Universidad Autónoma Metropolitana

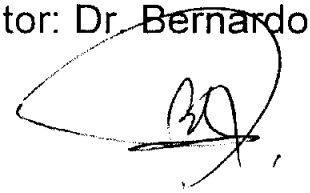
Ciencias Básicas e Ingeniería

El caso de igualdad en el problema de Erdös-Heilbronn

Presenta: Gabriel Bengochea Villegas

Para obtener el grado de Maestro
en Ciencias (Matemáticas)

Tutor: Dr. Bernardo Llano Pérez



Noviembre de 2005

Universidad Autónoma Metropolitana
Ciencias Básicas e Ingeniería

El caso de igualdad en el problema de Erdös-Heilbronn

Presenta: Gabriel Bengochea Villegas

Para obtener el grado de Maestro
en Ciencias (Matemáticas)

Tutor: Dr. Bernardo Llano Pérez

Noviembre de 2005

Índice

1 Introducción

La teoría aditiva de los números se divide en dos tipos de problemas: problemas directos e inversos. Los problemas directos son aquellos en los cuales se determina la estructura y propiedades de una suma de conjuntos de un grupo, conociendo a los sumandos. Los problemas inversos son aquellos en los que se determinan las propiedades de los sumandos a partir de conocer la propiedades del conjunto suma.

Para lo que sigue, sea el grupo de residuos $\mathbb{Z}_n$ módulo un número entero n. Denotaremos por $\mathbb{Z}_p$ al grupo cuando $n = p$ es un número primo. Además definimos

$$\begin{aligned} A + B &= \{a + b : a \in A, b \in B\}, \\ A \,\widehat{+}\, B &= \{a + b : a \in A, b \in B, a \neq b\}, \\ 2A &= A + A \\ 2\widehat{\ }A &= A \,\widehat{+}\, A. \end{aligned}$$

El primer teorema conocido es el de Cauchy [9], el cual lo aplicó para demostrar que todo residuo módulo p se puede representar como la suma de dos residuos cuadráticos, esto es, $x^2 + y^2 \equiv r \bmod p$ $(*)$ tiene solución para todo $r \in \mathbb{Z}_p$.

Teorema 1 *(Cauchy-Davenport). Sea $\varnothing \neq A, B \subseteq \mathbb{Z}_p$. Entonces se cumple que*

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

Observe que si definimos a A como el conjunto de los residuos cuadráticos módulo p (incluyendo al 0), entonces $|A| = \frac{p+1}{2}$. Si aplicamos el teorema

anterior, obtenemos que

$$|2A| = |A + A| \geq 2\,|A| - 1 = p.$$

Así $2A = \mathbb{Z}_p$ y la ecuación $(*)$ siempre tiene solución.

Este teorema fue demostrado por Cauchy en 1813 y después, independientemente, por Davenport en 1935 [3]. El propio Davenport encontró que su teorema ya había sido demostrado anteriormente.

El siguiente teorema, el cual es la solución a un problema inverso, da una caracterización de los conjuntos para los cuales se cumple la igualdad en el teorema de Cauchy-Davenport. Este teorema se publicó en 1956 por A. G. Vosper [2].

Teorema 2 *(Vosper). Sean $\varnothing \neq A, B \subseteq \mathbb{Z}_p$. Entonces se cumple que*

$$|A + B| = \min\{p, |A| + |B| - 1\}$$

si y sólo si A y B satisfacen una de las siguientes condiciones:

(i) $|A| + |B| > p$,

(ii) $\min\{|A|, |B|\} = 1$,

(iii) $\overline{B} = \mathbb{Z}_p \setminus B = c - A = \{c - a \mid a \in A\}$ *para alguna* $c \in \mathbb{Z}_p$,

(iv) A y B son progresiones aritméticas con la misma diferencia común.

Este teorema se utilizó para demostrar un resultado en teoría de números por Chowla, Mann y Straus en 1959 [10], el cual se enuncia a continuación. Al polinomio utilizado en el siguiente teorema se le llama forma diagonal.

Teorema 3 *Sea $p > 3$ un número primo, y sea k un entero positivo tal que*

$$1 < mcd(k, p-1) < \frac{p-1}{2}.$$

Sean $c_1, ..., c_n$ números distintos de cero que pertenecen al campo $\mathbb{Z}_p$, y

$$f(x_1, ..., x_n) = c_1 x_1^k + \cdots + c_n x_n^k$$

Sea $R(f)$ el rango de la forma diagonal f. Entonces

$$|R(f)| \geq \min\left\{p, \frac{(2n-1)\,(p-1)}{(k, p-1)} + 1\right\}$$

donde $R(f) = \{f(x_1, x_2, ..., x_n) : x_1, x_2, ..., x_n \in \mathbb{Z}_p\}$.

Esta teoría no sólo muestra un desarrollo para $\mathbb{Z}_p$, también existen teoremas muy importantes para $\mathbb{Z}$. El siguiente resultado fue demostrado y publicado por Freiman en el año de 1959 [8].

Teorema 4 *(Freiman) Sea A un subconjunto de enteros tal que $|A| = k \geq 3$. Si*

$$|2A| = 2k - 1 + b \leq 3k - 4,$$

entonces A está contenida en una progresión aritmética de longitud $k + b \leq 2k - 3$.

En 1993 Steining [11] da una generalización del teorema de Freiman, que consiste en el caso más general de $A + B$.

Freiman, que desarrolló mucho esta área, encontró una generalización al teorema inverso de Vosper.

Teorema 5 *(Freiman-Vosper). Sean C_0 y C_1 números reales tales que*

$$0 < C_0 \leq \frac{1}{12},$$

$$C_1 > 2,$$

$$\frac{2C_1 - 3}{3} < \frac{1 - C_0 C_1}{\sqrt[2]{C_1}}.$$

Sean p un número primo impar, $A \neq \varnothing$ y $A \subseteq \mathbb{Z}_p$ tales que

$$3 \leq k = |A| \leq C_0 p$$

y

$$|2A| \leq C_1 k - 3.$$

Defininimos el entero b como $|2A| = 2k - 1 + b$. Entonces A está contenido en una progresión aritmética de longitud $k + b$ en $\mathbb{Z}_p$.

La demostración usa dos métodos fundamentales en esta área. El primero se basa en la estimación de sumas exponenciales. El segundo usa argumentos aritméticos para reemplazar el conjunto A por un conjunto T de enteros tal que $2A$ y $2T$ estén en correspondencia biyectiva.

El siguiente resultado, obtenido por Chowla en 1935 [12], es una extensión del teorema de Cauchy-Davenport, el cual se cumple para cualquier clase de congruencias módulo un entero arbitrario $m \geq 2$.

Teorema 6 *(Chowla) Sean $m \geq 2$ y sean A y B dos subconjuntos de $\mathbb{Z}_m$. Si $0 \in B$ y $mcd(b, m) = 1$ para toda $b \in B \setminus \{0\}$, entonces*

$$|A + B| \geq \min\{m, |A| + |B| - 1\}.$$

B. Llano, en el 2003 [6], caracteriza los subconjuntos de $\mathbb{Z}_p$ para los cuales se cumple que

$$|A + B| = |A| + |B| + i, \ \ (i = 0, 1).$$

Varios de los resultados y generalizaciones demostrados en este artículo fueron publicados, en ese tiempo, también por Hamidoune-Rödseth [13] y Serra-Zémor [14]. Este resultado se separa en dos teoremas. Definimos

$$\begin{aligned} T_a[k, l] &= \{a + id \mid i \in [0] \cup [k, l], 2 \leq k \leq l - 1\}, \\ U_a(1, 2; m) &= \{a + id \mid i \in [0] \cup [2] \cup [a, m], m \geq 5\}, \\ U_a(1, 3; m) &= \{a + id \mid i \in [0] \cup [2, m] \cup [m + 2], m \geq 3\}, \\ U_a(2, 3; m) &= \{a + id \mid i \in [0, m] \cup [m + 2] \cup [m + 4], m \geq 1\} \end{aligned}$$

donde $[r]$ es el intervalo que sólo contiene al elemento r y d es un elemento fijo, llamado diferencia, de $\mathbb{Z}_p$. Una casi progresión aritmética es de la forma

$$\{a + id : 0 \leq i \leq k, i \neq t\}$$

con $t \in [1, k - 1]$ fijo.

Teorema 7 *Sean $\varnothing \neq A, B \subseteq \mathbb{Z}_p$. Tómese $a, b, c, d \in \mathbb{Z}_p$ con $d \neq 0$ y l, t enteros positivos. Supóngase que $|A + B| \geq |A| + |B|$. Entonces*

$$|A + B| = |A| + |B|$$

si y sólo si A y B satisfacen alguna de las siguientes condiciones:

(i) $|A| + |B| = p$.

(ii) $\overline{B} = (c - A) \cup e$ *para* $c \notin A + B$ *y alguna* $e \in \mathbb{Z}_p$.

(iii) $A = \{a, a + d\}$ *y* B *es la unión de dos progresiones aritméticas con la misma diferencia común* d.

(iv) A *y* B *son una progresión aritmética y una casi progresión aritmética con la misma diferencia común* d, *respectivamente.*

(v) $A = T_a[l, l + 1]$ *y* $B = T_b[l, l + 1]$ *para* $l \geq 2$ *y* $l \neq \frac{p-1}{2}$.

(vi) $A = T_a[2, l - 1]$ *y* $B = T_b[2, t - 1]$ *donde* $l \geq 4$ *y* $t \geq 4$.

Teorema 8 *Sean* $\varnothing \neq A, B \subseteq \mathbb{Z}_p$. *Tómese* $a, b, c, d \in \mathbb{Z}_p$ *con* $d \neq 0$ *y* l, t *enteros positivos. Supongase que* $|A+B| \geq |A| + |B| + 1$. *Entonces*

$$|A+B| = |A| + |B| + 1$$

si y sólo si A *y* B *satisfacen alguna de las siguientes condiciones:*

(i) $|A| + |B| = p - 1$.

(ii) $\overline{B} = (c - A) \cup \{t_1, t_2\}$ *para* $c \notin A + B$ *y* $t_1, t_2 \in \mathbb{Z}_p$ *tal que* $t_1 \neq t_2$.

(iii) $A = \{a, a+d, a+2d\}$ *y* B *sea la unión de dos progresiones aritméticas con la misma diferencia común* d *tal que la longitud de todos los hoyos de* B *sea al menos de* 2.

(iv) $A = \{a, a+d\}$ *y* B *sea la unión de tres progresiones aritméticas con la misma diferencia común* d.

(v) *Sea* A *una progresión con diferencia* d *y sea* B *la unión de dos o tres progresiones aritméticas con la misma diferencia* d *tal que*

$$B = \{b + id \mid i \in [0, r-1] \cup [r+2, s-1]\}$$

donde $r \leq s+1$ *y* $s \leq p-2$, *o*

$$B = \{b + id \mid i \in [0, r-1] \cup [r+1, t-1] \cup [t+1, v-1]\}$$

donde $r \leq t-2$, $t \leq v-2$ *y* $v \leq p-2$.

(vi) $3 \leq |A|, |B| \leq 4$ *y el par* (A, B) *es uno de la siguiente lista:*

$$(T_a[m, m+1], T_b[m+1, m+2]), \text{ para } m \geq 2,$$

$$(T_a[m, m+2], T_b[m+1, m+2]), \text{ para } m \geq 2,$$

$$(T_a[m, m+1], T_b[m, m+2]), \text{ para } m \geq 3 \text{ o}$$

$$(T_a[m, m+2], T_b[m, m+2]), \text{ para } m \geq 3.$$

(vii) *El par* (A, B) *es* $(T_a[m, n-1], T_b[3, t-1])$ *para* $m = 2$ *o* $m = 3$ *y* $n, t \geq 6$.

$(viii)$ A *y* B *son casi progresiones aritméticas con la misma diferencia común* d *tal que* $(A, B) \neq (T_a[2, l-1], T_b[2, t-1])$ $(l \geq 4, t \geq 4)$.

(ix) $(A, B) = (T_a[2, m-1], T_b[2, s-1] \cup [s+1, t-1])$, *donde* $s \leq t-2$.

(x) $(A, B) = (T_a[l, l+1], T_b[l, l+1] \cup [l+3, m-1])$, *donde* $2 \leq l \leq m-4$.

(xi) $(A, B) = (U_a(i, j; m), U_b(i, j; m))$, *para* $(i, j) \in \{(1,2), (1,3), (2,3)\}$.

La conjetura de Erdös-Heilbronn, que se menciona en el siguiente teorema, se formuló en los años 60's. Erdös y Heilbronn no la incluyeron en su artículo [23] sobre sumas de conjuntos de clase de congruencias. Sin embargo, en el año 1963, en una conferencia sobre teoría de números en la Universidad de Colorado, Erdös [22] establece la conjetura, la cual mencionaría, frecuentemente, en sus artículos y conferencias posteriores. Se dieron resultados parciales a la conjetura por Rickert en 1976 [15], Mansfield en 1981[16], Rödseth en 1993 [17], Pyber en una publicación personal [18] y Freiman, Low y Pitman en 1993 [19].

Teorema 9 *Si A es un conjunto de clases de congruencias módulo un número primo p entonces*

$$|2\hat{}A| \geq \min\{p, 2|A| - 3\}.$$

Llevó más de 30 años antes de que Dias da Silva y Hamidoune publicaran la demostración de este teorema en el año 1994 [20]. No sólo demostraron la conjetura sino también la generalización:

$$|h\hat{}A| \geq \min\left\{p, h|A| - h^2 + 1\right\},$$

donde

$$\begin{aligned} A_1 \mathbin{\widehat{+}} A_2 \mathbin{\widehat{+}} \cdots \mathbin{\widehat{+}} A_n &= \left\{ \begin{array}{c} x \mid x = a_1 + a_2 + \cdots + a_n, a_i \in A_i, a_i \neq a_j \\ \text{si } i \neq j \end{array} \right\} \\ \text{y } h\hat{}A &= \underbrace{A \mathbin{\widehat{+}} A \mathbin{\widehat{+}} \cdots \mathbin{\widehat{+}} A}_{h}. \end{aligned}$$

Obsérvese que si $h = 2$ entonces se obtiene la conjetura de Erdös-Heilbronn. Esta demostración utiliza resultados de la teoría de representaciones y álgebra lineal avanzada.

En 1995, Alon, Nathanson y Ruzsa [4-5] dieron una nueva demostración de la conjetura de Erdös-Heilbronn. En su demostración introducen el método polinomial.

En el artículo donde Alon, Nathanson y Ruzsa publican sus resultados, dejan abierto un problema (entre muchos otros), el cual pregunta para qué tipo de conjuntos se cumple que

$$|2\hat{}A| = 2|A| - 3. \tag{1}$$

Un hecho importante es que todo lo que se cumple para $\mathbb{Z}_p$ se cumple para $\mathbb{Z}$. Esto se debe al teorema fundamental de grupos abelianos finitamente

generados. O sea, si tenemos un subconjunto finito de $\mathbb{Z}$, solo es necesario buscar un número primo mayor a la suma de los dos elementos más grandes de dicho subconjunto y con esto podemos trabajar en $\mathbb{Z}_p$, donde se cumple el teorema, imitando estar trabajando en $\mathbb{Z}$.

De el hecho anterior podemos concluir que para cualquier subconjunto finito A de $\mathbb{Z}$ se cumple que

$$|h\hat{}A| \geq \min\left\{p, h\,|A| - h^2 + 1\right\}.$$

Nathanson demostró por el año de 1995 [21] que la igualdad, en el caso de $\mathbb{Z}$, se da sí y sólo si A es una progresión aritmética. En 1998, Hui-Qin Cao y Zhi-Wei Sun [7] demostraron el siguiente teorema.

Teorema 10 *Sean $A_1, A_2, ..., A_n$ subconjuntos de $\mathbb{Z}$ con $0 < |A_1| < |A_2| < ... < |A_n| < \infty$. Entonces se cumple que*

$$\left|A_1 \mathbin{\widehat{+}} A_2 \mathbin{\widehat{+}} \cdots \mathbin{\widehat{+}} A_n\right| \geq \sum_{i=1}^{n} |A_i| - \frac{n(n+1)}{2} + 1.$$

Más aún, la igualdad se cumple cuando $\bigcup_{i=1}^{m} A_i = A_m$ para cada

$$m \in M = \{1 \leq j \leq n-1 : |A_{j+1}| > |A_j| + 1\} \cup \{n\}$$

y A_n es una progresión aritmética para $n = 1$ o $|A_1| \leq 3$.

Este teorema da una buena aproximación a la estructura de los conjuntos en el caso de la igualdad.

En esta tesis, nos acercamos al problema inverso de caracterizar los conjuntos para los cuales la igualdad se cumple en $|2\hat{}A| = 2|A| - 3$.

En el capítulo 2 abordamos los resultados más relevantes de la teoría aditiva de números. Resaltamos la prueba del Teorema de Cauchy-Davenport según el segundo autor dada en 1935. En la misma, se da una demostración completa y novedosa del teorema, lo que posibilita su comprensión exacta en un lenguaje matemático muy actual.

En el capítulo 3 de la tesis se demuestra parte del problema de Nathanson, a saber, si $A = [0, l-1] \cup B$ con $[0, l-1]$ es la progresión aritmética más larga de A, entonces

$$\begin{aligned} 2\hat{}A &= \{a_i + a_j : a_i, a_j \in A, i \neq j\} \\ &= 2\hat{}[0, l-1] \cup ([0, l-1] + B) \cup 2\hat{}B. \end{aligned}$$

Se resuelven los siguientes casos:

1) Si $2\hat{}[0, l-1] \cup ([0, l-1] + B)$ es un intervalo.

2) Si $([0, l-1] + B) \cup 2\hat{}B$ es un intervalo.

3) Si $2\hat{}[0, l-1] \cup 2\hat{}B$ es un intervalo.

4) Si $2\hat{}[0, l-1] \cup ([0, l-1] + B) \cup 2\hat{}B$ es un intervalo.

Para completar la demostración de la igualdad, sólo queda considerar el caso en que no se dan las condiciones de 1-4. Este caso no se incluye.

Además, se demuestran algunos resultados interesantes que se fueron dando en la búsqueda de la solución al problema original. Se analizan diversos problemas directos con sumas de residuos distintos que permiten obtener conclusiones importantes acerca de la posible estructura de los conjuntos que satisfacen la igualdad en el problema de Erdös-Heilbronn. Es conocido y conjeturado que sólo los conjuntos que son progresiones aritméticas y sólo esos, dan la igualdad buscada. Para estos resultados se usan algunas de las ideas desarrolladas en [6].

Finalmente, se da una selección de las referencias más importantes de la vasta literatura existente en este tema.

2 Preliminares y resultados clásicos de la teoría aditiva de números

Sean $A \subseteq \mathbb{Z}_p$, p un número primo y $t \in \mathbb{Z}_p$. Se denota por $|A|$ a la cardinalidad del conjunto A y por $\overline{A}$ al complemento del conjunto A. Si $\varnothing \neq A, B \subseteq \mathbb{Z}_p$, entonces la suma de estos dos subconjuntos se define como

$$A + B = \{x \mid x = a + b, a \in A, b \in B\}.$$

Se define la suma de elementos distintos como

$$A \mathbin{\widehat{+}} B = \{x \mid x = a + b, a \in A, b \in B, a \neq b\}.$$

En el caso de n conjuntos definimos

$$A_1 + A_2 + \cdots + A_n = \{x \mid x = a_1 + a_2 + \cdots + a_n, a_i \in A_i\},$$

$$hA = \underbrace{A + A + \cdots + A}_{h},$$

$$A_1 \mathbin{\widehat{+}} A_2 \mathbin{\widehat{+}} \cdots \mathbin{\widehat{+}} A_n = \left\{ \begin{array}{c} x \mid x = a_1 + a_2 + \cdots + a_n, a_i \in A_i, a_i \neq a_j \\ \text{si } i \neq j \end{array} \right\},$$

$$h\widehat{\ }A = \underbrace{A \mathbin{\widehat{+}} A \mathbin{\widehat{+}} \cdots \mathbin{\widehat{+}} A}_{h}.$$

Se definen los siguientes conjuntos, donde $t \in \mathbb{Z}_p$:

$$\begin{aligned} A - B &= A + (-B), \\ -A &= \{-a \mid a \in A\}, \\ tA &= \{ta \mid a \in A\}, \\ A \setminus \{b\} &= \{a \in A \mid a \neq b\}, \\ A - t &= \{a - t \mid a \in A\}, \\ \overline{A} &= \{a' \in \mathbb{Z}_p \mid a' \notin A\}. \end{aligned}$$

Sean $a, d \in \mathbb{Z}_p$, $d \neq 0$ y $k \in \mathbb{N}$, entonces el conjunto

$$\{a + id : 0 \leq i \leq k\}$$

es una *progresión aritmética*. También existen conjuntos llamados *casi progresiones aritméticas*, los cuales son de la forma

$$\{a + id : 0 \leq i \leq k, i \neq t\},$$

donde $t \in [1, k-1]$, es decir, son conjuntos a los cuales le falta un solo elemento para ser una progresión aritmética.

Un *intervalo de* $\mathbb{Z}_p$ que se denota por $[m, n]$, para $m, n \in \mathbb{Z}_p$ con $m \leq n$, se define como el conjunto

$$[m, n] = \{m, m+1, ..., n\},$$

donde las sumas se toman módulo p.

A una progresión aritmética se le puede *normalizar*, esto es, restando el valor a y multiplicando por el inverso multiplicativo de $d \neq 0$, con lo cual el conjunto $\{a + id : 0 \leq i \leq k\}$ se transformaría en el intervalo $[0, k]$, el cual no pierde ninguna de sus propiedades estructurales, o sea

$$|2\{a + id : 0 \leq i \leq k\}| = |2[0, k]|$$

y

$$|2\hat{}\{a + id : 0 \leq i \leq k\}| = |2\hat{}[0, k]|.$$

En adelante, cuando hablemos de una progresión aritmética nos referiremos a ella como un intervalo.

Daremos a continuación una breve introducción a los anillos de polinomios, herramienta que usaremos en la exposición del método polinomial.

Sea $\mathbf{k}$ un campo. Un polinomio con coeficientes en $\mathbf{k}$ es una expresión de la forma

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

donde los $a_i \in \mathbf{k}$ y $n \geq 1$. El anillo de polinomios con coeficientes en un campo $\mathbf{k}$ se denota como $\mathbf{k}[x]$.

Sean $f(x), g(x) \in \mathbf{k}[x]$. La igualdad de estos polinomios

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n = b_0 + b_1 x + \cdots + b_m x^m = g(x)$$

es cierta sólo si se cumplen las condiciones $m = n$ y $a_j = b_j$ para todo $0 \leq j \leq n$.

La suma y multiplicación de dos polinomios se define como

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_i + b_i)x^i + \cdots$$

$$f(x) \cdot g(x) = c_0 + c_1 x + \cdots + c_i x^i + \cdots$$

respectivamente, donde

$$c_i := \sum_{r+s=i} a_r \cdot b_s.$$

El grado de un polinomio $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ con $a_n \neq 0$ se define como

$$gr(f(x)) := n.$$

Recordamos las propiedades para el grado de la suma y la multiplicación de polinomios:

(1) $gr(f \cdot g) = gr(f) + gr(g)$

(2) $gr(f + g) \leq \max\{gr(f), gr(g)\}$.

2.1 Conjetura Erdös-Heilbronn

2.1.1 Método polinomial

La conjetura de Erdös-Heilbronn nos dice que dados dos subconjuntos cualesquiera A y B de $\mathbb{Z}_p$ tales que sus cardinalidades sean distintas, la cardinalidad de $A \stackrel{\frown}{+} B$ siempre será mayor o igual al $\min\{p, |A| + |B| - 2\}$. Para la prueba de esta conjetura se utilizarán dos lemas, que están basados en la teoría de polinomios en un anillo $\mathbf{k}[x]$ con $\mathbf{k}$ un campo, y se demuestran a continuación.

Lema 11 *Sea A un subconjunto finito no vacío de un campo $\mathbf{k}$, y sea $|A| = k$. Para cualquier $m \geq 0$ existe un polinomio $g_m(x) \in \mathbf{k}[x]$ de grado a lo más $k-1$ tal que*

$$g_m(a) = a^m,$$

para toda $a \in A$.

Demostración. Sea $A = \{a_0, a_1, ..., a_{k-1}\}$ y sea $m \geq 0$. Lo que intentaremos probar será que existe un polinomio $u(x) = u_0 + u_1 x + \cdots + u_{k-1}x^{k-1} \in \mathbf{k}[x]$ tal que

$$u(a_i) = u_0 + u_1 a_i + \cdots + u_{k-1}a_i^{k-1} = a_i^m$$

para $i = 0, 1, ..., k-1$. Si le damos todos los valores a i entonces tenemos

$$\begin{aligned} u(a_0) &= u_0 + u_1 a_0 + \cdots + u_{k-1}a_0^{k-1} = a_0^m \\ u(a_1) &= u_0 + u_1 a_1 + \cdots + u_{k-1}a_1^{k-1} = a_1^m \\ &\vdots \\ u(a_{k-1}) &= u_0 + u_1 a_{k-1} + \cdots + u_{k-1}a_{k-1}^{k-1} = a_{k-1}^m. \end{aligned}$$

Lo cual es un sistema de k ecuaciones lineales en k variables $u_0, u_1, ..., u_{k-1}$ y el mismo tiene solución si el determinante asociado no es igual a cero. El determinante que resulta es

$$V = \begin{vmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^{k-1} \\ 1 & a_1 & a_1^2 & \cdots & a_1^{k-1} \\ \vdots & & & & \vdots \\ 1 & a_{k-1} & a_{k-1}^2 & \cdots & a_{k-1}^{k-1} \end{vmatrix},$$

el cual es un determinante de Vandermonde. Sabemos que

$$V = \prod_{0 \leq i < j \leq k-1} (a_j - a_i)$$

y como $(a_j - a_i) \neq 0$ para toda $0 \leq i < j \leq k-1$, por lo tanto $V \neq 0$. Se concluye que el sistema de ecuaciones planteado tiene solución única en las variables $u_0, u_1, ..., u_{k-1}$. ■

Lema 12 *Sean $h \geq 1$ y $A_0, A_1, ...A_{h-1}$ subconjuntos no vacíos de un campo $\mathbf{k}$ con $|A_i| = k_i$ para $i = 0, 1, ..., h-1$. Sea $f(x_0, x_1, ..., x_{h-1})$ un polinomio*

con coeficientes en $\mathbf{k}$ *y de grado a lo más* $k_i - 1$ *en* x_i *para* $i = 0, 1, ...h - 1$. *Si*

$$f(a_0, a_1, ..., a_{h-1}) = 0$$

para toda

$$(a_0, a_1, ..., a_{h-1}) \in A_0 \times A_1 \times ... \times A_{h-1},$$

entonces $f(x_0, x_1, ..., x_{h-1})$ *es el polinomio cero.*

Demostración. La demostración se hará por inducción sobre h. Para la base de inducción, cuando $h = 1$, se tiene un polinomio de una variable con grado a lo más $k_0 - 1$. Todo polinomio distinto de cero en $\mathbf{k}[x]$ con grado a lo más $k_0 - 1$ no puede tener k_0 raíces distintas en $\mathbf{k}$, por el teorema fundamental del álgebra, lo cual sería una contradicción de la hipótesis que $f(a_0) = 0$ para toda $a_0 \in A_0$ si $f(a_0)$ no fuera el polinomio cero. Por lo tanto $f(x_0)$ es el polinomio cero. Sea $h \geq 2$, y supongamos que el lema es cierto para polinomios de a lo más $h - 1$ variables. Podemos escribir el polinomio de la siguiente manera

$$f(x_0, x_1, ..., x_{h-1}) = \sum_{j=0}^{k_0-1} f_j(x_1, ...x_{h-1}) x_0^j,$$

donde $f_j(x_1, ..., x_{h-1})$ es un polinomio en las $h - 1$ variables $x_1, ..., x_{h-1}$ y su grado es a lo más $k_i - 1$ en x_i para $i = 1, ..., h - 1$. Fijemos

$$(a_1, ..., a_{h-1}) \in A_1 \times \cdots \times A_{h-1},$$

definamos $g(x_0)$ de la siguiente forma

$$g(x_0) \colon = f(x_0, a_1, ..., a_{h-1}) = \sum_{j=0}^{k_0-1} f_j(a_1, ..., a_{h-1}) x_0^j.$$

El polinomio $g(x_0)$ es un polinomio de grado a lo más $k_0 - 1$, con variable x_0 y coeficientes $f_j(a_1, ..., a_{h-1})$ para $0 \leq j \leq k_0 - 1$, tal que $g(a_0) = 0$ para toda $a_0 \in A_0$ ya que por hipótesis teníamos que $f(a_0, a_1, ..., a_{h-1}) = 0$ para toda $(a_0, a_1, ..., a_{h-1}) \in A_0 \times A_1 \times \cdots \times A_{h-1}$. Eso quiere decir que $g(x_0)$ tiene al menos $|A_0| = k_0$ raíces distintas y por el paso base de la inducción, entonces $g(x_0)$ es el polinomio cero. Ya con esto podemos decir que

$$f_j(a_1, ..., a_{h-1}) = 0$$

para toda

$$(a_1, ..., a_{h-1}) \in A_1 \times \cdots \times A_{h-1},$$

y $0 \leq j \leq k_0 - 1$. Por hipótesis de inducción podemos decir que el polinomio $f_j(x_1, ..., x_{h-1})$ es el idénticamente cero para $0 \leq j \leq k_0 - 1$. Como

$$f(x_0, x_1, ..., x_{h-1}) = \sum_{j=0}^{k_0-1} f_j(x_1, ..., x_{h-1}) x_0^j,$$

por lo tanto $f(x_0, x_1, ..., x_{h-1})$ es el polinomio cero. ■

Teorema 13 *Sea p un número primo, y sean A y B subconjuntos no vacíos de $\mathbb{Z}_p$ tal que $|A| \neq |B|$. Sea*

$$A \widehat{+} B = \{a + b : a \in A, b \in B, a \neq b\}.$$

Entonces

$$\left|A \widehat{+} B\right| \geq \min\{p, |A| + |B| - 2\}.$$

Demostración. Sea $|A| = k$ y $|B| = l$. Podemos suponer que

$$1 \leq l < k \leq p.$$

Caso 1: Si $k + l - 2 > p$, entonces la demostración se hará por inducción sobre la cardinalidad de B mayor o igual a 3. Si $|B| = l = 3$ entonces $k + 3 - 2 = k + 1 > p$, lo que implica que $|A| = k > p - 1$. Supongamos entonces que $|A| = p$. Sean

$$A = \{1, 2, ..., p - 1, p\}$$

y

$$B = \{b_1, b_2, b_3\}.$$

Se sigue que

$$\begin{aligned} A \widehat{+} B &= (\{1, 2, ..., p-1, p\} \widehat{+} \{b_1\}) \cup \\ &\quad (\{1, 2, ..., p-1, p\} \widehat{+} \{b_2\}) \cup \\ &\quad (\{1, 2, ..., p-1, p\} \widehat{+} \{b_3\}). \end{aligned}$$

Por la definición de $\widehat{+}$,

$$\{1, 2, ..., p-1, p\} \widehat{+} \{b_1\} = \mathbb{Z}_p \setminus \{2b_1\},$$

como $b_1 \neq b_2$ y $\mathbb{Z}_p$ es un campo entonces existe $c \in \mathbb{Z}_p$ con $c \neq b_2$ tal que $2b_1 = c + b_2$ por lo que $2b_1 \in (\{1, 2, ..., p-1, p\} \widehat{+} \{b_2\})$, entonces $A \widehat{+} B = \mathbb{Z}_p$. Por lo tanto

$$\left|A \widehat{+} B\right| = p \geq \min\{p, |A| + |B| - 2\}.$$

Podemos ahora suponer que se cumple para $3 \leq |B| \leq l - 1$ y demostraremos el teorema para $|B| = l$. Sea $l' = p - k + 2$. Entonces

$$2 \leq l' < l \leq k$$

y

$$k + l' - 2 = p.$$

Escojamos $B' \subseteq B$ tal que $|B'| = l'$. Como el teorema es cierto para $l' < l$ entonces tenemos que

$$\left|A \widehat{+} B'\right| \geq \min\{p, k + l' - 2\} = p = \min\{p, |A| + |B| - 2\}.$$

Como $A \widehat{+} B' \subseteq A \widehat{+} B$, se tiene que

$$\left|A \widehat{+} B'\right| < \left|A \widehat{+} B\right|.$$

Entonces

$$\left|A \widehat{+} B\right| \geq \min\{p, |A| + |B| - 2\}.$$

Caso 2: Si $k + l - 2 \leq p$. Sea $C = A \widehat{+} B$. Probaremos que $|C| \geq k + l - 2$. Si

$$|C| \leq k + l - 3$$

entonces escojemos una $r \geq 0$ tal que

$$r + |C| = k + l - 3.$$

Construyamos entonces tres polinomios f_0, f_1 y f en el anillo $\mathbb{Z}_p[x, y]$, de la siguiente forma. Sea

$$f_0(x, y) = \prod_{c \in C} (x + y - c).$$

Entonces el $gr(f_0) = |C| \leq k + l - 3$ y

$$f_0(a, b) = 0 \text{ para toda } a \in A, b \in B, a \neq b.$$

Sea

$$f_1(x,y) = (x-y)\, f_0\,(x,y)\,.$$

Entonces

$$\begin{aligned} gr(f_1) &= gr((x-y)\, f_0) = gr(f_0)+1 \\ &= |C|+1 \leq (k+l-3)+1 = k+l-2 \end{aligned}$$

y

$$f_1\,(a,b) = 0 \text{ para toda } a \in A, b \in B,$$

ya que $f_0\,(a,b) = 0$ para toda $a \in A, b \in B, a \neq b$ y por último si $a = b$ entonces $a-b=0$. Multipliquemos ahora a f_1 por $(x+y)^r$, con lo cual obtenemos el siguiente polinomio

$$f(x,y) = (x+y)^r\,(x-y)\prod_{c\in C}(x+y-c)$$

que sería de grado exactamente $1+r+|C| = k+l-2$ y cumpliría que

$$f(a,b) = 0 \text{ para toda } a \in A, b \in B.$$

Este polinomio tiene coeficientes $u_{m,n} \in \mathbb{Z}_p$ tales que podemos escribirlo de la siguiente forma

$$\begin{aligned} f(x,y) &= \sum_{\substack{m,n\geq 0 \\ m+n\leq k+l-2}} u_{m,n}x^m y^n \\ &= (x-y)\,(x+y)^r \prod_{c\in C}(x+y-c) \\ &= (x-y)\,(x+y)^{k+l-3} + \text{ términos de orden menor} \\ &= x\,(x+y)^{k+l-3} - y\,(x+y)^{k+l-3} + \text{ términos de orden menor.} \end{aligned}$$

Observemos que $1 \leq l < k \leq p$ y $1 \leq k+l-3 < p$, ya que por hipótesis teníamos que $k+l-2 \leq p$ y $k+l-3 \leq k+l-2$. Por la transitividad obtenemos la desigualdad estricta, se sigue que el coeficiente $u_{k-1,l-1}$ del monomio $x^{k-1}y^{l-1}$ en $f(x,y)$ se obtiene del desarrollo

$$x\,(x+y)^{k+l-3} = x\sum_{i=0}^{k+l-3}\binom{k+l-3}{i}x^i y^{k+l-3-i}.$$

Entonces $i = k-2$, por lo que el coeficiente es igual a

$$\binom{k+l-3}{k-2}.$$

Por otra parte, el coeficiente se obtiene también de:

$$y\,(x+y)^{k+l-3} = y\sum_{i=0}^{k+l-3}\binom{k+l-3}{i}x^i y^{k+l-3-i}$$

entonces $i = k-1$ por lo que el coeficiente sería

$$\binom{k+l-3}{k-1}.$$

Ahora el coeficiente general es la resta de los dos anteriores, esto es

$$\begin{aligned}
& \binom{k+l-3}{k-2} - \binom{k+l-3}{k-1} \\
= \; & \frac{(k+l-3)!}{(k+l-3-(k-2))!\,(k-2)!} - \frac{(k+l-3)!}{(k+l-3-(k-1))!\,(k-1)!} \\
= \; & \frac{(k-1)\,(k+l-3)!}{(k-1)!\,(l-1)!},
\end{aligned}$$

lo cual no es congruente a 0 modulo p. Esto es equivalente a decir que siempre es distinto de cero, ya que $1 < k$ y $(k+l-3)! \neq 0$. Por el Lema 11, para toda $m \geq k$ existe un polinomio $g_m(x)$ de grado a lo más $k-1$ tal que

$$g_m(a) = a^m \text{ para toda } a \in A,$$

y para toda $n \geq l$ existe un polinomio $h_n(y)$ de grado a lo más $l-1$ tal que $h_n(b) = b^n$ para toda $b \in B$. Utilicemos los polinomios $g_m(x)$ y $h_n(y)$ para construir un polinomio $f^*(x,y)$ a partir de $f(x,y)$ de la siguiente manera. Si $x^m y^n$ es un monomio en $f(x,y)$ con $m \geq k$, entonces reemplazamos $x^m y^n$ por $g_m(x)y^n$. Observemos que

$$gr(f(x,y)) = k+l-2.$$

Se sigue que si $m \geq k$, entonces $n \leq l-2$, ya que la suma de las potencias de cualquier monomio no puede ser mayor al grado del polinomio,

y así $g_m(x)y^n$ es la suma de monomios $x^i y^j$ con $i \leq k-1$ y $j \leq l-2$ (el grado de $g_m(x)$ es a lo más $k-1$). Similarmente, si $x^m y^n$ es un monomio en $f(x,y)$, pero ahora con $n \geq l$, entonces reemplazamos $x^m y^n$ por $x^m h_n(y)$. Si $n \geq l$ entonces $m \leq k-2$, ya que

$$gr(f(x,y)) = k + l - 2,$$

y asi $x^m h_n(y)$ es una suma de monomios $x^i y^j$ con $i \leq k-2$ y $j \leq l-1$. Lo que hicimos con este proceso es disminuir el grado de $f(x,y)$ obteniendo un nuevo polinomio $f^*(x,y)$ de grado $k-1$ en x y $l-1$ en y. El proceso de construcción de $f^*(x,y)$ no alteró el coeficiente $u_{k-1,l-1}$ del término $x^{k-1}y^{l-1}$, ya que el monomio $x^{k-1}y^{l-1}$ nunca aparece en $g_m(x)y^n$ y $x^m h_n(y)$, entonces $u_{k-1,l-1} \neq 0$. Por otro lado,

$$f^*(a,b) = f(a,b) = 0$$

para toda $a \in A$ y $b \in B$. Se sigue, por el Lema 12, que el polinomio $f^*(x,y)$ es el idénticamente cero. Esto contradice el hecho de que el coeficiente $u_{k-1,l-1}$ de $x^{k-1}y^{l-1}$ en $f^*(x,y)$ es distinto de cero. Por lo que

$$|C| \leq k + l - 3,$$

lo cual se quería demostrar. ■

De este teorema y del hecho que $2\hat{}A = A \mathbin{\widehat{+}} B$ cuando $B := A \setminus \{a\}$ se desprende el siguiente corolario:

Corolario 14 *Sea $a \in A \subset \mathbb{Z}_p$ cualquier elemento y $B := A \setminus \{a\}$, donde $|B| = |A| - 1$, entonces*

$$\left|A \mathbin{\widehat{+}} B\right| = |2\hat{}A| \geq 2|A| - 3 = |A| + |B| - 2.$$

Con esto se demuestra la conjetura de Erdös-Heilbrounn.

2.2 Teorema de Cauchy-Davenport

2.2.1 Demostración de Nathanson.

Para poder demostrar el teorema de Cauchy-Davenport primero tenemos que introducir algunos conceptos y demostrar algunos teoremas.

Lema 15 *Sea G un grupo abeliano, sean A y B subconjuntos de G tal que $|A| + |B| > |G|$. Entonces $A + B = G$.*

Demostración. Trivial. ■

Introducimos un concepto llamado la *e-transformación*, y demostramos algunas de sus propiedades.

Definición 16 *Sean $A, B \subseteq G$ y $e \in G$. La e-transformación de (A, B) es el par $(A(e), B(e))$, subconjuntos de G, definidos de la siguiente forma*

$$\begin{aligned} A(e) &= A \cup (B + e) \\ B(e) &= B \cap (A - e). \end{aligned}$$

Lema 17 *Sean A y B subconjuntos no vacíos de un grupo abeliano G, y sea e cualquier elemento de G. Sea $(A(e), B(e))$ el par de conjuntos obtenidos por la e-transformación del par (A, B). Entonces*

$$A(e) + B(e) \subseteq A + B$$

y

$$A(e) \diagdown A = e + (B \diagdown B(e)).$$

Si A y B son conjuntos finitos, entonces

$$|A(e)| + |B(e)| = |A| + |B|.$$

Si $e \in A$ y $0 \in B$ entonces $e \in A(e)$ y $0 \in B(e)$.

Demostración. Por la definición 16, $A(e) = A \cup (B + e)$ y $B(e) = B \cap (A - e)$ que son subconjuntos de A y B respectivamente, esto es, $A(e) \subseteq A$ y $B(e) \subseteq B$. Con lo que concluimos que

$$A(e) + B(e) \subseteq A + B.$$

Para probar que

$$A(e) \diagdown A = e + (B \diagdown B(e)),$$

sólo tenemos que observar que

$$\begin{aligned} A(e)\diagdown A &= (A \cup (B+e))\diagdown A \\ &= (B+e)\diagdown A \\ &= \{b+e : b \in B, b+e \notin A\} \\ &= e + \{b \in B : b \notin A - e\} \\ &= e + \{b \in B : b \notin B(e)\} \\ &= e + (B\diagdown B(e)). \end{aligned}$$

Es claro que $A \subseteq A(e)$ y $B(e) \subseteq B$. Para demostrar que

$$|A(e)| + |B(e)| = |A| + |B|$$

cuando A y B son conjuntos finitos sólo observemos que

$$\begin{aligned} |A(e)| - |A| &= |A(e)\diagdown A| \\ &= |e + (B\diagdown B(e))| \\ &= |B\diagdown B(e)| \\ & \quad |B| - |B(e)|\,. \end{aligned}$$

Entonces

$$\begin{aligned} |A(e)| - |A| &= |B| - |B(e)|\,, \\ |A(e)| + |B(e)| &= |A| + |B|\,. \end{aligned}$$

Si $e \in A$ y $0 \in B$ entonces $0 \in A - e$ y así $0 \in B \cap (A - e) = B(e)$ y como $A \subseteq A(e)$, entonces $e \in A(e)$. ■

Para la demostración del teorema de Cauchy-Davenport probaremos el teorema de I. Chowla que generaliza al anterior. Así, el teorema de Cauchy-Davenport resulta un corolario.

Teorema 18 *(I.Chowla) Sea $m \geq 2$, y sean A y B subconjuntos no vacíos de $\mathbb{Z}_m$. Si $0 \in B$ y $m.c.d(b,m) = 1$ para toda $b \in B\diagdown\{0\}$, entonces*

$$|A+B| \geq \min\{m, |A| + |B| - 1\}\,.$$

Demostración. Por el Lema 15, el resultado es cierto si $|A| + |B| > m$. Luego podemos suponer que $|A| + |B| \leq m$, y así

$$\min\{m, |A| + |B| - 1\} = |A| + |B| - 1 \leq m - 1.$$

Si $|A| = 1$, entonces

$$\begin{aligned} |A + B| &= |\{a + b : a \in A, b \in B\}| \\ &= |\{a + b : b \in B\}| = |B|. \end{aligned}$$

Por otro lado

$$\begin{aligned} \min\{m, |A| + |B| - 1\} &= |A| + |B| - 1 \\ &= 1 + |B| - 1 = |B|, \end{aligned}$$

por lo que

$$|A + B| \geq \min\{m, |A| + |B| - 1\}.$$

En el caso en que $|B| = 1$, se demuestra de igual forma el teorema. Ahora podemos asumir que $|A| \geq 2$ y $|B| \geq 2$, supongamos que

$$|A + B| < |A| + |B| - 1.$$

En particular, $A \neq \mathbb{Z}_m$. Tomemos el par (A, B) tal que la cardinalidad de B sea mínima. Observemos que $|B| \geq 2$, entonces existe un elemento $b^* \in B$ tal que $b^* \neq 0$. Si $a + b^* \in A$ para toda $a \in A$, entonces $a + jb^* \in A$ para toda $j = 0, 1, 2, ...$, ya que si $a + b^* = a' \in A$ entonces

$$a' + b^* = a + 2b^* \in A$$

y así sucesivamente. Observemos que m.c.d$(b^*, m) = 1$, lo cual implica que

$$\mathbb{Z}_m = \{a + jb^* : j = 0, 1, ..., m - 1\} \subseteq A \subseteq \mathbb{Z}_m,$$

y así $A = \mathbb{Z}_m$, lo cual es falso. Después, existe un elemento $e \in A$ tal que $e + b^* \notin A$. Aplicando la e-transformación al par (A, B). Por el Lema 17 se tiene que $A(e) + B(e) \subseteq A + B$, y así

$$|A(e) + B(e)| \leq |A + B| < |A| + |B| - 1 = |A(e)| + |B(e)| - 1.$$

Ya que $e \in A$ y $0 \in B$, se sigue que $0 \in B(e) \subseteq B$, y m.c.d$(b, m) = 1$ para toda $b \in B(e) \setminus \{0\}$ Luego $e + b^* \notin A$, se tiene que $e + b^* \notin A$, de donde se obtiene que $b^* \notin A - e$, y así

$$b^* \notin B \cap (A - e) = B(e).$$

Entonces, $|B(e)| < |B|$, lo cual contradice que $|B|$ sea mínima. Así completamos la prueba. ■

Teorema 19 *(Cauchy-Davenport) Sea p un número primo, y sean A, B subconjuntos no vacíos de $\mathbb{Z}_p$. Entonces*

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

Demostración. Sea $b_0 \in B$ y $B' = B - b_0$. Entonces $|B'| = |B|$ y

$$|A + B'| = |A + B - b_0| = |A + B|.$$

Sabemos que $0 \in B'$ y m.c.d$(b, p) = 1$ para toda $b \in B' \setminus \{0\}$ ya que $b_0 \in B$ y p es un número primo, aplicando el Teorema 18 al par (A, B') obtenemos que

$$\begin{aligned} |A + B| &= |A + B'| \\ &\geq \min\{p, |A| + |B'| - 1\} \\ &= \min\{p, |A| + |B| - 1\}. \end{aligned}$$

Con esto se completa la prueba. ■

2.2.2 Demostración de H. Davenport.

Teorema 20 *(Cauchy-Davenport). Sea $\varnothing \neq A, B \subseteq \mathbb{Z}_p$. Entonces se cumple que*

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

Demostración. Sean $A = \{a_1, ..., a_m\}$, $B = \{b_1, ..., b_n\}$ y

$$C = \{c_1, ..., c_l\} = A + B.$$

Supongamos que

$$\min\{p, |A| + |B| - 1\} = |A| + |B| - 1$$

o sea, $|A| + |B| - 1 \leq p$. La prueba la haremos por inducción sobre la cardinalidad de B. Para $|B| = n = 1$,

$$A + B = \{a_1 + b_1, ..., a_m + b_1\},$$

todos los elementos en este conjunto son distintos ya que si hubiera dos iguales entonces tendríamos que $a_i + b_1 = a_j + b_1$ lo cual implicaría que $a_i = a_j$, lo cual es imposible. Entonces

$$|A + B| = |A| = |A| + |B| - 1$$

por lo que se cumple el teorema. Para $n = 2$, escribamos $b = b_1 - b_2 \neq 0$ con $b_1, b_2 \in B$, y observemos que, si el teorema es falso, esto es,

$$|A + B| < |A| + |B| - 1 = m + 2 - 1 = m + 1 \leq p,$$

entonces, para cada a_i, el elemento $a_i + b \in A$, ya que si no fuera cierto,

$$a_i + b = t = a_i + b_1 - b_2$$

con $t \notin A$. Esto implicaría que $t + b_2 = a_i + b_1$ con $t \notin A$. Se tiene por un lado que $t + b_2 \notin A + B$ y por el otro lado tenemos que $a_i + b_1 \in A$, lo cual nos lleva a una contradicción. Entonces para cada entero u, $a_i + ub \in A$. La justificación de este hecho se hará de manera recursiva. Como $a_i + b \in A$, entonces $a_i + b$ es una $a_j \in A$, esto es, $a_j = a_i + b$. Sumando b de ambos lados de la igualdad obtenemos que $a_j + b = a_i + 2b$ y como $a_j + b \in A$ resultaría que $a_i + 2b \in A$. Utilizando ahora el hecho de que $a_i + 2b \in A$, entonces $a_i + 2b = a_r$ con $a_r \in A$. Sumando b de ambos lados, obtenemos que

$$a_r + b = a_i + 3b \in A.$$

Siguiendo recursivamente este algoritmo obtenemos la justificación. Como $\mathbb{Z}_p$ es un campo, entonces todos sus elementos pueden ser escritos de la forma $a_i + ub$, por lo que $m = p$, lo cual es una contradicción a la hipótesis de que $m + 2 - 1 \leq p$. Ahora podemos suponer que $n > 2$ y que el teorema es cierto para $n' < n$. También supongamos que $l < p$. Apliquemos el teorema para los conjuntos $\{c_1, ..., c_l\}$ y $\{b_1, b_n\}$. Como $l < p$ entonces $l + 2 - 1 \leq p$, con lo

que hay $l+1$ residuos de la forma c_i+b_1 y otros de la forma c_i+b_n. Entonces existe

$$c \in \{c_i + b_1 : 1 \leq i \leq l\} \setminus \{c_i + b_n : 1 \leq i \leq l\}.$$

Haciendo esto para cualquier par de elementos de B y renombrando los elementos de B, existe una r, $1 \leq r < n$, tal que

$$\begin{aligned} c - b_s &= c_s \in C \text{ para } 1 \leq s \leq r, \\ c - b_t &= e_t \notin C \text{ para } r < t \leq n, \\ e_t &\neq c_u \text{ para } r < t \leq n, 1 \leq u \leq l. \end{aligned}$$

Observamos que los residuos $c_s - b_t \notin A$ con $r < t \leq n$, $1 \leq s \leq r$ ya que si pasara lo contrario tendríamos que

$$\begin{aligned} c_s - b_t &= a_i, \\ c_s &= a_i + b_t, \\ c - b_s &= a_i + b_t, \\ c - b_t &= a_i + b_s \in C \end{aligned}$$

lo cual sería una contradicción. Entonces $c_s - b_t \notin A$ con $r < t \leq n, 1 \leq s \leq r$. Podría suceder que exista una $a \in A$ tal que

$$a + b_t = c_s = c - b_s,$$

es decir,

$$a + b_s = c - b_t = e_t,$$

y con esto obtener que $e_t \in C$, lo cual no es posible. Entonces los l' residuos representados en la forma $a_i + b_t$ $(1 \leq i \leq m, r < t \leq n)$ serían un subconjunto de $\{c_{r+1}, ..., c_l\}$. También $l' \leq l - r$. Pero por hipótesis de inducción y con $n' = n - r$, tenemos que

$$\begin{aligned} l' &\geq m + (n - r) - 1 \\ l &\geq m + n - 1 \end{aligned}$$

con lo que se concluye la demostración. ■

2.3 Teorema de Vosper

Primero daremos algunas definiciones, resolveremos algunos lemas y al final se dará la demostración del teorema. Trabajaremos con subconjuntos de un grupo abeliano G.

Definición 21 *Sean $A, B \subset G$, donde G es un grupo abeliano cualquiera, y $A, B \neq \varnothing$. Se dice que el par de conjuntos (A, B) es un par crítico si*

$$|A + B| = \min\{p, |A| + |B| - 1\}.$$

Esta definición habla de la igualdad en el teorema de Cauchy-Davenport.

Para la demostración de los lemas supondremos que

(i) $|A| + |B| < p - 1$,

(ii) $\min\{|A|, |B|\} > 1$,

(iii) $|A| = a$ y $|B| = b$.

Algo importante de notar es que si $|A| = a$, entonces $|A - t| = a$, ya que sólo se trata de una translación del conjunto.

Lema 22 *Si A es una progresión aritmética y (A, B) es un par crítico entonces A y B están en progresión aritmética con la misma diferencia.*

Demostración. Como A es progresión aritmética, entonces $A = [0, l - 1]$. El 1 es un generador de G, cada elemento de G es de la forma $r \cdot 1$ para un conjunto infinito de enteros r. Como $B \neq G$, entonces B debe tener al menos un hueco. Sea $[r, s]$ el hueco más largo de B de longitud t. Entonces $t \geq l$, ya que si $t < l$, tomemos un elemento cualquiera $g \in G$. El intervalo $[g - t, g]$ es de longitud $t + 1$. Entonces existe, por la definición de t, una $f \in [g - t, g]$ tal que $f \in B$ con $g - t \leq f \leq g$. Observamos que $0 \leq g - f \leq t < l$, de lo que se sigue que $g - f \in A$, y así

$$g = (g - f) + f \in A + B.$$

Entonces $G \subset A + B$, más aún, $G = A + B$. Llegamos con esto a una contradicción ya que $|A + B| < p - 1$. Denotemos

$$B - (s + 1) = \{n_0, n_1, ..., n_{b-1}\},$$

donde

$$0 \leq n_i < n_{i+1} < p \text{ para } 0 \leq i \leq b-1.$$

Como $s+1 \in B$, entonces $n_0 = 0$, y como $(r-1)-(s+1)$ es el mayor entero que está en B, entonces $n_{b-1} = p-t-1$, ya que la longitud del hueco más largo era t. Si definimos

$$A = A_1,\ B-(s+1) = B_1,$$

entonces (A_1, B_1) es un par crítico, ya que (A, B) lo es por hipótesis y

$$|A+B| = |(A_1+B)-(s+1)|,$$

con $|A_1| = l$, $|B_1| = b$, $|A_1+B_1| = l+b-1$ ya que $A_1+B_1 \supset B_1 \cup D$, donde

$$\begin{aligned} D &= A_1+(p-t-1) = [0, l-1]+(p-t-1) \\ &= [p-t-1, p+l-t-2], \end{aligned}$$

$|D| = |A_1|$ y $p+l-t-2 < p-1$ ya que $l \leq t$. Como el último elemento de B es $n_{b-1} = p-t-1$, entonces $B_1 \cap D = p-t-1$. Con lo que

$$\begin{aligned} |B_1 \cup D| &= |B_1|+|D|-|B_1 \cap D| \\ &= b+l-1 = |A_1+B_1|. \end{aligned}$$

Así $B_1 \cup D \subset A_1+B_1$ ya que $0 \in A_1$ y $D \subset A_1+B_1$. Con esto, podemos decir que $A_1+B_1 = B_1 \cup D$. Tomemos un elemento $\alpha \in B_1$, $0 \leq \alpha \leq p-t-2$. Como $1 \in A$, entonces $\alpha+1 \in A_1+B_1$. Pero $1 \leq \alpha+1 < p-t-1$, lo que implica que

$$\alpha+1 \notin D = [p-t-1, p+l-t-2],$$

y entonces $\alpha+1 \in B_1$. Por lo tanto, tenemos que $\alpha \in B_1$ para toda $\alpha \in [0, p-t-2]$, $B_1 = [0, p-t-2]$ y como $B = B_1-(s+1)$ tenemos que B es progresión aritmética. Luego, A y B están en progresión aritmética con la misma diferencia. ■

Corolario 23 *Si* $\min\{a, b\} = 2$ *y* (A, B) *es un par crítico, entonces* A *y* B *están en progresión aritmética con la misma diferencia.*

Demostración. Supongamos que $|A| = 2$. Cualquier conjunto con dos elementos siempre se encuentra en progresión aritmética. Entonces A está en progresión aritmética y aplicando el Lema 22 obtenemos el resultado. ■

Lema 24 *Si $a = b = 3$, y (A, B) es un par crítico entonces A y B están en progresión aritmética con la misma diferencia.*

Demostración. Sea $B = \{b_1, b_2, b_3\}$. Si

$$|(A + b_1) \cap (A + b_2)| \leq 1$$

entonces

$$|(A + b_1) \cup (A + b_2)| \geq 5 = |A + B|,$$

ya que (A, B) es un par crítico. Además

$$A + B = (A + b_1) \cup (A + b_2) \supset (A + b_3),$$

por lo que

$$|(A + b_3) \cap (A + b_i)| \geq 2$$

para $i = 1$ o 2. Por lo tanto podemos suponer que

$$|(A + b_1) \cap (A + b_2)| \geq 2,$$

pues si no fuera cierto, sólo renombramos a las $b's$. Entonces

$$\begin{aligned} & |(A + b_1) \cup (A + b_2)| \\ = \; & |(A + b_1)| + |(A + b_2)| - |(A + b_1) \cap (A + b_2)| \\ \leq \; & 3 + 3 - 2 = 4, \end{aligned}$$

pero por el Teorema 19 (Cauchy-Davenport)

$$|(A + b_1) \cup (A + b_2)| = 4,$$

por lo que (A, B_1), con $B_1 = \{b_1, b_2\}$, es un par crítico. Utilizando el Corolario 23, A y B_1 están en progresión aritmética con la misma diferencia y entonces A está en progresión aritmética. Por el Lema 22, A y B están en progresión aritmética con la misma diferencia. ■

Antes de pasar al siguiente lema demostraremos dos proposiciones relacionadas con la teoría de conjuntos.

Proposición 25 *Sean A, B, C, D conjuntos cualesquiera, entonces se cumple que*

$$(A + B) \cap C = \varnothing \Leftrightarrow A \cap (C - B) = \varnothing$$

Demostración. Supongamos que

$$\begin{aligned}(A+B)\cap C &= \varnothing \\ A\cap(C-B) &\neq \varnothing.\end{aligned}$$

Como $(A+B)\cap C=\varnothing$ entonces todo elemento de la forma $a+b\neq c$ para toda $a\in A, b\in B, c\in C$. Pero como $A\cap(C-B)\neq\varnothing$ existe un elemento $a\in A$ tal que $a=c-b$ con $c\in C, b\in B$, esto implica que $a+b=c$ lo que contradice el hecho de que $(A+B)\cap C=\varnothing$. Ahora supongamos que

$$\begin{aligned}(A+B)\cap C &\neq \varnothing \\ A\cap(C-B) &= \varnothing.\end{aligned}$$

Como $A\cap(C-B)=\varnothing$ entonces todo elemento de la forma $c-b\neq a$ para toda $a\in A, b\in B, c\in C$. Pero como $(A+B)\cap C\neq\varnothing$ existe un elemento $c\in C$ tal que $c=a+b$ con $a\in A, b\in B$. Esto implica que $a=c-b$ lo que contradice el hecho de que $A\cap(C-B)=\varnothing$. ■

Proposición 26 *Sean A, B, C, D conjuntos cualesquiera, entonces se cumple que*

$$(A-B)\cap(C+D)=\varnothing \Leftrightarrow (A-C)\cap(B+D)=\varnothing.$$

Demostración. Supongamos que

$$\begin{aligned}(A-B)\cap(C+D) &= \varnothing \\ (A-C)\cap(B+D) &\neq \varnothing.\end{aligned}$$

Entonces $a-b\neq c+d$ para toda $a\in A, b\in B, c\in C, d\in D$, esto implica que $a-c\neq b+d$ para toda $a\in A, b\in B, c\in C, d\in D$, lo cual contradice el hecho de que $(A-C)\cap(B+D)\neq\varnothing$. Por lo que $(A-C)\cap(B+D)=\varnothing$. Ahora supongamos que

$$\begin{aligned}(A-B)\cap(C+D) &\neq \varnothing \\ (A-C)\cap(B+D) &= \varnothing.\end{aligned}$$

Como $(A-B)\cap(C+D)\neq\varnothing$, entonces existen $a\in A, b\in B, c\in C, d\in D$ tales que $a-b=c+d$. Esto implica que $a-c=b+d$ teniendo como consecuencia que $(A-C)\cap(B+D)\neq\varnothing$, lo cual contradice el hecho que $(A-C)\cap(B+D)=\varnothing$. Por tanto $(A-C)\cap(B+D)\neq\varnothing$. ■

Podemos ahora, con las proposiciones 25 y 26, demostrar el siguiente lema.

Lema 27 *Si (A, B) es par crítico entonces $(-A, D)$ es par crítico, donde $D = \overline{A + B}$.*

Demostración. Se tiene que

$$(A + B) \cap D = \varnothing$$

ya que D es el complemento, por la Proposición 25 tenemos que

$$B \cap (D - A) = \varnothing,$$

y se sigue que

$$B \subseteq \overline{(D - A)} = X.$$

Luego,

$$X \cap (D - A) = \varnothing$$

y así, por la Proposición 25

$$(A + X) \cap D = \varnothing,$$

entonces

$$A + X \subset \overline{D} = A + B.$$

Como $B \subseteq X$, entonces

$$A + B \subseteq A + X$$

por lo que

$$A + B = A + X.$$

Como (A, B) es un par crítico,

$$\min\{p, a + |X| - 1\} \leq |A + X| = |A + B| = a + b - 1.$$

Por lo tanto $|X| \leq b$; pero $B \subseteq X$ con lo que $B = X$, $B = \overline{(D - A)}$ y $\overline{B} = D - A$. Entonces

$$|D - A| = p - b = \min\{p, |D| + |-A| - 1\},$$

ya que $|D| = p - a - b + 1$, y así $(-A, D)$ es un par crítico. ■

Corolario 28 *Si $a = b = \frac{1}{2}(p - 1)$ y (A, B) es un par crítico entonces A y B están en progresión aritmética con la misma diferencia.*

Demostración. Se tiene que

$$\begin{aligned} |A+B| &= |A|+|B|-1 \\ &= \frac{1}{2}(p-1)+\frac{1}{2}(p-1)-1 = p-2, \end{aligned}$$

ya que (A,B) es un par crítico, entonces $|D| = \left|\overline{A+B}\right| = 2$. Por el Lema 27 sabemos que $(-A,D)$ es un par crítico. Aplicando el Corolario 23 tenemos que $-A$ y D son progresiones aritméticas con la misma diferencia. Si $-A$ es progresión aritmética entonces A también lo es. Por el Lema 22 concluimos que A y B están en progresión aritmética con la misma diferencia. ■

Lema 29 *Si $b \geq a \geq 3$, $b \geq 4$ y $a, b \neq \frac{1}{2}(p-1)$ entonces existen $b_1, b_2 \in B$ tales que $(C+B) \cap (\overline{C+b_1}) \cap (\overline{C+b_2}) \neq \varnothing$, donde $C = A+B$.*

Demostración. Como (A,B) es un par crítico se cumple que

$$|C| = |A+B| = a+b-1,$$

si $|C+B| = s$, entonces

$$s \geq \min\{p, (a+b-1)+b-1\}$$

por el Teorema 19 (Cauchy-Davenport). Sea $B = \{b_1, b_2, ..., b_t\}$ con $b = t$, y supongamos que el Lema es falso. Los t conjuntos

$$X_i = (C+B) \cap (\overline{C+b_i}),\ i = 1, 2, ..., t$$

son todos disjuntos, ya que si no fueran disjuntos existirían i, j tales que

$$X_i \cap X_j = (C+B) \cap (\overline{C+b_i}) \cap (\overline{C+b_j}) \neq \varnothing$$

pero esto contradice el hecho que habíamos supuesto. Entonces $C+b_i \subseteq C+B$ y con esto

$$\begin{aligned} |X_i| &= s - |C+b_i| = s-a-b+1, \\ X_i &\subseteq (C+B). \end{aligned}$$

por lo que

$$\left| \bigcup_{1 \leq i \leq t} X_i \right| \leq |C+B|.$$

Entonces $b(s-a-b+1) \leq s$, o lo que es lo mismo,

$$b(a+b-1) \geq s(b-1). \tag{2}$$

Ahora hay tres casos que distinguir; en cada uno llegaremos a una contradicción:

Caso 1: Si $p \geq a+2b-2$. Entonces $s \geq a+2b-2$ y como

$$b(a+b-1) \geq s(b-1), b(a+b-1) \geq (a+2b-2)(b-1),$$

entonces

$$\begin{aligned} b^2 &\leq 3b+a-2 \leq 4b-2 \\ &\Leftrightarrow b^2-4b+2 \leq 0 \\ &\Leftrightarrow (b-(2+\sqrt{2}))(b-(2-\sqrt{2})) \leq 0. \end{aligned}$$

Esto nos diría que

$$(2-\sqrt{2}) \leq b \leq (2+\sqrt{2})$$

lo cual es falso, ya que $b \geq 4$.

Caso 2: Si $p < a+2b-2$ y $a \leq b-1$. Entonces $s = p$, ya que

$$s \geq \min\{p, a+2b-2\}.$$

Como $p \geq a+b+1$,

$$b(a+b-1) \geq (a+b+1)(b-1)$$

por (2). De aquí se sigue que $a \geq b-1$, por lo que $a = b-1$. Entonces, observando que $p \geq a+b+1 = 2b$ y p es un número primo, $p \geq 2b+1$. Aplicando (2), $s = p$, y $a = b-1$ se obtiene que

$$b(2b-2) \geq (2b+1)(b-1),$$

lo cual nos dice que

$$\begin{aligned} 2b^2-b-1 &\leq 2b^2-2b \\ &\Leftrightarrow -b-1 \leq -2b \\ &\Leftrightarrow b \leq 1, \end{aligned}$$

lo cual es falso ya que $b \geq 4$.

Caso 3: Si $p < a + 2b - 2$ y $a = b$. Entonces $s = p \geq 2b + 1$. Podemos suponer que $p \geq 2b + 3$, ya que el lema nos pide que $b \neq \frac{1}{2}(p-1)$. Por (2),

$$b(a + b - 1) \geq s(b - 1)$$

y como $a = b$, entonces

$$b(2b - 1) \geq (2b + 3)(b - 1)$$

$$\Leftrightarrow b + 2b^2 - 3 \leq 2b^2 - b$$

$$\Leftrightarrow b \leq \frac{3}{2},$$

lo cual es falso ya que $b \geq 4$. Con esto concluimos la demostración del lema. ■

Teorema 30 *(Vosper)* (A, B) *es un par crítico si y sólo si satisface una de las siguientes condiciones:*

(i) $|A| + |B| > p$,

(ii) $\min\{|A|, |B|\} = 1$,

(iii) $A = \overline{(\alpha - B)}$ *para alguna* $\alpha \in G$,

(iv) A *y* B *están en progresión aritmética con la misma diferencia.*

Demostración. Primero consideraremos la suficiencia ($\Leftarrow$) de las condiciones.

(i) Si $|A| + |B| > p$, tenemos que $|A| + |B| - 1 > p - 1$, $|A| + |B| - 1 \geq p$ y el mínimo es p. Por el teorema de Cauchy-Davenport sabemos que

$$|A + B| \geq \min\{p, |A| + |B| - 1\} = p$$

y como $A, B \subset G$ entonces $|A + B| = p$, por lo que (A, B) es un par crítico.

(ii) Si $\min\{|A|, |B|\} = 1$, supongamos que $|A| = 1$, entonces tenemos que

$$|A + B| = |a + B| = |B|,$$

ya que es sólo una translación del conjunto B. Pero $|B| < p$ entonces

$$\min\{p, |A| + |B| - 1\} = \min\{p, 1 + |B| - 1\} = \min\{p, |B|\} = |B|.$$

Por lo tanto,

$$|A + B| = \min\{p, |A| + |B| - 1\},$$

y así (A, B) es un par crítico.

(iii) Si $A = \overline{(\alpha - B)}$, entonces

$$A \cap (\alpha - B) = \varnothing$$

y por la proposición 25 tenemos que

$$(A + B) \cap \alpha = \varnothing.$$

Entonces $|A + B| \leq p - 1$, ya que $\alpha \notin A + B$. Pero

$$p - 1 = \min\{p, |A| + |B| - 1\},$$

esto se sigue de que $|A| = \left|\overline{B}\right| = p - |B|$ y $|A| + |B| = p$. Utilizando el teorema de Cauchy-Davenport

$$p - 1 = \min\{p, |A| + |B| - 1\} \leq |A + B| \leq p - 1$$

por lo que $|A + B| = p - 1$. Entonces (A, B) es un par crítico.

(iv) Si A y B estan en progresión aritmética con la misma diferencia, tenemos que $A = [0, a - 1]$ y $B = [0, b - 1]$, entonces

$$A + B = [0, a + b - 2].$$

Luego,

$$\begin{aligned} |A + B| &= |[0, a + b - 2]| = a + b - 1 \\ &= \min\{p, |A| + |B| - 1\}. \end{aligned}$$

Nuevamente, (A, B) es un par crítico.

Ahora consideremos la necesidad ($\Rightarrow$). Supondremos que (A, B) es un par crítico.

(a) Si $|A| + |B| > p$, tenemos el (i).

(b) Si $|A| + |B| = p$, entonces

$$|A + B| = |A| + |B| - 1 = p - 1$$

y así $(A + B) = \overline{\alpha}$ para alguna $\alpha \in G$. Se sigue que

$$(A + B) \cap \alpha = \varnothing,$$

y utilizando la proposición 25 $A \cap (\alpha - B) = \varnothing$. Entonces $A \subset \overline{(\alpha - B)}$. Pero

$$|A| = p - |B| = p - |(\alpha - B)| = \left|\overline{(\alpha - B)}\right|,$$

por lo que $A = \overline{(\alpha - B)}$ y tenemos (iii).

(c) Si $|A| + |B| < p$, la prueba la haremos por inducción sobre la suma $|A| + |B| = a + b$.

(i) Primer caso de la inducción es cuando $a + b = 6$ o sea $a = 3$, $b = 3$, pero por el Lema 24 sabemos que A y B estan en progresón aritmética con la misma diferencia.

(ii) Supongamos que A y B están en progresión aritmetica con la misma diferencia si $3 \leq a, b, a + b \leq r$

(iii) Demostraremos que A y B están en progresión aritmética con la misma diferencia si $3 \leq a, b, a + b = r + 1$. Si $a = b = \frac{1}{2}(p - 1)$, A y B están en progresión aritmética por el Colorario 28. Entonces si $a = b$ podemos suponer que $a \neq \frac{1}{2}(p - 1)$ También podemos suponer que $a \leq b$ y que $b \geq 4$. Por el Lema 29 existen $b_1, b_2 \in B$ tales que

$$(C + B) \cap (\overline{C + b_1}) \cap (\overline{C + b_2}) \neq \varnothing,$$

donde $C = A + B$, por lo que también existen $c \in C, \delta \in C + B$, $b_3 \in B$ tales que

$$\delta = c + b_3 \in (C + B) \cap (\overline{C + b_1}) \cap (\overline{C + b_2}) \neq \varnothing$$

Sea B_1 el conjunto de elementos $\omega \in B$ tal que $\delta - \omega \in C$, y $B_2 = \overline{B_1} \cap B$. Entonces $b_1, b_2 \in B_2$ y $b_3 \in B_1$, $2 \leq |B_2| \leq b-1$. Aseguramos que (A, B_2) es un par crítico; ya que si no fuera el caso se tendría que

$$|A + B_2| > a + |B_2| - 1.$$

Ahora $(\delta - B_2) \cap C = \varnothing$, ya que $B_2 = \overline{B_1}$. Tenemos que

$$(\delta - B_2) \cap (A + B_1) = \varnothing,$$

y así por la Proposición 26,

$$(\delta - B_1) \cap (A + B_2) = \varnothing. \tag{3}$$

Entonces, como $\delta - B_1 \subset C$, $A + B_2 \subset C$, se sigue que

$$|(\delta - B_1) \cup (A + B_2)| \leq |C|,$$

$$\begin{aligned} & |(\delta - B_1) \cup (A + B_2)| \\ = \; & |(\delta - B_1)| + |(A + B_2)| - |(\delta - B_1) \cap (A + B_2)| \leq |C|, \end{aligned}$$

y por (2) se obtiene que

$$|(\delta - B_1)| + |(A + B_2)| \leq |C|,$$

$$|(A + B_2)| \leq |C| - |(\delta - B_1)|,$$

$$|(A + B_2)| \leq |C| - |B_1|.$$

Entonces

$$|C| \geq |(A + B_2)| + |B_1| > a + |B_2| - 1 + |B_1| = a + b - 1$$

ya que supusimos que (A, B_2) no era un par crítico, lo cual contradice la hipótesis de que (A, B) es un par crítico. Concluímos que (A, B_2) es un par crítico. Si $|B_2| = 2$, A y B_2 son progresiones aritméticas con la misma diferencia por el Corolario 23 y si $|B_2| \geq 3$, A y B_2 son progresiones aritméticas con la misma diferencia por la hipótesis de inducción, observando que $a + |B_2| \leq r$, ya que $2 \leq |B_2| \leq b-1$. Entonces A es una progresión aritmética. Por el Lema 22 A y B son progresiones aritméticas con la misma diferencia. ■

3 Resultados

3.1 Cardinalidad de la suma en dependencia de la estructura del conjunto $2\hat{}A$

En esta sección analizamos los cuatro casos mencionados en la introducción.

Sea $A \subset Z_p$ con p un número primo. Podemos suponer que

$$A = [0, l-1] \cup \{a_1, a_2, ..., a_k\}$$

con $[0, l-1]$ $(l \geq 1)$ la progresión aritmética más grande de A y llamemos

$$B = \{a_1, a_2, ..., a_k\}.$$

El elemento más pequeño y más grande de $A \subseteq \mathbb{Z}_p$ serán el más pequeño y más grande de A vistos en $\mathbb{Z}$, respectivamente.

Proposición 31 *Sea $A \subset Z_p$ con $|A| = t = l + k \geq 4$ y tal que A no es progresión aritmética. Si $2\hat{}[0, l-1] \cup (B + [0, l-1])$ es un intervalo entonces*

$$|2\hat{}A \,| \geq 2\,|A| - 2.$$

Demostración. Como $2\hat{}A \ \cup (B + [0, l-1])$ es un intervalo podemos dividir la demostración en tres casos.

Caso 1: Si $2\hat{}[0, l-1] \cup (B + [0, l-1]) = [0, a_k + l - 1]$ entonces

$$2\hat{}A \ = [0, a_k + l - 1] \cup 2\hat{}B.$$

Definamos $A' = (A \backslash \{a_k\}) \cup \{l\}$ y $B' = B \backslash \{a_k\}$. Entonces tenemos que $2\hat{}[0, l-1] \cup (B' + [0, l-1])$ sigue siendo un intervalo y más aún,

$$2\hat{}[0, l] \cup (B' + [0, l])$$

es un intervalo. Luego

$$2\hat{}A\,' = [0, a_{k-1} + l] \cup 2\hat{}B' \subseteq 2\hat{}A\ = [0, a_k + l - 1] \cup 2\hat{}B$$

ya que $a_{k-1} \leq a_k - 1$. Entonces $a_{k-1} + l \leq a_k + l - 1$ y $2\hat{}B' \subseteq 2\hat{}B$. Por lo tanto $|2\hat{}A\,'| \leq |2\hat{}A|$. Continuando con este mismo proceso, parando antes de que A' sea un intervalo, tendríamos dos casos:

(a) Cuando $A' = [0, l + k - 2] \cup \{a_s\}$ con $s \in [1, k]$, $a_s \geq l + k$ y $|2\hat{}A'| \leq |2\hat{}A|$. Pero observemos entonces que

$$2\hat{}A' = [1, 2l + 2k - 5] \cup [a_s, a_s + l + k - 2]$$

por lo que $|2\hat{}A'| \geq 2l + 2k - 5 + \min\{a_s - l - k + 3, l + k - 1\}$. Si el mínimo fuera $a_s - l - k + 3$ entonces por la condición $a_s \geq l + k$ tendríamos que $a_s - l - k + 3 \geq 3$, por lo que

$$\begin{aligned} |2\hat{}A'| &\geq 2l + 2k - 5 + \min\{a_s - l - k + 2, l + k - 1\} \\ &\geq 2l + 2k - 5 + 3 = 2l + 2k - 2 \\ &= 2(l + k) - 2 = 2\,|A| - 2. \end{aligned}$$

Si el mínimo fuera $l + k - 1$, entonces por la condición $l + k \geq 4$ tenemos que $l + k - 1 \geq 3$, por lo que

$$\begin{aligned} |2\hat{}A'| &\geq 2l + 2k - 5 + \min\{a_s - l - k + 2, l + k - 1\} \\ &\geq 2l + 2k - 5 + l + k - 1 \\ &\geq 2(l + k) - 5 + 3 \geq 2\,|A| - 2. \end{aligned}$$

(b) Cuando $A' = [0, a_s] \cup [a_s + 2, l + k]$ con $s \in [1, k]$ y $|2\hat{}A'| \leq |2\hat{}A|$, entonces $2\hat{}A' = [1, 2l + 2k - 1]$ y $|2\hat{}A'| = 2l + 2k - 1$. Y como $|2\hat{}A'| \leq |2\hat{}A|$ entonces tendríamos que

$$|2\hat{}A| \geq 2l + 2k - 1 = 2(l + k) - 1 = 2\,|A| - 1 \geq 2\,|A| - 2.$$

En ambos casos, si utilizamos el hecho de que $|2\hat{}A| \geq |2\hat{}A'|$ podemos concluir que $|2\hat{}A| \geq 2\,|A| - 2$.

Caso 2: Si $2\hat{}[0, l-1] \cup (B + [0, l-1]) = [0, 2l-3] \cup [a_1, p-1]$. Este caso es análogo al Caso 1, solo tenemos que multiplicar a A por -1, sumarle $l-1$ y la prueba sería la misma.

Caso 3: Si $2\hat{}[0, l-1] \cup (B + [0, l-1]) = [0, a_s + l - 1] \cup [a_{s+1}, p-1]$. Lo primero que haremos será quitar los elementos $\{a_{s+1}, ..., a_k\}$ y transformar a A' en el conjunto

$$\begin{aligned} & [p - (k - s - 1 + 1), p-1] \cup [0, l-1] \cup \{a_1, ..., a_s\} \\ = \; & [p - k + s, p-1] \cup [0, l-1] \cup \{a_1, ..., a_s\}. \end{aligned}$$

O sea, lo que haremos será comprimir a A por un lado y con esto reducir la demostración al Caso 1. Si definimos a $A' = (A \backslash \{a_{s+1}\}) \cup \{p-1\}$ demostraremos $|2\hat{}A'| \leq |2\hat{}A|$. Sabemos que

$$2\hat{}A = [0, a_s + l - 1] \cup [a_{s+1}, p-1] \cup 2\hat{}B$$

y

$$2\hat{}A' = [0, a_s + l - 1] \cup [a_{s+2}, p-1] \cup 2\hat{}(B \backslash \{a_{s+1}\}).$$

Como

$$[0, a_{s+1} + l - 1] \cup [a_{s+2}, p-1] \subset [0, a_s + l - 1] \cup [a_{s+1}, p-1]$$

y

$$2\hat{}(B \backslash \{a_{s+1}\}) \subseteq 2\hat{}B,$$

entonces $2\hat{}A' \subseteq 2\hat{}A$, por lo que $|2\hat{}A'| \leq |2\hat{}A|$. Continuamos con este proceso hasta que lleguemos al caso en que

$$A' = [p - k + s, p-1] \cup [0, l-1] \cup \{a_1, ...a_s\}.$$

Ahora definamos

$$A'' = A' + k - s,$$

entonces tenemos que

$$A'' = [0, l + k - s - 1] \cup \{a'_1, ..., a'_s\}$$

con $a'_i = a_i + k - s$ con $i \in [1, s]$ y $|2\hat{}A''| \leq |2\hat{}A'|$. Aplicando el caso 1 a A'' tenemos que

$$|2\hat{}A''| \geq 2\,|A''| - 2$$

y como $|A| = |A'| = |A''|$ y $|2\hat{}A''| \leq |2\hat{}A'| \leq |2\hat{}A|$ por lo tanto

$$|2\hat{}A| \geq 2\,|A| - 2.$$

Con esto terminamos la demostración. ■

Proposición 32 *Sea $A \subset Z_p$ con $|A| = t = l + k \geq 4$ y tal que A no es progresión aritmética. Si $([0, l-1] + B) \cup (2\hat{}B)$ es un intervalo y $2\hat{}A$ no lo es, entonces*

$$|2\hat{}A| \geq 2\,|A| - 2.$$

Demostración. Supongamos que A es el conjunto más pequeño que cumple

$$|2\hat{}A| = 2|A| - 3$$

y A no es progresión aritmética. Entonces tenemos que

$$2\hat{}[0, l-1] \cap (([0, l-1] + B) \cup (2\hat{}B)) = \varnothing.$$

Definamos $A' = [0, l-2] \cup B$ y por el hecho de que $2\hat{}A$ no es progresión aritmética y por la suposición de que $|2\hat{}A| = 2\,|A| - 3$ tenemos que

$$|2\hat{}A'| = 2(|A| - 1) - 3.$$

Como A era el más pequeño, entonces A' es progresión aritmética, por lo tanto A es la unión de un intervalo y un conjunto con un solo elemento. Podemos ahora escribir

$$A = [0, l + k - 2] \cup \{a\}$$

con $a \in B$ y $a \geq l + k = |A| \geq 4$. Entonces

$$2\hat{}A = [1, l + k - 5] \cup [a, a + l + k - 2]$$

y

$$|2\hat{}A| = 2l + 2k - 5 + \min\{a - l - k + 5, a + l + k - 1\},$$

pero $\min\{a - l - k + 5, l + k - 1\} \geq 3$ por lo que

$$|2\hat{}A| \geq 2|A| - 2.$$

Con esto, concluímos la demostración. ■

Proposición 33 *Sea* $A = [0, l-1] \cup B \subset Z_p$ *con* $|A| = t = l + k \geq 4$ *y* A *no es progresión aritmética. Si* $2\hat{}[0, l-1] \cup 2\hat{}B$ *es un intervalo y* $2\hat{}A$ *no lo es, entonces*

$$|2\hat{}A| \geq 2\,|A| - 2.$$

Demostración. Sea $a_m \in B$ el elemento más pequeño tal que

$$(a_m + [0, l-1]) \cap (2\hat{}[0, l-1] \cup 2\hat{}B) = \varnothing$$

y $a_M \in B$ el elemento más grande tal que

$$(a_M + [0, l-1]) \cap (2\hat{}[0, l-1] \cup 2\hat{}B) = \varnothing.$$

Estos elementos existen ya que $2\hat{}A$ no es un intervalo. Se cumple que

$$(a_i \mathbin{\widehat{+}} B) \in (2\hat{}[0, l-1] \cup 2\hat{}B)$$

para $i = m, m+1, ..., M$ ya que $2\hat{}B \subseteq (2\hat{}[0, l-1] \cup 2\hat{}B)$. Aún más,

$$([a_m, a_M] \mathbin{\widehat{+}} B) \subseteq (2\hat{}[0, l-1] \cup 2\hat{}B)$$

ya que $a_m + a_1, a_M + a_k \in (2\hat{}[0, l-1] \cup 2\hat{}B)$. Ahora podemos cambiar el conjunto

$$\{a_m, a_m + 1, ..., a_M\}$$

por el conjunto $[a_m, a_m + M - m + 1]$. Si definimos

$$A' = [0, l-1] \cup \{a_1, ...a_{m-1}, a_M + 1, ..., a_k\} \cup [a_m, a_m + M - m + 1],$$

cumpliría que $|2\hat{}A'| \leq |2\hat{}A|$. Esto es porque

$$\begin{aligned} 2\hat{}A' \;=\; & 2\hat{}[0, l-1] \cup 2\hat{}\{a_1, ..., a_{m-1}, a_M + 1, ..., a_k\} \cup \\ & 2\hat{}[a_m, a_m + M - m + 1] \cup \\ & (\{a_1, ..., a_{m-1}, a_M + 1, ..., a_k\} + [0, l-1]) \cup \\ & ([a_m, a_m + M - m + 1] + [0, l-1]), \end{aligned}$$

$$\begin{aligned} & 2\hat{}[0, l-1] \cup 2\hat{}\{a_1, ..., a_{m-1}, a_M + 1, ..., a_k\} \cup \\ & 2\hat{}[a_m, a_m + M - m + 1] \cup \\ & (\{a_1, ..., a_{m-1}, a_M + 1, ..., a_k\} + [0, l-1]) \subseteq 2\hat{}A \end{aligned}$$

y

$$|([a_m, a_m + M - m + 1] + [0, l-1])| \leq |\{a_m, a_m + 1, ..., a_M\} + [0, l-1]|,$$

donde

$$\begin{aligned} ([a_m, a_m + M - m + 1] + [0, l-1]) \cap (2\hat{}[0, l-1] \cup 2\hat{}B) &= \varnothing, \\ (\{a_m, a_m + 1, ..., a_M\} + [0, l-1]) \cap (2\hat{}[0, l-1] \cup 2\hat{}B) &= \varnothing. \end{aligned}$$

Hagamos otra modificación a A', la cual consiste en que

$$[0, l-1] \cup \{a_1, ..., a_m - 1, a_M + 1, ..., a_k\}$$

lo volvamos un solo intervalo, el cual es

$$[p - (k - (M+1) + 1), l - 1 + m - 1] = [p - k + M, l + m - 2].$$

Observemos que

$$2\hat{}[p - k + M, l + m - 2] \subseteq (2\hat{}[0, l-1] \cup 2\hat{}B)$$

es un intervalo. Tenemos entonces que $2\hat{}A' \subseteq 2\hat{}A$ y como A' es la unión de dos intervalos, con un pequeño cálculo podemos observar que

$$|2\hat{}A'| \geq 2|A'| - 2,$$

por lo que

$$|2\hat{}A| \geq 2|A'| - 2 = 2|A| - 2,$$

lo cual queríamos demostrar. ■

Proposición 34 *Sea $A \subset Z_p$ con $|A| = t = l + k \geq 4$ y A no es progresión aritmética. Si*

$$2\hat{}[0, l-1] \cup (B + [0, l-1]) \cup 2\hat{}B = 2\hat{}A$$

es un intervalo, entonces

$$|2\hat{}A| \geq 2|A| - 2.$$

Demostración. Como $2^{\frown}A$ es un intervalo, entonces podemos suponer que es de la forma $[r, p-1] \cup [0, s]$. Como $(B + [0, l-1]) \subseteq 2^{\frown} A$ y a_i,$a_i + l - 1 \in (B + [0, l-1])$, entonces

$$\begin{aligned} a_i + l - 1 &\in [r, p-1] \cup [0, s], \\ a_i &\in [r, p-1] \cup [0, s] \end{aligned}$$

para toda $i = 1, ..., k$. Fijemos $M \in [1, k]$ tal que

$$a_i + l - 1 \in [0, s] \text{ si } i \leq M$$

y

$$a_j + l - 1 \in [r, p-1] \text{ si } M < j.$$

El caso en que $M = 1$ o $M = k$, se analiza al final de la prueba. Definamos el siguiente procedimiento que dividiremos en dos etapas:

Etapa 1: Sea $A' = (A \setminus \{a_{M+1}\}) \cup \{p-1\}$, entonces

$$2^{\frown}A' \subseteq [r, p-1] \cup [0, s]$$

ya que

$$\begin{aligned} a_w &< a_{M+1} < a_t, \\ a_{M+1} + l - 1 &\leq a_t + l - 1 + p - 1 = a_t + l - 2 \end{aligned}$$

y

$$0 < a_w + p - 1 = a_w - 1 \leq a_M$$

para toda $1 \leq w < M + 1 < t < k$. Este argumento nos lleva a que

$$|2^{\frown}A'| \leq |\, [r, p-1] \cup [0, s] \,| = |2^{\frown}A|.$$

Siguiendo el argumento anterior para cada a_j con $j > M + 1$, se llega a que

$$A' = (A \setminus \{a_{M+1}, a_{M+2}, ..., a_k\}) \cup [p - (k - M), p - 1]$$

y

$$2^{\frown}A' \subseteq [r, p-1] \cup [0, s].$$

Por lo que

$$|2^{\frown}A'| \leq |\, [r, p-1] \cup [0, s] \,| = |2^{\frown}A|.$$

Con el proceso anterior, el conjunto A' quedó transformado en

$$A' = [p-k+M, l-1] \cup \{a_1, ..., a_M\}.$$

La suma $\widehat{+}$ de A' es

$$\begin{aligned} 2\widehat{\ }A' &= 2\widehat{\ }[p-k+M, l-1] \cup (\{a_1, ..., a_M\} + [p-k+M, l-1]) \cup \\ & \quad 2\widehat{\ }\{a_1, ..., a_M\}, \end{aligned}$$

con la propiedad

$$2\widehat{\ }A' \subseteq [r, p-1] \cup [0, s].$$

Etapa 2: Intercambiando a_M por l , tenemos que

$$A' = [p-k+M, l] \cup \{a_1, ..., a_{M-1}\}$$

y

$$2\widehat{\ }A' \subseteq [r, p-1] \cup [0, s] = 2\widehat{\ }A$$

ya que

$$\begin{aligned} a_{M-1} + 1 &\leq a_M, \\ a_{M-1} + l &\leq a_M + l - 1 \leq s \end{aligned}$$

y

$$2l - 1 \leq a_1 + l - 1 < s.$$

Continuamos la etapa 2 y nos detenemos cuando A' tenga un solo hueco de longitud 1. Así tendríamos dos posibles casos con la propiedad

$$2\widehat{\ }A' \subseteq [r, p-1] \cup [0, s] = 2\widehat{\ }A.$$

Caso 1: Si

$$A' = [p-k+M, l+M-2] \cup \{a_w\}$$

con $w \in [1, M-1]$ y $a_w \geq k+l$, entonces

$$\begin{aligned} 2\widehat{\ }A' &= [p-2k+2M+1, 2l+2M-5] \cup \\ & \quad [a_w + p - k + M, a_w + l + M - 2]. \end{aligned}$$

(a) Si $a_w + p - k + M \in [p - 2k + 2M + 1, 2l + 2M - 5]$, entonces los intervalos de $2^\frown A'$ se intersectan. Como $l + M - 3 < a_w$, se tiene que

$$2l + 2M - 5 < a_w + l + M - 2.$$

Obtenemos con esto que

$$\begin{aligned} |2^\frown A'| &= (p-1) - (p - 2k + 2M + 1) + a_w + l + M - 1 \\ &= 2k - M + l + a_w - 3, \end{aligned}$$

y ya que $a_w > l$, se sigue que

$$\begin{aligned} M + 2k + l + a_w - 3 &> 2k + 2l - 3 + M \\ &= 2(k+l) - 3 + M \\ &= 2\,|A| - 3 + M, \end{aligned}$$

por lo que

$$|2^\frown A| \geq |2^\frown A'| > 2\,|A| - 3 + M.$$

(b) Si $a_w + p - k + M \notin [p - 2k + 2M + 1, 2l + 2M - 5]$, los intervalos de $2^\frown A'$ son disjuntos, por lo que la cardinalidad de $2^\frown A'$ sería aún mayor que en el caso (a), y con esto se obtiene el resultado deseado.

Caso 2: Si

$$A' = [p - k + M, l + c_1 - 1] \cup [l + c_1 + 1, l + c_1 + c_2]$$

donde $c_1 + c_2 = M$, entonces

$$\begin{aligned} 2^\frown A' &= 2^\frown [p - k + M, l + c_1 - 1] \cup 2^\frown [l + c_1 + 1, l + c_1 + c_2] \\ &\quad \cup ([p - k + M, l + c_1 - 1] + [l + c_1 + 1, l + c_1 + c_2]) \\ &= [2p - 2k + 2M + 1, 2l + 2c_1 + 2c_2 - 1], \end{aligned}$$

con lo que

$$\begin{aligned} |2^\frown A'| &= |[2k + 2M + 1, 2l + 2c_1 + 2c_2 - 1]| \\ &= ((2p-1) - (2p - 2k + 2M + 1) + 1) + \\ &\quad ((2l + 2c_1 + 2c_2 - 1) + 1) \\ &= 2k - 2M + 2l + 2c_1 + 2c_2 - 1 \\ &= 2(k+l) - 2M + 2(c_1 + c_2) - 1 \\ &= 2\,|A| - 2M + 2M - 1 = 2\,|A| - 1 > 2\,|A| - 3. \end{aligned}$$

Con esto, concluimos en ambos casos que

$$|2\hat{}A| \geq |2\hat{}A'| \geq 2\,|A| - 2.$$

Sólo nos falta considerar el caso en que la M no existe. Que la M no exista quiere decir que

$$a_i + l - 1 \in [0, s]$$

o

$$a_i + l - 1 \in [r, p-1]$$

para toda $i \in [1, k]$. Si $a_i + l - 1 \in [0, s]$, aplicamos la etapa 2 del procedimiento y obtenemos el resultado. Si $a_i + l - 1 \in [r, p-1]$, multiplicamos por -1 y le sumamos $l - 1$ al conjunto A, y con esto transformamos al caso $a_i + l - 1 \in [0, s]$, analizado anteriormente. ■

Finalizamos con un resultado muy sencillo que se deja al lector:

Proposición 35 *Sea $\varnothing \neq A \subseteq \mathbb{Z}_p$, donde $|A| \geq 2$. Si A es una progresión aritmética, entonces*

$$|2\hat{}A| = 2\,|A| - 3.$$

3.2 Problemas directos con sumas de residuos distintos

Sea $A = \bigcup_{l=0}^{k-1} [m_l, n_l - 1]$, donde $k \geq 2$, $m_0 = 0$, $m_l \geq n_{l-1} + 1$ $(l \in [1, k-1])$, $n_{k-1} \leq p - 1$. Definimos m y M como la longitud mínima y máxima de los intervalos de A, respectivamente. Los intervalos de $\overline{A}$ serán llamados los huecos de $A \subseteq \mathbb{Z}_p$. Para los siguientes lemas, k y j son el número de intervalos de A y B, respectivamente, y λ el número de huecos de B. Nosotros decimos que λ intervalos están igualmente distribuidos en A y B si el orden en el cual aparecen en la secuencia de intervalos coincide en ambos conjuntos A y B.

Usaremos los siguientes lemas (lemas 3.7, 3.16 y 3.18 de [6]):

Lema 36 *Si $m \geq 2$ y todos los huecos de B tienen longitud menor que o igual a $m - 1$ excepto uno de longitud mayor que o igual a M, entonces*

$$|A + B| \geq |A| + |B| + k + j - 3.$$

Lema 37 *Supóngase que A' y B' son conjuntos que satisfacen las condiciones del Lema 36 con $k-1$ y $j-1$ $(k,j \geq 2)$ intervalos respectivamente, y tal que $0,1 \notin A', 0,1 \notin B'$ y $|A'+B'| \leq p-4$. Sea $A = [0] \cup A'$ y $B = [0] \cup B'$. Entonces*

$$|A+B| \geq |A| + |B| + k + j - 4.$$

Lema 38 *Supóngase que A' y B' son conjuntos que satisfacen las condiciones del Lema 36 con $k-\lambda$ y $j-\lambda$ $(k,j \geq 2$ y $1 \leq \lambda \leq k,j)$ intervalos respectivamente, y tal que $|A'+B'| \leq p-4$. Sean los conjuntos A y B la unión de A' y B' respectivamente, con λ intervalos de longitud 1 igualmente distribuídos. Entonces*

$$|A+B| \geq |A| + |B| + k + j - 3 - \lambda.$$

Proposición 39 *Si $m \geq 2$ y $2\hat{}A$ es un intervalo entonces $2A$ es un intervalo.*

Demostración. Como $2\hat{}A$ es un intervalo, podemos transformar a A de tal forma que $2\hat{}A = [0,l]$. Sabemos que

$$2A = 2\hat{}A \cup \{2a | a \in A\},$$

y supongamos que $2A$ no es un intervalo, o sea, existe $a \in A$ tal que $2a > l+1$. Como $m \geq 2$, entonces existe un intervalo de longitud mayor que dos tal que

$$a \in [m_i, n_i - 1]$$

y

$$2a > l + 1.$$

De aquí se desprenden tres posibles casos:

Caso 1: Si $a \neq m_i, n_i - 1$ entonces $|[m_i, n_i - 1]| \geq 3$. Como $a \in [m_i, n_i - 1]$ y $|[m_i, n_i - 1]| \geq 3$ entonces existen $m_{i_1}, m_{i_2} \in [m_i, n_i - 1]$ tales que $2a = m_{i_1} + m_{i_2}$ con $m_{i_1} \neq m_{i_2}$ o sea que $2a \in 2\hat{}A$, lo cual es una contradicción.

Antes de ver el segundo caso, es importante recordar que $m_i + 1 \in [m_i, n_i - 1]$ ya que $|[m_i, n_i - 1]| \geq 2$ para toda $i = 0, 1, ..., k-1$. También veamos que $m_i + m_i + 1 = 2m_i + 1 \in 2\hat{}A$, lo que implica que $2m_i + 1 \in [0,l]$.

Caso 2: Si $a = m_i$ entonces $2a = 2m_i$ y como $2m_i + 1$ forma parte del intervalo $[0, l]$ entonces lo haría también $2a$, lo cual es una contradicción.

Caso 3: Si $a = n_i - 1$ entonces por un argumento similar al Caso 2 llegamos a una contradicción. Por lo tanto $2A$ es también un intervalo. ■

Proposición 40 *Sea* $2\hat{}A$ *un intervalo y* $m \geq 2$, *entonces*

$$|2\hat{}A| \geq 2\,|A| + 2k - 5.$$

Demostración. Por la proposición anterior y el hecho de que $2\hat{}A$ es un intervalo podemos suponer que $2A$ es un intervalo.

Como $2A$ es un intervalo, entonces por el Lema 36, se cumple que

$$|2A| \geq 2\,|A| + 2k - 3.$$

Como $2\hat{}A$ y $2A$ son intervalos y $2\hat{}A \subseteq 2A$, entonces podemos suponer que $2\hat{}A = [s, t]$ y $2A = [0, l]$ con $0 \leq s \leq t \leq l$.

Detengámonos un momento para demostrar que $|2\hat{}A| + 2 \geq |2A|$ usando el hecho de que $2\hat{}A$ y $2A$ son intervalos. Tenemos cuatro casos:

Caso 1: Si $s = 0$, $l = t$ entonces $2\hat{}A = 2A$, por lo que se cumple que $|2\hat{}A| + 2 \geq |2A|$.

Caso 2: Si $s \neq 0$ y $t \neq l$ entonces estamos diciendo que $0, l \notin 2\hat{}A$, por lo que

$$0 = 2a$$

con $a \in [m_{r_1}, n_{r_1} - 1]$ y

$$l = 2b$$

con $b \in [m_{r_2}, n_{r_2} - 1]$, entonces $a = m_{r_1}$ y $b = n_{r_2} - 1$. Ahora

$$2m_{r_1} = 0$$

y

$$2n_{r_2} - 2 = l,$$

lo cual implica que

$$\begin{aligned} 2m_{r_1} + 1 &= 1 \\ 2n_{r_2} - 3 &= l - 1, \end{aligned}$$

pero como

$$\begin{aligned} |[m_{r_1}, n_{r_1} - 1]| &\geq 2 \\ |[m_{r_2}, n_{r_2} - 1]| &\geq 2, \end{aligned}$$

entonces

$$\begin{aligned} m_{r_1} + 1 &\in |[m_{r_1}, n_{r_1} - 1]| \\ n_{r_2} - 2 &\in |[m_{r_2}, n_{r_2} - 1]|, \end{aligned}$$

por lo que

$$\begin{aligned} 2m_{r_1} + 1 &\in 2\hat{}A, \\ 2n_{r_2} - 3 &\in 2\hat{}A, \\ 1, l - 1 &\in 2\hat{}A, \\ |2\hat{}A| + 2 &= |2A| \end{aligned}$$

y por último se cumple que

$$|2\hat{}A| + 2 \geq |2A|.$$

Caso 3: Si $s \neq 0$ y $l = t$, entonces decimos que $l \in 2\hat{}A$ y $s \notin 2\hat{}A$. Se sigue que

$$0 = 2a$$

con $a \in [m_{r_1}, n_{r_1} - 1]$, por lo que existe

$$m_{r_0} \in [m_{r_1}, n_{r_1} - 1],$$

tal que

$$2m_{r_0} = 0,$$

lo cual implica que

$$2m_{r_0} + 1 = 1$$

y como $|[m_{r_1}, n_{r_1} - 1]| \geq 2$ se puede tomar

$$m_{r_1} + 1 \in [m_{r_1}, n_{r_1} - 1],$$

por lo tanto

$$\begin{aligned} 2m_{r_1}+1 &\in 2\hat{}A, \\ 1 &\in 2\hat{}A, \\ |2\hat{}A|+1 &= |2A| \end{aligned}$$

y

$$|2\hat{}A|+2 \geq |2A|\,,$$

que es lo que se quería demostrar.

Caso 4: Si $s=0, l \neq t$ se aplica un argumento similar al Caso 3.

Por lo tanto $|2\hat{}A|+2 \geq |2A|$.

Regresando a la demostración original, nosotros sabíamos que $|2A| \geq 2\,|A|+2k-3$ y por lo que se demostró, se cumple que

$$|2\hat{}A|+2 \geq |2A| \geq 2\,|A|+2k-3$$

por lo tanto

$$|2\hat{}A| \geq 2\,|A|+2k-5$$

con k el número de intervalos de A. ■

Observación 41 *Si en el Lema 40, $k=1$, esto es, A es una progresión aritmética, entonces $|2\hat{}A| \geq 2\,|A|-3$, y en virtud de la Proposición 35, se tiene la igualdad en este caso.*

Proposición 42 *Supongamos que $2\hat{}A'$ es un intervalo y A' está formado por $k-1$ intervalos con $k \geq 3$, $m \geq 2$ y $0,1 \notin A'$, $|2\hat{}A| \leq p-6$. Sea $A=[0]\cup A'$ entonces*

$$|2\hat{}A| \geq 2\,|A|+2k-7.$$

Demostración. Sabemos que

1) $2A'$ es un intervalo ya que $2\hat{}A'$ lo es,

2) $|2\hat{}A'|+2 \geq |2A'|$ lo cual se demostró en el lema anterior,

3) $p-6+2 \geq |2\hat{}A'|+2 \geq 2\,|A'| \Longrightarrow p-4 \geq 2\,|A'|$.

Estas son las condiciones del Lema 37, entonces

$$|2A| \geq 2\,|A|+2k-4. \tag{4}$$

Por otro lado sabemos que

$$2\hat{}A = A' \cup 2\hat{}A',$$

ya que $A = [0] \cup A'$ y $2A = 2\hat{}A' \cup A' \cup \{0, 2m_1, 2n_{k-1} - 2\}$. Por tanto

$$|2\hat{}A| + 3 \geq |2A|.$$

La igualdad se cumple en el caso que

$$\{0, 2m_1, 2n_{k-1} - 2\} \in 2\hat{}A,$$

y utilizando (4) tenemos que

$$\begin{aligned} |2\hat{}A| + 3 &\geq 2\,|A| + 2k - 4, \\ |2\hat{}A| &\geq 2\,|A| + 2k - 7 \end{aligned}$$

con k el número de intervalos de A lo cual queríamos demostrar. ■

Comentarios Finales

En la sección 2 algunas demostraciones se reescribieron en lenguaje más actualizado, lo cual permite tener una lectura más sencilla.

Las demostraciones en la sección 3.1 son fáciles de verificar siguiendo un ejemplo. La idea en estas demostraciones es la de reducir los conjuntos sin aumentar su cardinalidad. Con la técnica utilizada para resolver los casos en la sección 3.1 se podría demostrar, con las mismas hipótesis, cuales son los conjuntos que cumplen $2\hat{}A = 2\,|A| - 2$, ya que todos los conjuntos pueden ser reducidos a conjuntos que son la unión de dos intervalos o la unión de un intervalo un elemento. Solo hay que tener mucho cuidado con la cardinalidad de A. En el caso que no se incluye no se puede utilizar esta técnica, ya que no tenemos manera de mantener un orden y por lo que llega un momento en que se pierde el control de las cardinalidades. Se logró hacer para este caso una demostración que no se pudo simplificar, por lo que no se incluyó en la tesis.

En el estudio del problema original se fueron dando algunos resultados del artículo de B. Llano [6] de forma casi directa. La idea en esto fue considerar que si $2\ A$ es un intervalo, entonces también lo es $2\hat{}A$. Con esto, los resultados son casi inmediatos.

Bibliografía

1. M. B. Nathanson. *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Graduate Texts in Math. 165 (Springer-Verlag, 1996).

2. A. G. Vosper. 'The critical pairs of sumset of a group of prime order', *J. London Math. Soc.* 31 (1956) 200-205.

3. H. Davenport. 'On the addition of residue classes', *J. London Math. Soc.* 10 (1935) 30-32.

4. N. Alon, M. B. Nathanson and I. Ruzsa. 'Adding distinct congruence classes modulo a prime', *American Math. Monthly* 102 (1995) 250-255.

5. N. Alon, M. B. Nathanson and I. Ruzsa. 'The polynomial method and restricted sums of congruence classes', *J. Number Theory* 56, No.29, (1996) 404-417.

6. B. Llano. 'Small sumset in a prime order group', *Bol. Soc. Mat. Mexicana* (3) Vol. 9 (2003) 61-78.

7. Hui-Qin Cao and Zhi-Wei Sun. 'On sums of distinct representatives', *Acta Arithmetica* LXXXVII.2 (1998) 159-169.

8. G. A. Freiman. *Foundations of a Structural Theory of Set Addition*, Translations of Mathematical Monographs. 37 (American Mathematical Society, 1973).

9. A. Cauchy. 'Recherche sur les nombres', *J. Ecole Polytechn.* 9 (1813) 99-106.

10. S Chowla, H. B. Mann, and E. G. Straus. 'Some applications of the Cauchy-Davenport theorem', *Det Kongelige Norske Videnskabers Selskabs* 32(13) (1959) 74-80.

11. J. Steing. 'On G. A. Freiman's theorems concernig the sum of two finite sets of integers'. In Conference on the Structure Theory of Set Addition, pages 173-186. CIRM, Marseille (1993).

12. I. Chowla. 'A theorem on the addition of residue classes: Application to the number $\Gamma(k)$ in Waring's problem', *Proc. Indian Acad. Sci.*, Section A, 1:242-243 (1935).

13. Y. O. Hamidoune and Ö. J. Rödseth. On bases for σ-finite groups. Math. Scand. 78 (1996) 246-254.

14. O. Serra and G. Zémor. On a generalization of a theorem by Vosper, INTEGERS: Electronic Journal of Combinatorial Number Theory, #A10 (2000) http://www.integers-ejcnt.org/vol0.html.

15. U.-W. Rickert. *Über eine Vermutung in der additiven Zahlentheorie.* PhD thesis, Technical University of Braunschweig (1976).

16. R. Mansfields. 'How many slopes in a polygon?', *Israel J. Math.*, 39:265-270 (1981).

17. Ö. J. Rödseth. Sums of distinct residues mod p, *Acta Arith.*, 65:181-184 (1993).

18. L. Pyber. 'On the Erdős-Heilbronn conjecture' (comunicación personal).

19. G. A. Freiman, L. Low, and J. Pitman. 'The proof of Paul Erdős' conjecture of the addition of different residue classes modulo prime number'. In Structure Theory of Set Addition, 7-11, 99-108, Marseille (1993). CIRM.

20. J. A. Dias de Silva and Y. O. Hamidoune. 'Cyclic spaces for Grassmann derivatives and additive theory', *Bull. London Math. Soc.*, 26:140-146 (1994).

21. M. B. Nathanson. 'Inverse theorems for sumset sums', *Trans. Am. Math. Soc.*, 347:1409-1418 (1995).

22. P. Erdös. 'On the addition of residue classes (mod p)', In Proceedings of the 1963 Number Theory Conference at the University of Colorado, pp. 16-17, Boulder, 1963. University of Colorado.

23. P. Erdös and H. Heilbronn. 'On the addition of residue classes (mod p)', *Acta Arith.* 9:149-159 (1964).

24. P. Erdös and R. L. Graham. *Old and New Problems and Results in Combinatorial Number Theory.* L'Enseignement Matématique, Geneva, 1980.

25. Y. Bilu. 'Structure of sets with small sumsets', Mathematiques Stochastiques, Univ. Bordeaux 2, Preprint 94-10, 1994.

26. H. B. Mann. *Addition Theorems.* Wiley-Interscience, New York, 1965.

27. S. S. Pillai. 'Generalization of a theorem of Davenport on the addition of residue classes', *Proc. Indian Acad. Sci. Ser. A*, 6:179-180 (1938).

28. J. M. Pollard. 'A generalization of a theorem of Cauchy and Davenport', *J. London Math. Soc.,* 8:460-462 (1974).

29. I. Z. Ruzsa. 'Arithmetic progressions and the number of sums', *Periodica Math. Hungar.,* 25:105-111 (1992).

30. I. Z. Ruzsa. 'Sums of finite sets', In D. Chudnovsky, G. V. Chudnovsky and M. B. Nathanson, editors, *Number Theory: New York Seminar.* Springer-Verlag, New York, 1996.

31. G. Károlyi (comunicación personal).