ENSAYO SOBRE CONJUNTOS CON ADICIÓN MULTIPLE EN $\mathbb{Z}_P$

JADER MELENDEZ BELEÑO

Monografía presentada como requisito para optar titulo de Matemático

UNIVERSIDAD DE CARTAGENA

FACULTAD DE CIENCIAS E INGENIERÍA

PROGRAMA DE MATEMÁTICA

CARTAGENA

2007

ENSAYO SOBRE CONJUNTOS CON ADICIÓN MULTIPLE EN $\mathbb{Z}_P$

JADER MELENDEZ BELEÑO

NESTOR RODRIGUEZ VEGA

Asesor

Monografía presentada como requisito para optar titulo de Matemático

UNIVERSIDAD DE CARTAGENA

FACULTAD DE CIENCIAS E INGENIERÍA

PROGRAMA DE MATEMÁTICA

CARTAGENA

2007

TABLA DE CONTENIDO

AGRADECIMIENTOS

A mi familia por haberme iniciado en este hermoso camino, en particular a mis hijos por no dejarme apartar de él.

A mi asesor Néstor Rodríguez Vega.

A mis grandes e incondicionales amigos Ana maria Torres y Adalberto Talaigua T.

A mis profesores, en especial a Pedro Ortega y Humberto Pérez.

A mis amigos y compañeros de la Universidad.

RESUMEN

Sea A un subconjunto no vacío de $\mathbb{Z}_p$ con p primo, para $h \geq 2$ en $\mathbb{Z}^+$. El conjunto de las h sumas de A está definida como

$$hA = \{a_1 + \cdots + a_n : a_1, \cdots, a_n \in A\}$$

G. Freiman mostró que si $|A| \leq p/35$, para algún primo p, y si $|2A| \leq 2{,}4\,|A| - 3$. Entonces A esta contenido en una progresión aritmética de $\mathbb{Z}_p$.

Este trabajo muestra la generalización de este hecho para el conjunto hA, siempre que A y hA cumplan una serie de condiciones que implican que el conjunto A está contenido en una tal progresión aritmética.

INTRODUCCIÓN

El Álgebra abstracta, es sin duda uno de los mayores aportes del mundo matemático, ya que el estudio de sus teorías ha enriquecido notablemente a otras ramas de las matemáticas como el análisis, cálculo, etc.

Este trabajo toca uno de los temas mas apasionantes de este género. Como son los conjuntos $\mathbb{Z}_p$. El cual es el conjunto de las clases de equivalencia de $\mathbb{Z}$ modulo p, que tiene su origen en la aplicación de los criterios de divisibilidad con una gran influencia del algoritmo de euclides.

La primera parte de este trabajo trata de conceptos básicos del álgebra abstracta en el sentido de $\mathbb{Z}$ y $\mathbb{Z}_p$ y a conjuntos que se forman bajo la operación de elementos de estos conjuntos.
En la segunda parte mostraremos que dado un subconjunto A, no vacío cualesquiera de $\mathbb{Z}_p$ y un subconjunto hA formado por la suma de los elementos del conjunto A y bajo ciertas condiciones este conjunto está contenido en alguna progresión aritmética. Refiriéndose a la generalización del teorema de FREIMAN realizado por le polaco Tomasz Schoen.

1. PRELIMINARES

El propósito de este capítulo es mostrar la notación y resultados básicos que se utilizan a lo largo de este trabajo.
Se presentan las demostraciones de algunos teoremas y conceptos más importantes.

1.1. Nociones de Álgebra abstracta y análisis

Definición 1.1.1 (Conjunto $\mathbb{Z}_p$). Sea $\mathbb{Z}$ el conjunto de los enteros, llamaremos $\mathbb{Z}_p$ al conjunto de las clases de equivalencia modulo p. Esto es

$$\mathbb{Z}_p = \{[0],\ [1], \cdots, [p-1]\}$$

donde

$$[0] = \{x \in \mathbb{Z} / x \equiv 0 \mod p\}$$
$$\vdots$$
$$[p-1] = \{x \in \mathbb{Z} / x \equiv (p-1) \mod p\}$$

Nótese que $x \equiv a \mod p$ si $a - x \in p\mathbb{Z}$ y esto equivale a que $a - x$ es múltiplo de p con

$$p\mathbb{Z} = \{pn / p \in \mathbb{Z}^+ \ fijo \ y \ n \in \mathbb{Z}\}$$

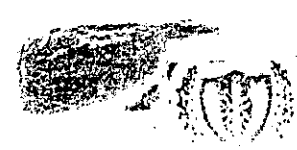
Definición 1.1.2 (Función Característica). Sea $A \subseteq \mathbb{Z}_n$, entonces

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

Definición 1.1.3 (Transformada discreta de Fourier). Sea $f : \mathbb{Z}_n \longrightarrow \mathbb{R}$ una función. Sea $w = e^{2\pi i/n}$; definimos la transformada discreta de fourier de f por

$$\widehat{f}(r) = \sum_{x \in \mathbb{Z}_n} f(x) w^{rx} \ \ para \ todo \ r \in \mathbb{Z}_n$$

Proposición 1.1.1 (Formulas de Fourier). *Sean $f,\ g : \mathbb{Z}_n \longrightarrow \mathbb{R}$. Tenemos que:*



i) $f(x) = n^{-1} \sum_r \widehat{f}(r) w^{-rx}$ *(Transformada Inversa)*

ii) $\sum_x f(x) \cdot g(x) = n^{-1} \sum_r \widehat{f}(r)\overline{\widehat{g}(r)}$ *(Identidad de Parseval)*

iii) Si $f * g(x) = \sum_y f(y)g(y-x)$ *entonces* $(\widehat{f * g})(r) = \widehat{f}(r)\overline{\widehat{g}(r)}$ *(convolución)*

En lo que sigue $|A|$ es precisamente el cardinal del conjunto A.

Definición 1.1.4. Un grupo G es abeliano si su operación binaria $*$ es conmutativa.

Definición 1.1.5. Un isomorfismo de un grupo G en si mismo es un automorfismo del grupo G.

Definición 1.1.6. Un subgrupo H de un grupo G es un subgrupo normal (o invariante) de G si $g^{-1}Hg = H$ para todas las $g \in G$. Esto es, si H permanece invariante bajo todo automorfismo interno de G.

Definición 1.1.7. Si N es un subgrupo normal de un grupo G, el grupo de las clases laterales de N bajo la operación inducida, es el grupo factor de G módulo N y se denota por G/N. las clases residuales de G módulo N son las clases laterales.

Ejemplo:

Las clases laterales a izquierda de $3\mathbb{Z}$ como subgrupo de $\mathbb{Z}$ bajo la suma son: el mismo $3\mathbb{Z} = 0 + 3\mathbb{Z}$, $1 + 3\mathbb{Z}$ formado por todos los enteros que dejan residuo 1 al dividirlos entre 3 y $2 + 3\mathbb{Z}$ formado por todos los enteros que dejan residuo 2 al dividirlos por 3.
Como $\mathbb{Z}$ es abeliano, $3\mathbb{Z}$ es un subgrupo normal y así $\mathbb{Z}/3\mathbb{Z}$ es el grupo factor de las tres clase residuales de $0 + 3\mathbb{Z}$, $1 + 3\mathbb{Z}$, $2 + 3\mathbb{Z}$. es un grupo de orden 3 isomórfico a $\mathbb{Z}_3$. Así el subgrupo $n\mathbb{Z}$ es normal en $\mathbb{Z}$ para todos los $n \in \mathbb{Z}^+$, con n clases residuales

$$0 + n\mathbb{Z},\ 1 + n\mathbb{Z}, \cdots,\ (n-1) + n\mathbb{Z}$$

el cual con la transformación $\phi_n : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}_n$ dada por $\phi_n(m + n\mathbb{Z}) = m$ para $0 \leq m < n$ es un isomorfismo.

Definición 1.1.8. Sea $(G, *)$ un grupo, N subgrupo normal de G y $G/N = \{xN/x \in G\}$. Entonces $f : G \longrightarrow G/N$ definida por $a \longrightarrow f(a) = aN$ es un homeomorfismo sobre f, se llama el homeomorfismo canónico.

Definición 1.1.9 (Conjunto Denso). Sea $(G, <)$ un grupo ordenado, y sean $x_1, x_2 \in G$. G es denso si existe y en G tal que $x_1 < y < x_2$.

2. CONJUNTOS SUMA Y TEOREMA DE FREIMAN

En lo que sigue estudiaremos el teorema de Freiman, sus condiciones y la demostración de un teorema que en cierta forma lo generaliza.

El teorema de Freiman nos habla de la estructura de conjuntos con conjunto suma pequeño. ¿Qué significa eso? Si A es un subconjunto (finito y no vacío) de un grupo abeliano G, definimos su conjunto suma como

$$A + A = \{a + a' : a, a' \in A\}$$

donde a y a' no son necesariamente distintos. ¿Cuántos elementos puede tener $A + A$? El número de sumas que se pueden formar (algunas, por supuesto, podrían dar el mismo resultado) es $\frac{|A|(|A|+1)}{2}$. Así lo muestra la siguiente figura, que es la tabla de sumar en A(digamos que $A = \{a_1, a_2, ..., a_n\}$ y por lo tanto $|A| = n$)

$+$	a_1	a_2	$\cdots$	a_n
a_1	•	•	•	•
a_2	o	•	•	•
$\cdots$	o	o	•	•
a_n	o	o	o	•

Pues $1 + 2 + \cdots n = \frac{n(n+1)}{2}$. Así $|A + A| = \frac{|A|(|A|+1)}{2}$, y la igualdad puede darse si, por ejemplo, $G = \mathbb{Z}$ y $A = \{1, 2, 2^2, 2^3, \cdots, 2^{n-1}\}$ (si alguna suma se repitiera tendríamos un número que se escribe de dos formas distintas en base 2 y eso es imposible).
Por otro lado, es claro que siempre tenemos la desigualdad $|A + A| \geq |A|$ y la igualdad también puede darse (por ejemplo si A es un subgrupo de G). Uno no tarda en darse cuenta de que es fácil encontrar conjuntos con conjunto suma grande, pero es mucho más difícil encontrar ejemplos en los que el conjunto suma sea pequeño. De hecho, si tomamos, por ejemplo, un conjunto A de n enteros al azar en el conjunto $\{1, 2, \cdots, x\}$ con $x \geq n^{4+\varepsilon}$ entonces la probabilidad de que no se repita ninguna suma (esto es, de que $|A + A| = \frac{|A|(|A|+1)}{2}$) tiende a 1 cuando $n \longrightarrow \infty$. Es decir, $|A+A|$ es grande y sólo en casos muy especiales es pequeño. ¿Podemos caracterizar estos pocos casos? ¿El hecho de que $|A+A|$ sea pequeño implica que A debe tener cierta

estructura? El resultado de Freiman nos dice exactamente eso. A partir de ahora nos centraremos exclusivamente en el caso $G = \mathbb{Z}$.

Lemma 1. *Sea $A \subseteq \mathbb{Z}$ de tamaño n, entonces $|A + A| \geq 2n-1$, con igualdad si y sólo si A es una progresión aritmética de longitud n.*

Demostración. Como $|A| = n$ podemos escribir $A = a_1, a_2, \cdots, a_n$ con $a_1 < a_2 < \cdots < a_n$. Es fácil escribir $2n-1$ elementos distintos de $A + A$.

$$a_1 + a_1 < a_1 + a_2 < \cdots < a_1 + a_n < a_2 + a_n < \cdots < a_n + a_n. \quad (1)$$

También podemos dar otras listas de $2n-1$ elementos distintos, como las $n-2$ siguientes. Para todo $2 \leq i \leq n-1$ tenemos

$$a_1 + a_1 < \cdots < a_1 + a_i < \cdots < a_i + a_i < \cdots < a_i + a_n < \cdots < a_n + a_n. \quad (2)$$

Luego ya hemos demostrado de $n-1$ formas que $|A + A| \leq 2n-1$. Ahora bien, si $|A + A| = 2n-1$ entonces todas las listas de $2n-1$ elementos tienen que coincidir. Eso quiere decir que para todo $2 \leq i \leq n-1$ se cumple, comparando (1) con (2), que

$$a_2 + a_i = a_1 + a_{i+1}$$

de donde $a_2 - a_1 = a_{i+1} - a_i \; \forall 2 \leq i \leq n-1$. Y decir que $a_2 - a_1 = a_3 - a_2 = a_4 - a_3 = \cdots = a_n - a_{n-1}$ es decir que A es una progresión aritmética de longitud n. Por otra parte, es trivial que para una progresión aritmética de longitud n se tiene la igualdad. ❋

Así que en los enteros, lo mínimo que vale $|A + A|$ es $2|A| - 1$ y los conjuntos que alcanzan la cota tienen mucha estructura (son progresiones aritméticas). No es difícil encontrar conjuntos un poco menos estructurados para los que $|A + A|$ siga siendo pequeño. Por ejemplo, si queremos que $|A+A| \leq 4|A|$, podemos tomar como A cualquier subconjunto de n elementos de una progresión aritmética de longitud $2n$. Este tipo de conjuntos son una parte significativa de una progresión aritmética. Pero si seguimos buscando podemos encontrar ejemplos de conjuntos con conjunto suma pequeño que no son de esta forma. Si tenemos $x_0, x_1, \cdots, x_d \in \mathbb{Z}$ y $m_1, \cdots, m_d \in \mathbb{Z}_{>0}$, podemos definir una progresión aritmética generalizada P de dimensión d como sigue

$$P = \{x_0 + \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_d x_d | 0 \leq \lambda_j \leq m_j - 1\}. \quad (3)$$

Definimos el volumen de P como $m_1 m_2 \cdots m_d$ y el tamaño como $|P|$. Decimos que la progresión es propia si y sólo si el volumen es igual al tamaño, es decir, si y sólo si todas las sumas del conjunto (3) son distintas. Podemos pensar en P como la imagen de una aplicación del *prisma* d $-$ *dimensional* a los enteros. Es decir, una progresión aritmética generalizada de dimensión 2.

Bien, pues para este tipo de conjuntos es fácil ver que se tiene $|P+P| \leq 2d|P|$ (geométricamente, el prisma $d-$ *dimensional* se ve repetido $2d$ veces para formar el prisma de $P+P$). Es decir, una progresión aritmética generalizada también tiene conjunto suma pequeño, al igual que las progresiones aritméticas y sus subconjuntos significativos. Pero una progresión aritmética es obviamente una progresión aritmética generalizada de dimensión 1. Por lo tanto, hasta ahora hemos probado que las progresiones aritméticas generalizadas y sus subconjuntos grandes tienen conjunto suma pequeño. El profundo resultado de Freiman nos dice que esos son todos los ejemplos posibles.

Definición 2.0.10. Sea k un entero positivo y A un subconjunto de un grupo abeliano G. Sea $\phi : A \longrightarrow H$ una función de A en un grupo abeliano H. Decimos que ϕ es un k- homomorfismo (según Freiman) si para $x_1, x_2, \cdots, x_{2k}$ elementos de A con

$$x_1 + \cdots + x_k = x_{k+1} + \cdots + x_{2k}$$

tenemos que:

$$\phi(x_1) + \cdots + \phi(x_k) = \phi(x_{k+1}) + \cdots + \phi(x_{2k})$$

Si ϕ tiene una inversa siendo esta un Freiman homomorfismo, entonces decimos que ϕ es un Freiman isomorfismo.

Usaremos la notación $A \cong_k B$ para indicar un k- isomorfismo de Freiman de A en B o más brevemente F_k- isomorfismos. En particular un F_k- isomorfismo preserva el tamaño de la h- suma.

En lo seguido daremos unas definiciones y teoremas buscando la relación entre $\mathbb{Z}$ y $\mathbb{Z}_p$ con p primo.

Proposición 2.0.2 (RUZSA). *Sea $A \subseteq \mathbb{Z}$ un conjunto de tamaño n con $|A+A| \leq Cn$. Sea $k \geq 2$ un entero y sea $m > C^{2k}n$. Entonces existe un conjunto $A' \subseteq A$ de tamaño al menos n/k que es k-isomorfo a un subconjunto de $\mathbb{Z}_m$.*

Demostración. Sea p un número primo muy grande (en el siguiente párrafo diremos cómo de grande), y consideremos la composición de funciones

$$\mathbb{Z} \xrightarrow{\psi} \mathbb{Z}_p \xrightarrow{\psi_2(q)} \mathbb{Z}_p \xrightarrow{\psi_3} \mathbb{Z} \xrightarrow{\psi_4} \mathbb{Z}_m$$

donde ψ_1 y ψ_4 son las reducciones módulo p y m respectivamente, $\psi_2(q)$ es la multiplicación por q y ψ_3 es la función que manda a un $x \in \mathbb{Z}_p$ al correspondiente residuo en el intervalo $\{0, 1, ..., p-1\}$.
ψ_1, ψ_2 y ψ_4 son trivialmente homomorfismos de Freiman de cualquier orden. ψ_3 es un homomorfismo de orden k cuando lo restringimos a cualquier intervalo de la forma $I_j = \left(\frac{j-1}{k}p, \frac{j}{k}p\right]$ porque si coges k representantes en $\{0, \cdots, p-1\}$ de elementos de un intervalo de esos y los sumas, siempre obtienes un número en el intervalo de $\mathbb{Z} : ((j-1)p, jp]$. Luego la igualdad de la suma en $\mathbb{Z}_p$ implica la igualdad de la suma cogiendo representantes. Elegimos p suficientemente grande para que $\psi_1|_A$ sea inyectiva. Escribimos $S_j = \{x \in A | \psi_2(\psi_1(x)) \in I_j\}$. Entonces, para todo q existe un $j = j(q)$ tal que $|S_j| \geq n/k$ porque en $\mathbb{Z}_p$ sólo hay k intervalos de la forma $\left(\frac{j-1}{k}p, \frac{j}{k}p\right]$.
Observemos entonces que para todo q la composición $\psi = \psi_1 \circ \psi_2(q) \circ \psi_3 \circ \psi_4$ es un k-homomorfismo cuando se restringe a $S_j(q)$. Para concluir la prueba, mostraremos que existe una elección de q para la que es invertible y su inversa es también un k-homomorfismo. Basta probar que hay una elección de q para la que

$$\psi(x_1) + \cdots + \psi(x_k) = \psi(x_{k+1}) + \cdots + \psi(x_{2k}) \quad *$$

implica

$$x_1 + \cdots + x_k = x_{k+1} + \cdots + x_{2k},$$

porque esto prueba por un lado que ψ es inyectiva y por tanto que existe la inversa y por otro la condición de k-homomorfismo para esa inversa. De la única forma que puede fallar la condición para un q dado, es si tenemos un número no nulo $s = x_1 + \cdots + x_k - x_{k+1} - \cdots - x_{2k}$ tal que $qs(\mod p) \equiv 0(\mod m)$
donde $(\mod p)$ quiere decir coger el menor residuo no negativo módulo p. Fijamos s y nos preguntamos para qué valores de q puede cumplirse $*$, lo que deseamos es que falle para algún q porque así se cumpliría la condición. Como q recorre Z_p^x , $qs(\mod p)$ cubre $[1, ..., p-1]$. El número de elementos divisibles por m en éste intervalo es a lo sumo $(p-1)/m$. Luego fijado s,

$*$ se cumple a lo sumo para $(p-1)/m$ valores de q. Ahora, cada s está en el conjunto $(kA - kA)/\{0\}$, y por la desigualdad de Plünnecke ese conjunto tiene cardinal menor que $C^{2k}n$. Es decir, $*$ se cumple a lo sumo para $C^{2k}n(p-1)/m < p-1$ valores de q. Así que por lo menos existe un valor de q para el que falla $*$ y por tanto se cumple la condición que pedíamos. Así, hemos probado que tomando ese valor de q y $A' = S_j(q)$, tenemos que$\psi = \psi_1 \circ \psi_2(q) \circ \psi_3 \circ \psi_4$ es un k-homomorfismo de Freiman de A' (que tiene cardinal $\geq n/k$) a un subconjunto de $\mathbb{Z}_m$. ⁂

Teorema 2.0.1 (Freiman). *Sea A un subconjunto de $\mathbb{Z}_p$ con p primo, tal que $|A| \leq p/35$. Si $|2A| \leq 2{,}4|A| - 3$, entonces A esta contenido en una progresión aritmética de $\mathbb{Z}_p$ con $|2A| - |A| + 1$ términos.*

Demostración. Ver [5] ⁂

El sentido de esta demostración es la siguiente:
Como A tiene una 2- suma que es pequeña, entonces la función característica de A tiene coeficientes de Fourier grande y diferente de cero, entonces A es denso en alguna progresión aritmética $P \subseteq \mathbb{Z}_p$ de longitud $\frac{(p-1)}{2}$. El conjunto $A' = A \cap P$ es isomórfico (en el sentido de Freiman) a un subconjunto de enteros, aplicando el teorema aditivo de Freiman a A' para enteros e inferir que A' esta contenida en una progresión aritmética de cardinalidad $|2A'| - |A'| + 1$.
Como último paso se muestra que $A' = A$, de lo contrario nos resultaría que $|2A| > 2{,}4|A| - 3$.

Definición 2.0.11. Sea A un subconjunto no vacío de un grupo aditivo y sea h un entero $h \geq 2$. El conjunto suma h de A que denotamos $h - sumA$ se define como

$$hA = \{a_1 + \cdots + a_n : a_1, \cdots, a_n \in A\}$$

Ejemplo:
Sea $p = 5$; $\mathbb{Z}_5 = \{[0],\ [1],\ [2],\ [3],\ [4]\}$
Sea $A \subseteq \mathbb{Z}_5$, $A = \{[0],\ [1],\ [2]\}$, sea $h = 2$, así la $2 - sumA$ es

$$\begin{aligned} 2A &= \{[0]+[1], [0]+[2], [1]+[2], [1]+[1], [0]+[0], [2]+[2]\} \\ &= \{[1],\ [2],\ [3],\ [2],\ [0],\ [4]\} \\ &= \{[0],\ [1],\ [2],\ [2],\ [3],\ [4]\} \subseteq \mathbb{Z}_5 \end{aligned}$$

Teorema 2.0.2. *Sea $h \geq 2$ y A un subconjunto finito de $\mathbb{Z}$, $|A| \geq 2$ tal que*

$$|hA| \leq \frac{(h+1)h}{2}|A| - h^2.$$

Entonces

$$L(A) \leq \max_{1 \leq j \leq h-1} \frac{|hA| - p_j(|A|)}{h-j} + 1$$

donde $p_j(n) = \frac{(j+1)j}{2}n - j^2 + 1$ y $L(A)$ denota la cardinalidad de la progresión aritmética mas pequeña que contiene a A.

Demostración. Ver [7] ❋

Teorema 2.0.3 (Cauchy - Davenport). *Sea p un número primo y sea A un subconjunto no vacío de $\mathbb{Z}_p$. Entonces para todo entero $h \geq 2$,*

$$|hA| \geq \min(p,\ h|A| - h + 1)$$

Demostración. Ver [7] ❋

Corolario 2.0.1. *Sea p un número primo y sea A un subconjunto no vacío de $\mathbb{Z}_p$ tal que $|hA| < p$. Entonces para los enteros h y h_1 tal que $h \geq h_1 \geq 2$,*

$$|h_1A| < [h/h_1]^{-1}|hA| + 1$$

Demostración. Por 2.0.3,

$$|hA| \geq |[h/h_1](h_1A)| \geq [h/h_1]|h_1A| - [h/h_1] + 1$$

ya que $h_1A \subseteq \mathbb{Z}_p$ y $|hA| < p$, así

$$\begin{aligned} |hA| &\geq [h/h_1]|h_1A| - [h/h_1] + 1 \\ |hA|[h/h_1]^{-1} &\geq |h_1A| + [h/h_1]^{-1} - 1 \\ |hA|[h/h_1]^{-1} + 1 &\geq |h_1A| + [h/h_1]^{-1} > |h_1A| \end{aligned}$$

Así

$$|hA|[h/h_1]^{-1} + 1 > |h_1A|$$

❋

2.1. GENERALIZACIÓN DEL TEOREMA DE FREIMAN

Ahora generalizaremos el teorema de Freiman para h sumandos con h grande. El teorema es el siguiente:

Teorema 2.1.1. *Sea H una constante positiva tal que para todo $h > H$, todo primo p y todo $A \subseteq \mathbb{Z}_p$ que satisface*

$$10 \leq |A| \leq \frac{P(\ln h)^{1/2}}{9h^{9/4}}$$

y

$$|hA| \leq \frac{h^{3/2}}{8(\ln h)^{1/2}}|A|$$

El conjunto A está contenido en una progresión aritmética de cardinalidad

$$\max_{1\leq j\leq h-1} \frac{|hA| - P_j(|A|)}{h-j} + 1$$

donde $P_j(n) = \frac{(j+1)j}{2}n - j^2 + 1$.

Demostración. Para un conjunto $S \subseteq \mathbb{Z}_p$ el conjunto $\{\widehat{S}(r)\}_{r\in\mathbb{Z}_p}$ denota los coeficientes de Fourier de la función indicadora de S. ($\widehat{S}(r) = \sum_{s\in S} e^{2\pi irs/p}$). Es claro que $|\widehat{S}(0)| = |S|$.

Aplicando la identidad de Parseval a la función indicadora de S tenemos:

$$\begin{aligned} P^{-1}\sum_{r=0}^{p-1}|\widehat{S}(r)|^2 &= P^{-1}\sum_{r=0}^{p-1}\widehat{S}(r)\cdot\widehat{S}(r) \\ &= P^{-1}\sum_{r=0}^{p-1}\Big(\Big(\sum_{x\in\mathbb{Z}_n}S(x)w^{rx}\Big)\Big(\sum_{x\in\mathbb{Z}_n}S(x)w^{-rx}\Big)\Big) \\ &= P^{-1}\sum_{r=0}^{p-1}\Big(\sum_{x\in\mathbb{Z}_n}S(x)w^{rx-rx}\Big) \\ &= P^{-1}\sum_{r=0}^{p-1}\Big(\sum_{x\in\mathbb{Z}_n}S(x)\Big) \\ &= P^{-1}\sum_{r=0}^{p-1}|S| = P^{-1}|S|P = |S| \end{aligned}$$

Así

$$P^{-1}\sum_{r=0}^{p-1}|\widehat{S}(r)|^2 = |S|$$

Luego

$$\sum_{r=0}^{p-1}|\widehat{S}(r)|^2 = P|S|.$$

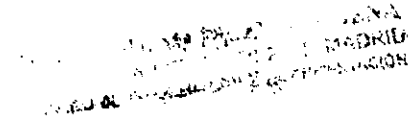
Por la definición todas las sumas $a_1+\cdots+a_n\in A$ están en el conjunto hA, entonces

$$\sum_{r=0}^{p-1}\widehat{A}(r)^h(\widehat{hA})(-r) = |A|^hP$$

y

$$\sum_{r=1}^{p-1}\widehat{A}(r)^h(\widehat{hA})(-r) = |A|^hP - |A|^h|hA| \geq |A|^hP/2$$

Sea $M = \max_{r\neq 0}|\widehat{A}(r)|$ y por la desigualdad de Cauchy- Schwartz y la identidad



de Parseval

$$|A|^h p/2 \leq \sum_{r=1}^{p-1} |\widehat{A}(r)|^h |(\widehat{hA})(-r)| \leq M^{h-1} \sum_{r=1}^{p-1} |\widehat{A}(r)||(\widehat{hA})(-r)|$$
$$\leq M^{h-1} \Big(\sum_{r=1}^{p-1} |\widehat{A}(r)|^2\Big)^{1/2} \Big(\sum_{r=1}^{p-1} |(\widehat{hA})(-r)|^2\Big)^{1/2}$$
$$< M^{h-1} |A|^{1/2} |hA|^{1/2} p$$

Así

$$M > \Big(\frac{|A|}{4|hA|}\Big)^{\frac{1}{2(h-1)}} |A| \geq (h^{-3/2})^{\frac{1}{2(h-1)}} |A| \ (porhipotesis)$$
$$= \exp\Big(-\frac{3}{4}\frac{\ln h}{h-1}\Big)|A|$$
$$> \Big(1 - \frac{3}{4}\frac{\ln h}{h-1}\Big)|A|$$
$$> \Big(1 - \frac{\ln h}{h}\Big)|A| \qquad (1)$$

Sea $r_0 \in \mathbb{Z}_p) \setminus \{0\}$ tal que $|\widehat{A}(r_0)| = M$. Tomemos $r = \arg \widehat{A}(r_0)$, $\alpha = \arccos(1 - \frac{2\ln h}{h})$, así que $\alpha \leq \pi\Big(\frac{\ln h}{2h}\Big)^{1/2}$. Definamos el conjunto B como

$$B = \{r_0 \alpha : a \in A \ y \ d(r - 2\pi\frac{(r_0 a)_p}{P}) \leq \alpha\}$$

donde $(r_0 a)_p$ esta dado como el menor entero no negativo que es congruente a $r_0 a$ modulo P y $d(x)$ denota la distancia de x al número más proximo de la forma $2\pi k$, $k \in \mathbb{Z}$, se sigue que

$$|\widehat{A}(r_0)| \leq |B| + (\cos\alpha)(|A| - |B|),$$

y por 1

$$|B| \geq \frac{1 - \frac{\ln h}{h} - \cos\alpha}{1 - \cos\alpha}|A| = |A|/2 \qquad (2)$$

Obsérvese que B es F_{h_0}- isomórfico a un subconjunto de enteros, donde $h_0 = [2\pi/\alpha]$. Entonces

$$h_0 \geq 2\Big(\frac{h}{\ln h}\Big)^{1/2}$$

y por 2.0.1, 1 y 2 obtenemos

$$\begin{aligned}|h_0B| &\leq \frac{|hB|}{[h/h_0]} + 1 \leq \frac{2h_0|hA|}{h} + 1 \\ &\leq \frac{2|hB|}{h_0[h/h_0]} + 1 \leq \frac{h_0 h^{1/2}|B|}{2(\ln h)^{1/2}} + 1 \\ &\leq \frac{h_0^2}{4}|B| + 1 < \frac{(h_0+1)h_0|B|}{2} - h_0^2 + 1\end{aligned}$$

Así podemos aplicar el teorema 2.0.2 al conjunto B, así que B está contenido en una progresión aritmética en $\mathbb{Z}_p$ de tamaño

$$\begin{aligned}\max_{1\leq j\leq h_0-1} \frac{|h_0B| - P_j(|B|)}{h_0 - j} + 1 &\leq \frac{2|h_0B|}{h_0} + 1 \\ &\leq \frac{2|hB|}{h_0[h/h_0]} + 2 \\ &\leq \frac{4|hA|}{h} + 2 \\ &\leq \frac{h^{1/2}|A|}{2(\ln h)^{1/2}} + 2 \\ &\leq \frac{P}{2h^{7/4}} \qquad (3)\end{aligned}$$

Sea A_1 un subconjunto de A con cardinalidad máxima, contenida en una progresión aritmética de cardinalidad $[p/h]$. De 2 y 3 se sigue que $|A_1| \geq |A|/2$. Un argumento análogo al usado en 3 muestra que A_1 esta contenido en una progresión aritmética de tamaño a lo mas $p/(2h^{7/4})$, además sin perdida de generalidad podemos asumir que A_1 es un subconjunto de la progresión aritmética con la diferencia común 1 y centrada en 0 que significa $\|a\| \leq p/(4h^{7/4})$ para todo $a \in A_1$, donde $\|x\| = \min((x)_p,\ (p-x)_p)$. Si $a_o \in A \setminus A_1$, entonces

$$\|ka_o\| \leq \frac{p}{2h}$$

para algún $k \in \mathbb{N}$. Sea k el menor número con esta propiedad. obsérvese que si $k \leq h^{3/4}$, entonces para todo $a \in A_1$

$$\|ka\| \leq k\|a\| \leq h^{3/4}\frac{p}{4h^{7/4}} < \frac{p}{2h}$$

Así el conjunto $A_1 \cup \{a_o\}$ está contenido en una progresión aritmética de tamaño a lo más p/h y diferencia común k^{-1} (el inverso multiplicativo de k

en $\mathbb{Z}_p$) contradiciendo la maximalidad de A_1. Podemos asumir que $k \geq h^{3/4}$. Sea $\rho = [h^{3/4}]$, entonces los elementos $a_o,\ 2a_o, \cdots, \rho a_o$ están bien espaciados:

$$\|ia_o - ja_o\| = \|(i-j)a_o\| \geq \frac{p}{2h}$$

para todo $i \neq j,\ i,\ j \in \{1, \cdots, \rho\}$.
Consecuentemente, los conjuntos

$$\rho A_1,\ a_o + (\rho-1)A_1, \cdots, (\rho-1)a_o + A_1 \tag{4}$$

son disjuntos dos a dos. En efecto, si $(ia_o+(\rho-i)A_1)\cap(ja_o+(\rho-j)A_1) \neq \phi$ para algún $i \neq j,\ i,\ j \in \{0, \cdots, \rho-1\}$, hay elementos $a_1, \cdots, a_{\rho-j},\ b_1, \cdots, b_{\rho-j} \in A_1$ tales que

$$ia_o + a_1 + \cdots + a_{\rho-i} = ja_o + b_1 + \cdots + b_{\rho-j},$$

de manera que deseamos tener

$$\begin{aligned}\|ja_o - ia_o\| &= \|a_1 + \cdots + a_{\rho-i} - b_1 - \cdots - b_{\rho-j}\| \\ &\leq \|a_1\| + \cdots + \|a_{\rho-i}\| + \|b_1\| + \cdots + \|b_{\rho-j}\| \leq \frac{p}{2h}\end{aligned}$$

Ahora por 4 y 2.0.3

$$\begin{aligned}|hA| &\geq |\rho A_1| + |a_o + (\rho-1)A_1| + \cdots + |(\rho-1)a_o + A_1| \\ &\geq (\rho|A_1| - \rho + 1) + ((\rho-1)|A_1| - \rho + 2) + \cdots + |A_1| \\ &> \rho^2|A|/4 - \rho^2/2 > |hA|\end{aligned}$$

Una contradicción. Entonces A está contenida en una progresión aritmética de cardinalidad $[p/h]$ en $\mathbb{Z}_p$ y es F_n-isomórfica a un subconjunto de enteros. Aplicando 2.0.2 podemos inferir que A está contenida en una progresión aritmética de tamaño

$$\max_{1 \leq j \leq h-1} \frac{|hA| - P_j(|A|)}{h-j} + 1.$$

*

Bibliografía

[1] Y. BILU, V. F. LEV and I. Z. RUZSA *Rectification principles in additive number theory*, Discrete computational geometry 19 343 - 353 (1998).

[2] J. F. CAICEDO *Teoría de Grupos.*

[3] E. CROOT, I. RUZSA, T. SCHOEN *Arithmetic Progressions in sparse sumsets*, (2005).

[4] J. B. FRALEIGH, *Algebra Abstracta.*

[5] G. FREIMAN *Foundations of a structural theory of set addition*, Translations of Math, Monographs 37 American Math. Soc, providence (1973).

[6] B. F. GREEN *Structure theory of set addition*,

[7] V. F. LEV,*Structure theorem for multiple addition and the Frobenius problem* Journal of Number theory 58 79-82 (1996).