$$F_{2,g}^-(N) \leq (gN)^{1/2} + (gN)^{1/4} + 1. \tag{1}$$

La prueba, que se presenta en [2], del teorema anterior es un cálculo directo que se apoya en la desigualdad de *Cauchy–Schwarz* y en la definición de conjunto $B_2^-[g]$.

En la sección 2 de este artículo se presentan, sin demostración, algunos resultados básicos del análisis de Fourier sobre $\mathbb{Z}_N$. El lector interesado en ampliar los detalles puede consultar [3]. En la sección 3 se usa la convolución definida sobre $\mathbb{Z}$ para caracterizar los conjuntos $B_2^-[g]$. Finalmente se prueba en forma alternativa el Teorema 1.1. Para ello se siguen las ideas desarrolladas por Ben Green [1] en el caso $g = 1$.

2 Análisis de Fourier sobre $\mathbb{Z}_N$

Sea V el espacio vectorial de todas las funciones de valor complejo definidas sobre $\mathbb{Z}_N$. La *transformada de Fourier sobre* $\mathbb{Z}_N$, de una función $f \in V$, denotada por $\hat{f}$, se define por

$$\hat{f}(r) = \sum_{x \in \mathbb{Z}_N} f(x) w^{rx}, \quad \text{donde} \quad w = e^{2\pi i/N}.$$

Adicionalmente, si $f, g : G \to \mathbb{C}$ son funciones sobre un grupo abeliano G, la *convolución* de f y g, denotada $f * g$, se define por

$$(f * g)(x) = \sum_{y \in G} f(y)\overline{g(y-x)}, \tag{2}$$

donde $\overline{z}$ indica el complejo conjugado de z. Similarmente al caso real, en la transformada de Fourier sobre $\mathbb{Z}_N$ se resaltan las siguientes propiedades.

Propiedad 1. *Si $f, g \in V$, entonces se tiene*

(*a*) *Fórmula de Parseval*

$$\sum_{x \in \mathbb{Z}_N} f(x)\overline{g(x)} = \frac{1}{N} \sum_{r \in \mathbb{Z}_N} \hat{f}(r)\overline{\hat{g}(r)}.$$

(*b*)

$$\widehat{(f * g)}(r) = \hat{f}(r)\overline{\hat{g}(r)}.$$

Ejemplo 2.1. *Sean $A, B \subseteq \mathbb{Z}$. En lo que sigue del artículo siempre se identificará un conjunto con su función característica. Así, por ejemplo $A(x)$ está definida por*

$$A(x) = \begin{cases} 1 & si \quad x \in A, \\ 0 & si \quad x \notin A. \end{cases}$$

Ahora bien, teniendo en cuenta (2), se tiene que

$$(A * B)(x) = \sum_{y \in \mathbb{Z}} A(y)B(y-x).$$

Note que $(A*B)(x)$ cuenta el número de parejas $(a, b) \in A \times B$ tales que $x = a-b$. En particular, $(A * A)(x) = \delta_A(x)$. Claramente $(A * A)(0) = |A|$.

3 Otra prueba del teorema 1.1

Antes de presentar los resultados que conducen a (1), considere el siguiente ejemplo.

Ejemplo 3.1. *Sea $A = \{1, 3, 4, 5, 6, 7\}$. En la Tabla 1 se presentan las diferencias $(a - a', a \neq a')$ de los elementos del conjunto A.*

Tabla 1. Diferencias

-	1	3	4	5	6	7
1		2	3	4	5	6
3	-2		1	2	3	4
4	-3	-1		1	2	3
5	-4	-2	-1		1	2
6	-5	-3	-2	-1		1
7	-6	-4	-3	-2	-1	

Tabla 2. Versión modular

-	1	3	4	5	6	7
1		2	3	4	5	6
3	6		1	2	3	4
4	5	7		1	2	3
5	4	6	7		1	2
6	3	5	6	7		1
7	2	4	5	6	7	

Claramente $\delta_A(d) = \delta_A(-d)$. Como $A \in B_2^-[4]$, tenemos que $(A * A)(d) \leq 4$ para todo $d \neq 0$. Ahora considere la versión modular de $A * A$, para ello vea al conjunto A como subconjunto de $\mathbb{Z}_8$ en la forma natural. En este orden de ideas, la Tabla 1 se convierte en la Tabla 2. Note que en la nueva versión no es cierto que $(A * A)(d) \leq 4$, para todo $d \neq 0$. En general, Si $A \in B_2^-[g]$, entonces

$$(A * A)(d) \leq g, \quad \textit{para todo entero } d \neq 0, \tag{3}$$

pero en la versión modular de $A * A$, es decir, considerando al conjunto A como subconjunto de $\mathbb{Z}_N$ para algún entero positivo N, ya no es cierta la desigualdad (3) que, sin embargo, es válida para algunos valores apropiados del entero d, tal como se revela en la siguiente prueba.

Demostración del Teorema 1.1. Considere al conjunto A como subconjunto de $\mathbb{Z}_{N+u}$, donde $u < N$ es un entero positivo que se define mas adelante. Sea I la función característica del conjunto $\{1, 2, \ldots, u\}$ y defina a E por la siguiente expresión

$$E = \sum_{x \in \mathbb{Z}_{N+u}} (A * A)(x)(I * I)(x). \tag{4}$$

Se acota E superior e inferiormente. En primera instancia, en la versión modular de $A*A$ se tiene que $(A*A)(x) \leq g$ para $0 < |x| \leq u$, adicionalmente $(I*I)(x) = 0$ para $u + 1 \leq x \leq N - 1$. Con lo cual se obtiene

$$E \leq |A|u + g \sum_{0<|x|\leq u} (I * I)(x) = |A|u + 2g \sum_{0<x\leq u} (I * I)(x).$$

Ahora, por definición de convolución, $(I * I)(s) = u - s$, $s = 1, 2, \ldots, u$, en consecuencia

$$E \leq |A|u + gu(u - 1). \tag{5}$$

En segunda instancia, aplicando los resultados de la Propiedad 1, de (4) resulta

$$E = \frac{1}{N+u} \sum_{r \in \mathbb{Z}_{N+u}} |\hat{A}(r)|^2 |\hat{I}(r)|^2 \geq \frac{1}{N+u} |\hat{A}(0)|^2 |\hat{I}(0)|^2 = \frac{|A|^2 u^2}{N+u}.$$

Es decir

$$E \geq \frac{|A|^2 u^2}{N+u}. \tag{6}$$

Del acotamiento en (5) y (6) se sigue

$$\frac{|A|^2 u^2}{N+u} \leq |A|u + gu(u-1),$$

esto es

$$|A|^2 \leq \left(\frac{N+u}{u}\right) |A| + g \left(\frac{N+u}{u}\right) (u-1). \tag{7}$$

Sea $u = \left\lfloor \left(\frac{N^3}{g}\right)^{1/4} \right\rfloor + 1$, donde $\lfloor \cdot \rfloor$ es la función parte entera. Con lo anterior, de (7) se obtiene

$$|A|^2 \leq \big((gN)^{1/4} + 1\big)|A| + gN + (gN)^{3/4}.$$

Completando cuadrados en la última expresión se llega a que

$$\left(|A| - \frac{(gN)^{1/4}+1}{2}\right)^2 \leq \left(\frac{(gN)^{1/4}+1}{2} + (gN)^{1/2}\right)^2 - (gN)^{1/2}.$$

De donde $|A| \leq (gN)^{1/2} + (gN)^{1/4} + 1$. □

Agradecimientos El autor agradece al Dr. Carlos A. Trujillo S., profesor de la Universidad del Cauca, por la propuesta del tema y sus valiosas sugerencias en el desarrollo de este trabajo.

Referencias

[1] B. Green, The number of squares and $B_h[g]$ sets, Acta Arithmética, 100 (2001), No 4, 365–390.

[2] C. Trujillo, G. García and J. Velásquez, $B_2^{\pm}[g]$ Finite Sets, JP Journal of Algebra, Number Theory and Applications, 4(3) (2004), 593–604.

[3] A. Terras, Fourier Analysis on Finite Groups and Applications, Cambridge University Press, New York, 1999.

Dirección del autor

Jhon Jairo Bravo G. — Universidad del Cauca, Departamento de Matemáticas, Grupo de Investigación: Álgebra, Teoría de Números y Aplicaciones.

e-mail: jbravo@unicauca.edu.co