

## Conjuntos suma pequeños en $p$ -grupos finitos

WILSON FERNANDO MUTIS<sup>a,\*</sup>, FERNANDO ANDRÉS BENAVIDES<sup>a</sup>,  
JOHN HERMES CASTILLO<sup>a</sup>

<sup>a</sup> Universidad de Nariño, Departamento de Matemáticas y Estadística, A.A. 1175-1176,  
San Juan de Pasto, Nariño, Colombia.

**Resumen.** En este artículo presentamos una fórmula explícita para la función  $\mu_G(r, s) = \min |A \cdot B|$ , donde  $A$  y  $B$  son subconjuntos de un  $p$ -grupo finito  $G$  con  $|A| = r$ ,  $|B| = s$  y  $1 \leq r, s \leq |G|$ .

**Palabras claves:** Conjunto suma,  $p$ -grupo, teoría aditiva de números.

**MSC2000:** 11B34, 20D60.

### *Small Sumsets in Finite $p$ -groups*

**Abstract.** In this paper we present an explicit formula for the function  $\mu_G(r, s) = \min |A \cdot B|$ , where  $A$  and  $B$  are subsets of a finite  $p$ -group  $G$  with  $|A| = r$ ,  $|B| = s$  and  $1 \leq r, s \leq |G|$ .

**Keywords:** Sumset,  $p$ -group, additive number theory.

### 1. Introducción

Sea  $(G, \cdot)$  un grupo finito. El conjunto suma (o conjunto producto) de dos subconjuntos no vacíos  $A$  y  $B$  de  $G$ , denotado con  $A \cdot B$ , esta dado por

$$A \cdot B = \{a \cdot b : a \in A \text{ y } b \in B\}.$$

Un problema de interés en Teoría Aditiva de Números, denominado el problema de los conjuntos suma pequeños, es determinar una fórmula explícita que permita calcular el mínimo de los cardinales  $|A \cdot B|$ , donde  $A$  y  $B$  son subconjuntos de grupo  $G$  tales que  $|A| = r$  y  $|B| = s$ , es decir, se desea hallar una fórmula que permita calcular los valores de la función

$$\mu_G : [1, |G|] \times [1, |G|] \mapsto \mathbb{N}$$

definida por

$$\mu_G(r, s) = \min \{|A \cdot B| : A, B \subseteq G, |A| = r \text{ y } |B| = s\}.$$

---

\* Autor para correspondencia: E-mail: wfmutis@gmail.com.

Recibido: 12 de mayo de 2010, Aceptado: 17 de noviembre de 2010.

Este problema en general no es fácil, pero Eliahou y Kervaire en [4] probaron que si  $G$  es un grupo abeliano finito, se satisface la igualdad

$$\mu_G(r, s) = \kappa_G(r, s) = \min_{h \in \mathcal{H}(G)} \left\{ \left( \left\lceil \frac{r}{h} \right\rceil + \left\lceil \frac{s}{h} \right\rceil - 1 \right) h \right\}, \quad (1)$$

donde  $\mathcal{H}(G)$  denota en conjunto de órdenes de subgrupos de  $G$ . En el caso de que  $G$  es un grupo finito no abeliano, se desconoce una fórmula explícita para  $\mu_G(r, s)$ , pero existen grupos no abelianos para los cuales la igualdad (1) se cumple. Por ejemplo, Kemperman en [6] demuestra que  $\mu_G(r, s) = \kappa_G(r, s)$  cuando  $G$  es un grupo libre de torsion; Eliahou y Kervaire en [5] probaron que esta ecuación también se tiene para grupos diédricos de orden  $2p^n$  con  $p$  primo, y Benavides, Castillo y Mutis en [1] obtienen la misma expresión para grupos hamiltonianos de la forma  $\mathcal{Q} \times (\mathbb{Z}/2\mathbb{Z})^k \times G$ , donde  $G$  es cíclico de orden impar. Sin embargo, la igualdad (1) no se puede generalizar para todo grupo finito no abeliano, pues en el producto semidirecto  $G = C_{13} \times C_3$ , donde  $C_i$  denota el grupo cíclico de orden  $i$ , se tiene la desigualdad  $\kappa_G(6, 6) < \mu_G(6, 6)$  (ver [2]).

El objetivo de este artículo es ampliar la clase de grupos finitos no abelianos para los cuales se cumple  $\mu_G(r, s) = \kappa_G(r, s)$ . En particular, se demuestra que esta igualdad se satisface en todo  $p$ -grupo finito.

## 2. La función $\mu_G$ en $p$ -grupos finitos

En esta sección se demuestra que la fórmula obtenida para la función  $\mu_G$ , cuando  $G$  es un grupo abeliano finito, también se cumple para el caso en que  $G$  es un  $p$ -grupo finito. En verdad, se demuestra el siguiente teorema:

**Teorema 2.1.** *Sea  $p$  un número primo y sea  $G$  un  $p$ -grupo finito. Si  $r, s$  son dos enteros tales que  $1 \leq r, s \leq |G|$ , entonces  $\mu_G(r, s) = \kappa_G(r, s)$ .*

*Demostración.* Dado que  $G$  es un  $p$ -grupo finito, existe un entero positivo  $n$  tal que  $|G| = p^n$ . Así, el conjunto  $\mathcal{H}(G)$  de órdenes de subgrupos normales de  $G$  está dado por  $\mathcal{H}(G) = \{1, p, p^2, \dots, p^n\}$ . Sea  $p^x \in \mathcal{H}(G)$  tal que

$$\kappa_G(r, s) = \left( \left\lceil \frac{r}{p^x} \right\rceil + \left\lceil \frac{s}{p^x} \right\rceil - 1 \right) p^x.$$

Como todo  $p$ -grupo finito es soluble, entonces por Lema 2,2 de [5] se tiene

$$\mu_G(r, s) \leq \left( \left\lceil \frac{r}{p^x} \right\rceil + \left\lceil \frac{s}{p^x} \right\rceil - 1 \right) p^x = \kappa_G(r, s).$$

La desigualdad  $\mu_G(r, s) \geq \kappa_G(r, s)$  se probará por inducción sobre el orden del  $p$ -grupo  $G$ . Para  $n = 1$  se tiene  $|G| = p$ , luego  $G \cong \mathbb{Z}_p$ , donde  $\mathbb{Z}_p$  denota el grupo de congruencias módulo  $p$ ; así  $G$  es cíclico, y por lo tanto  $\mu_G(r, s) = \kappa_G(r, s)$ .

Supóngase que el teorema es válido para  $p$ -grupos de orden  $p^n$ , con  $n > 1$ . Sean  $G$  un  $p$ - grupo de orden  $p^{n+1}$  y  $T$  un subgrupo normal de  $G$  de orden  $p^n$ . Entonces  $T$  es de índice  $p$  y existe  $c \in G \setminus T$  tal que  $G$  se puede expresar como la unión de  $p$  clases laterales derechas disjuntas, así:

$$G = T \cup Tc \cup Tc^2 \cup \dots \cup Tc^{p-1}. \tag{2}$$

Sean  $r, s$  enteros positivos con  $r, s \leq p^{n+1}$ , y sean  $A, B$  dos subconjuntos de  $G$  tales que  $A$  y  $B$  realizan  $\mu_G(r, s)$ . Por la igualdad (2),  $T$  contiene subconjuntos  $A_0, A_1, \dots, A_{p-1}$  de cardinales  $r_0, r_1, \dots, r_{p-1}$ , respectivamente, y subconjuntos  $B_0, B_1, \dots, B_{p-1}$  de cardinales  $s_0, s_1, \dots, s_{p-1}$ , respectivamente, tales que

$$A = A_0 \cup A_1c \cup A_2c^2 \cup \dots \cup A_{p-1}c^{p-1} = \bigcup_{i=0}^{p-1} A_i c^i, \tag{3}$$

$$B = B_0 \cup B_1c \cup B_2c^2 \cup \dots \cup B_{p-1}c^{p-1} = \bigcup_{j=0}^{p-1} B_j c^j. \tag{4}$$

Para cada  $0 \leq l \leq p - 1$ , definamos

$$F_l = \{(i, j) : 0 \leq i, j \leq p - 1 \text{ y } i + j \cong l \text{ mód } p\}$$

y

$$H_l = \bigcup_{(i,j) \in F_l} (A_i c^i)(B_j c^j).$$

Entonces,

$$|AB| = \left| \left( \bigcup_{i=0}^{p-1} A_i c^i \right) \left( \bigcup_{j=0}^{p-1} B_j c^j \right) \right| = \bigcup_{l=0}^{p-1} |H_l|,$$

y dado que  $\mu_G(r, s) = |AB|$ , se tiene

$$\begin{aligned} \mu_G(r, s) &\geq \sum_{l=0}^{p-1} (\text{máx } \{|A_i B_j| : (i, j) \in F_l\}) \\ &\geq \sum_{l=0}^{p-1} (\text{máx } \{\mu_T(r_i, s_j) : (i, j) \in F_l\}). \end{aligned}$$

La hipótesis inductiva aplicada al  $p$ -grupo  $T$  implica que

$$\mu_G(r, s) \geq \sum_{l=0}^{p-1} (\text{máx } \{\kappa_T(r_i, s_j) : (i, j) \in F_l\}). \tag{5}$$

Ahora bien, el conjunto  $\mathbb{N}_0$  de los enteros no negativos tiene estructura de espacio vectorial sobre el campo finito  $\mathbb{F}_p$ , donde la suma de vectores es la suma  $p$ -ádica. Sean  $\mathcal{V}$  el subespacio de  $\mathbb{N}_0$  generado por el conjunto  $\{1, p, p^2, \dots, p^{n-1}\}$ , es decir,  $\mathcal{V} = \{0, 1, 2, \dots, p^n - 1\}$ , e  $I_t$  el segmento inicial de longitud  $t$  de  $\mathcal{V}$ . Por el Teorema 2.1 y la Proposición 3.1 de [3] se sigue que

$$\mu_{\mathcal{V}}(u, v) = |I_u \oplus_p I_v| \text{ siempre que } 1 \leq u, v \leq |\mathcal{V}|.$$

Además de la definición de segmento inicial y de la Proposición 3.1 de [3], se obtiene

$$\begin{cases} I_u \oplus_p I_v = I_{\mu_{\mathcal{V}}(u,v)} & \text{siempre que } 1 \leq u, v \leq |\mathcal{V}|, \\ I_u \cup I_v = I_{\max\{u,v\}} & \text{para todo par de enteros no negativos } u \text{ y } v. \end{cases} \quad (6)$$

Sea  $M$  el grupo abeliano de orden  $p^{n+1}$  definido por  $M = \mathcal{V} \times \mathbb{Z}_p$ . Entonces el conjunto  $\mathcal{H}(M)$  de los órdenes de subgrupos de  $M$  coincide con el conjunto  $\mathcal{H}(G)$  de los órdenes de subgrupos de  $G$ , así que

$$\mu_M(r, s) = \kappa_M(r, s) = \kappa_G(r, s). \quad (7)$$

Ahora bien, viendo al grupo  $\mathcal{V}$  como un subgrupo de  $M$  y tomando  $b = (0, 1) \in M$ , se sigue que

$$M = \mathcal{V} \cup (\mathcal{V} + b) \cup \dots \cup (\mathcal{V} + (p - 1)b).$$

Para  $0 \leq i, j \leq p - 1$ , sean  $I_{r_i}$  e  $I_{s_j}$  los segmentos iniciales de  $\mathcal{V}$  de longitudes  $r_i$  y  $s_j$ , respectivamente, y considérense los conjuntos

$$E = I_{r_0} \cup (I_{r_1} + b) \cup (I_{r_2} + 2b) \cup \dots \cup (I_{r_{p-1}} + (p - 1)b) = \bigcup_{i=0}^{p-1} (I_{r_i} + ib),$$

$$D = I_{s_0} \cup (I_{s_1} + b) \cup (I_{s_2} + 2b) \cup \dots \cup (I_{s_{p-1}} + (p - 1)b) = \bigcup_{j=0}^{p-1} (I_{s_j} + jb);$$

entonces  $|E| = r$  y  $|D| = s$ . Para  $0 \leq l \leq p - 1$ , sea

$$W_l = \bigcup_{(i,j) \in F_l} (I_{r_i} \oplus_p I_{s_j}).$$

Realizando algunos cálculos, se puede observar que

$$E + D = W_0 \cup (W_1 + b) \cup (W_2 + 2b) \cup \dots \cup (W_{p-1} + (p - 1)b).$$

Aplicando la igualdad (7) se sigue que

$$\sum_{l=0}^{p-1} |W_l| = |E + D| \geq \mu_M(r, s) = \kappa_M(r, s) = \kappa_G(r, s). \quad (8)$$

Utilizando las igualdades (6) se tiene

$$\sum_{l=0}^{p-1} |W_l| = \sum_{l=0}^{p-1} \left| \bigcup_{(i,j) \in F_l} I_{\mu_{\mathcal{V}}(r_i, s_j)} \right| = \sum_{l=0}^{p-1} (\max \{ \mu_{\mathcal{V}}(r_i, s_j) : (i, j) \in F_l \}),$$

pero  $\mathcal{V}$  es un grupo abeliano; entonces,

$$\sum_{l=0}^{p-1} |W_l| = \sum_{l=0}^{p-1} (\max \{ \kappa_{\mathcal{V}}(r_i, s_j) : (i, j) \in F_l \});$$

además,  $\mathcal{V}$  y  $T$  son  $p$ -grupos del mismo orden, así que  $\kappa_{\mathcal{V}}(r_i, s_j) = \kappa_T(r_i, s_j)$  para toda  $(i, j) \in F_l$  y toda  $0 \leq l \leq p-1$ ; entonces,

$$\sum_{l=0}^{p-1} |W_l| = \sum_{l=0}^{p-1} (\max \{ \kappa_T(r_i, s_j) : (i, j) \in F_l \}). \quad (9)$$

De la igualdad (9) y las desigualdades (5) y (8) se concluye finalmente que

$$\mu_G(r, s) \geq \sum_{l=0}^{p-1} |W_l| \geq \kappa_G(r, s). \quad \square$$

### 3. Agradecimientos

Este artículo es fruto de un trabajo de investigación que los autores realizaron gracias a la financiación de la Vicerrectoría de Investigaciones, Posgrados y Relaciones Internacionales de la Universidad de Nariño.

### Referencias

- [1] Benavides F., Castillo J., y Mutis W., Conjuntos suma pequeños en grupos hamiltonianos, Preprint, 2009.
- [2] Eliahou S., and Kervaire M., Bounds on the minimal sumsets size function in groups, *J. Number Theory*, 4 (2007), 503–511.
- [3] Eliahou S., and Kervaire M., Sumsets in vector spaces over finite fields, *J. Number Theory*, 71 (1998), 12–39. MR1631038 (99d:11020)
- [4] Eliahou S., and Kervaire M., Minimal sumsets in infinite abelian groups, *J. Algebra*, 287 (2005), 449–457. MR2134154 (2006c:11018)
- [5] Eliahou S., and Kervaire M., Sumsets in dihedral groups, *European J. Combin.*, 27 (2006), 617–628. MR2215221 (2007a:11027)
- [6] Kemperman J.H.B., On complexes in a semigroup, *Nederl. Akad. Wetensch. Proc. Ser. A*. 59 = *Indag. Math.*, 18 (1956), 247–254. MR0079005 (18,14a)