CONJUNTOS DE SIDON LIBRES DE SUMAS

SANTIAGO DAVID CARLOSAMA
JESUS FABIAN MUÑOZ POMEO

UNIVERSIDAD DEL CAUCA
FACULTAD DE CIENCIAS NATURALES, EXACTAS Y DE LA EDUCACIÓN
PROGRAMA DE MATEMÁTICAS
POPAYÁN
2015

CONJUNTOS DE SIDON LIBRES DE SUMAS

SANTIAGO DAVID CARLOSAMA
JESUS FABIAN MUÑOZ POMEO

Trabajo de grado presentado en la modalidad trabajo de investigación como requisito parcial para optar el título de Matemático

Director: Dr. Carlos Alberto Trujillo Solarte

UNIVERSIDAD DEL CAUCA
FACULTAD DE CIENCIAS NATURALES, EXACTAS Y DE LA EDUCACIÓN
PROGRAMA DE MATEMÁTICAS
POPAYÁN
2015

Nota de Aceptación

_____

_____

_____

_____

Director _____

Dr. Carlos Alberto Trujillo Solarte

Evaluador _____

Dr. Jhon Jairo Bravo Grijalba

Evaluador Yadira Caicedo Bravo

Mg. Nidia Yadira Caicedo Bravo

Popayán Cauca, 4 de Agosto de 2015

Agradecimientos

Agradecemos a Dios por protegernos durante todo el camino y darnos fuerzas para superar obstáculos y dificultades a lo largo de toda la vida.

A nuestra familia fuente de apoyo constante e incondicional en toda nuestra vida y más aún en nuestros duros años de carrera profesional y en especial queremos expresar nuestros más grandes agradecimientos a las mujeres más importantes de nuestra vida, nuestras madres por cuidarnos, amarnos, alimentarnos y porque sin su ayuda hubiera sido imposible culminar nuestra carrera.

Por otra parte, nos gustaría agradecer sinceramente a nuestro Director de Tesis, Dr. Carlos Alberto Trujillo Solarte, su esfuerzo, dedicación, sus conocimientos, sus orientaciones, su manera de trabajar, su paciencia y su motivación han sido fundamentales para nuestra formación como profesionales.

Índice general

Introducción **IV**

1. Preliminares **1**

2. Conjuntos Libres de Sumas módulo N **7**
2.1. Conceptos fundamentales 7
2.2. Resultados Importantes 8

3. Construcciones clásicas de conjuntos de Sidon módulo N **15**

4. Conjuntos de Sidon Libres de Sumas Módulo N **19**
4.1. Conceptos fundamentales 19
4.2. Resultados Importantes 20

Conclusiones **30**

Apéndice **32**

A. Algoritmos **32**

B. Un Resultado General **40**

Bibliografía **42**

Introducción

La Teoría de Números es un área de las Matemáticas especializada en la busqueda de propiedades y relaciones entre números y conjuntos de números enteros. Uno de los problemas favoritos de Paul Erdös, y que mejor ha descrito su gusto por la aritmética combinatoria, es el de los conjuntos de Sidon.

A principios de los años 30 del siglo XX, Simon Sidon, le preguntó a Erdös sobre conjuntos de enteros positivos con todas las sumas de dos elementos distintos; especificamente pregunta: ¿Cuál es el mayor tamaño de un conjunto de enteros no negativos, todos ellos menores que una cantidad dada, en el cual todas las sumas de dos elementos del conjunto son distintas?. A partir de entonces el mismo Erdös le asigna el nombre de Conjuntos Sidon a este tipo de conjuntos.

Otro problema que surge en el mismo contexto aditivo de la Teoría de Números es el relacionado con la siguiente pregunta: ¿Cuál es el mayor tamaño de un conjunto de números enteros no negativos que tiene la propiedad que todas las sumas de dos de sus elementos sean distintas a los elementos del conjunto original?. A este tipo de conjuntos se los llama conjuntos libres de sumas.

En este trabajo nos interesamos en la intersección de los dos tipos de conjuntos frente a la pregunta: ¿Cuál es el mayor tamaño de un conjunto de números enteros no negativos que cumple con los dos conceptos anteriores?

Para responder esta pregunta recurrimos a las construcciones conocidas de conjuntos de Sidon modulares para investigar sobre el máximo cardinal de un subconjunto libre de sumas en cada una de ellas.

En el primer capítulo de este trabajo presentamos los conceptos y la notación que se utilizan en el desarrollo del mismo.

En el segundo capítulo consideramos de manera independiente los conjuntos libres de sumas módulo N y las funciones extremas relacionadas con ellos.

En el tercer capítulo presentamos una breve descripción de las tres construcciones clásicas de conjuntos de Sidon modulares.

Finalmente en el capítulo cuatro buscamos respuesta a la pregunta relacionada con el máximo cardinal de un conjunto libre de sumas contenido en cada uno de los tres tipos de conjuntos de Sidon modulares. Es en este capítulo donde se encuentran los resultados mas importantes de nuestro trabajo, que podriamos resumirlos así:

Para toda potencia prima q, el máximo número de elementos que puede tener un conjunto de Sidon y libre de sumas módulo q^2+q+1 es q.

Para toda potencia prima q impar, el máximo número de elementos que puede tener un conjunto de Sidon y libre de sumas módulo q^2-1 es mayor o igual que $\frac{q-1}{2}$.

Para toda primo impar p, el máximo número de elementos que puede tener un conjunto de Sidon y libre de sumas módulo p^2-p es mayor o igual que $\frac{p-1}{2}$.

Destacamos nuestras presentaciones como ponentes en los siguientes congresos especializados:

- ALTENCOA6-2014, Universidad de Nariño, 11-15 de Agosto de 2014, San Juan de Pasto-Nariño.

- V Encuentro Nacional de Matemáticas y Estadística, Universidad del Tolima, 6-8 de Mayo de 2015, Ibague-Tolima.

- XX Congreso Colombiano de Matemáticas, Universidad Nacional Sede Manizales, 21 al 24 de Julio de 2015, Manizales-Caldas.

Capítulo 1

Preliminares

Sean $(G, +)$ un grupo conmutativo, notado aditivamente, y A un subconjunto de G. Se definen el conjunto suma y el conjunto diferencia de A, notados $A+A$ y $A - A$, respectivamente, como:

$$A + A := \{a + b : a, b \in A\};$$

$$A - A := \{a - b : a, b \in A\}.$$

Definición 1.1 ***(Conjunto Libre de Sumas).*** *A es un conjunto libre de sumas si la ecuación $x + y = z$ con $x, y, z \in A$ no tiene solución en A.*

Esto es equivalente a decir que la suma de dos elementos de A nunca está en A, es decir:

$$(A + A) \cap A = \emptyset.$$

Observación 1.1 *Un conjunto A es libre de diferencias si cumple que todas las restas de dos elementos de A nunca estan en A, es decir*

$$(A - A) \cap A = \emptyset.$$

A continuación se presentan algunos ejemplos de conjuntos libres de sumas.

Ejemplo 1.1 *En* $(\mathbb{Z}, +)$ *el conjunto de los números impares es libre de sumas.*

$+$	1	3	5	7	9	$11....$
	2	4	6	8	10	12 ....
		6	8	10	12	$14....$
			10	12	14	$16....$
				14	16	$18....$
					18	$20....$
						$22....$

Ejemplo 1.2 *En* $(\mathbb{Z}, +)$ *el conjunto de los cuadrados no es libre de sumas, ya que si tomamos 9,16 y 25 esto nos da una solución a la ecuación* $x+y=z$.

1	4	9	16	25	$36....$
2	5	10	17	26	$37....$
	8	13	20	29	$40....$
		18	25	34	$45....$
			32	41	$52....$
				50	$61....$
					$72....$

Ejemplo 1.3 *En* $(\mathbb{Z}, +)$ *el conjunto de las* n*-ésimas potencias positivas, con* $n \geq 3$*, es libre de sumas. (Último Teorema de Fermat).*

Ejemplo 1.4 *En* $(\mathbb{Z}_{12}, +)$ *el conjunto* $A = \{1, 3, 5, 7, 9, 11\}$ *es libre de sumas.*

$+$(mód 12)	1	3	5	7	9	11
	2	4	6	8	10	0
		6	8	10	0	2
			10	0	2	4
				2	4	6
					6	8
						10

Notación 1.1 *Sea* A *un conjunto finito cualquiera, en adelante se utiliza* $|A|$ *para denotar la cantidad de elementos que tiene el conjunto* A*, es decir su cardinal.*

Definición 1.2 ***(Conjunto de Sidon).*** *Sea $A \subseteq G$, A es un conjunto de Sidon en G si todas las sumas de dos elementos de A son distintas (salvo conmutatividad). Es decir, si para todo $a, b, c, d \in A$*

$$a + b = c + d \Rightarrow \{a, b\} = \{c, d\}.$$

Esto es también equivalente a requerir que para todo $x \in G$ se tiene que:

$$|A \cap (x - A)| \leq 1,$$

donde

$$x - A = \{x - a : a \in A\}.$$

En efecto,

$$\begin{aligned} z \in A \cap (x - A) &\Leftrightarrow z \in A \wedge z \in (x - A) \\ &\Leftrightarrow z = a \wedge z = x - b, \text{ para algunos } a, b \in A. \\ &\Leftrightarrow x = a + b, \text{ para algunos } a, b \in A. \end{aligned}$$

En el caso finito, $A = \{a_1, a_2, \ldots, a_k\}$ es un conjunto de Sidon si y sólo si

$$|A + A| = \binom{k+1}{2}.$$

Nota 1.1 *$A = \{a_1, a_2, \ldots, a_k\}$ es conjunto Sidon si y sólo si*

$$\begin{aligned} |A \ominus A| &= 2\binom{k}{2}, \\ &= k^2 - k, \end{aligned}$$

donde

$$A \ominus A = \left\{a - a' : a, a' \in A, a \neq a'\right\}.$$

Es decir, A es conjunto de Sidon si y sólo si todas las diferencias de dos elementos diferentes de A son distintas. Esto equivale a requerir que

$$a - b = c - d \Rightarrow a = c \text{ y } b = d,$$

para todo $a, b, c, d \in A, a \neq b, c \neq d$.

A continuación se presentan algunos ejemplos de conjuntos de Sidon.

Ejemplo 1.5 *En* $(\mathbb{Z}, +)$ *el conjunto de las potencias de 2 es un conjunto de Sidon.*

$+$	2	4	8	16	$32....$
	4	6	10	18	$34....$
	6	8	12	20	$36....$
	10	12	16	24	$40....$
	18	20	24	32	$48....$
	34	36	40	48	$64....$

Observación 1.2 *En* $(\mathbb{Z}^+, \cdot)$ *el conjunto de los primos es un conjunto de Sidon.*

$\bullet$	2	3	5	7	$11....$
	4	6	10	14	$22....$
	6	9	15	21	$33....$
	10	15	25	35	$55....$
	14	21	35	49	$77....$
	22	33	55	77	$121....$

Note que $(\mathbb{Z}^+, \cdot)$ *no es un grupo, así ser grupo no es condición indispensble para definir un conjunto de Sidon.*

Ejemplo 1.6 *En* $(\mathbb{Z}, +)$ *el conjunto de los cuadrados no es un conjunto de Sidon, porque* $1 + 64 = 16 + 49$.

1	16	25	36	49	$64....$
2	17	26	37	50	$65...$
17	32	41	52	65	$80...$
26	41	50	61	74	$89...$
37	52	61	72	85	$100...$
50	65	74	85	98	$118...$
65	80	89	100	118	$128\ ...$

Note que si C denota el conjunto de los cuadrados perfectos

$$|C \cap (65 - C)| = 4$$

Lema 1.1 *Un conjunto A es libre de sumas si y sólo si es libre de diferencias, esto es*

$$(A+A)\cap A=\emptyset \Leftrightarrow (A-A)\cap A=\emptyset$$

Demostración.

($\Rightarrow$) Supongamos que existe $x\in(A-A)\cap A$

$$\Rightarrow x\in(A-A) \ \wedge \ x\in A$$

$$\Rightarrow x=a-b \ \wedge \ x\in A, \ para\ algunos\ a,b\in A$$

$$\Rightarrow x+b=a \ \ para\ algunos\ a,b\in A$$

lo cual es una contradición, ya que A es libre de sumas.

($\Leftarrow$) Supongamos que existe $x\in(A+A)\cap A$

$$\Rightarrow x\in(A+A) \ \wedge \ x\in A$$

$$\Rightarrow x=a+b \ \wedge \ x\in A, para\ algunos\ a,b\in A$$

$$\Rightarrow x-b=a \ \ para\ algunos\ a,b\in A$$

lo cual es una contradición, ya que A es libre de diferencias.

■

Corolario 1.1 *Si $0\in G$ y $A\subseteq G$ libre de sumas, entonces $0\notin A$.*

Corolario 1.2 *Todo subconjunto de un conjunto libre de sumas es libre de sumas y de restas.*

El siguiente ejemplo muestra un conjunto A libre de restas.

Ejemplo 1.7 *Sea* $A = \{7, 11, 17, 19, 21, 23\}$

-	*7*	*11*	*17*	*19*	*21*	*23*
	0	*4*	*10*	*12*	*14*	*16*
		0	*6*	*8*	*10*	*12*
			0	*2*	*4*	*6*
				0	*2*	*4*
					0	*2*
						0

El siguiente conjunto es simultaneamente un conjunto de Sidon y un conjunto libre de sumas módulo 57.

Ejemplo 1.8 *Sea* $A = \{1, 4, 12, 14, 30, 37, 52\}$

+(mód 57)	*1*	*4*	*12*	*14*	*30*	*37*	*52*
	2	*5*	*13*	*15*	*31*	*38*	*53*
		8	*16*	*18*	*34*	*41*	*56*
			24	*26*	*42*	*49*	*7*
				28	*44*	*51*	*9*
					3	*10*	*25*
						17	*32*
							47

Capítulo 2

Conjuntos Libres de Sumas módulo N

En este capítulo presentamos las funciones extremas asociadas a los conjuntos libres de sumas módulo N y algunos resultados asociados a estas funciones, los cuales nos permitirán construir conjuntos libres de sumas modulares.

2.1. Conceptos fundamentales

En este trabajo nos dedicamos al caso en el cual el grupo ambiente son los enteros módulo N:

$$\mathbb{Z}_N := \{0, 1, 2, \ldots N-1\},$$

con las operaciones usuales módulo N.

Mediante $LS(\mathbb{Z}_N)$ denotamos la familia de los conjuntos libres de sumas módulo N, esto es:

$$LS(\mathbb{Z}_N) := \{A \subseteq \mathbb{Z}_N : A \textit{ es un conjunto libre de sumas}\}.$$

Definición 2.1 ***(Función maximal).*** *La función maximal para los conjuntos libres de sumas esta definida por:*

$$LS(N) := \max\{|A| : A \in LS(\mathbb{Z}_N)\}.$$

Así, $LS(N)$ es el máximo número de elementos que puede tener un conjunto libre de sumas módulo N.

Definición 2.2 ***(Función mínima)***. *La función mínima de los conjuntos libre de sumas esta definida por:*

$$GL(k) := \min\{N \in \mathbb{N} : existe\ A \in LS(\mathbb{Z}_N), |A| = k\}.$$

Así, $GL(k)$ es el mínimo módulo para el cual existe un conjunto libre se sumas módulo N con k elementos.

2.2. Resultados Importantes

Teorema 2.1 *Para todo $N \in \mathbb{N}$, el máximo número de elementos que tiene un conjunto libre de sumas módulo $2N$ es igual a N; esto es*

$$LS(2N) = N.$$

Demostración.

Primero probamos que $LS(2N) \geq N$, presentando una construcción general.

El conjunto de residuos impares módulo $2N$:

$$A = \{1, 3, 5, \ldots 2N-1\} \subseteq \mathbb{Z}_{2N};$$

claramente es libre de sumas módulo $2N$ y tiene exactamente $|A| = N$ elementos; luego

$$LS(2N) \geq N. \tag{2.1}$$

Ahora, probemos que $LS(2N) \leq N$.

Si suponemos que $LS(2N) > N$, entonces existe un conjunto $A \subseteq \mathbb{Z}_{2N}$ libre de sumas, y tal que

$$|A| > N;$$

así, también se tiene que

$$|A + A| > N.$$

Por tanto

$$\begin{aligned} |(A+A)\cup A| &= |A+A|+|A|-|(A+A)\cap A| \\ &> N+N-0 = 2N. \end{aligned}$$

Lo cual es una contradicción, ya que no puede haber un conjunto con más de $2N$ elementos en $\mathbb{Z}_{2N}$;

en consecuencia

$$LS\,(2N) \leq N. \tag{2.2}$$

De (2.1) y (2.2) se tiene que

$$LS\,(2N) = N.$$

■

El siguiente ejemplo ilustra un conjunto A que cumple con las condiciones del teorema anterior.

Ejemplo 2.1 *Sea* $A = \{1,3,5,7,9,11,13,15,17\} \subseteq \mathbb{Z}_{18}$

+(mód 18)	*1*	*3*	*5*	*7*	*9*	*11*	*13*	*15*	*17*
	2	*4*	*6*	*8*	*10*	*12*	*14*	*16*	*0*
		6	*8*	*10*	*12*	*14*	*16*	*0*	*2*
			10	*12*	*14*	*16*	*0*	*2*	*4*
				14	*16*	*0*	*2*	*4*	*6*
					0	*2*	*4*	*6*	*8*
						4	*6*	*8*	*10*
							8	*10*	*12*
								12	*14*
									16

Corolario 2.1 *Sea* $k \in \mathbb{N}$. *El mínimo módulo para el cual existe un conjunto libre de sumas con* k *elementos es* $2k$, *esto es*

$$GL\,(k) = 2k.$$

Demostración.

Se puede ver fácilmente del Teorema 2.1 que

$$GL\,(k) \leq 2k. \tag{2.3}$$

Ahora supongamos que $GL\,(k) < 2k$. Esto es, existe $N \in \mathbb{N}$ y $A \in LS\,(\mathbb{Z}_N)$ tal que

$$|A| = k \text{ y } k < N < 2k;$$

luego se tiene que:

$$|A + A| \geq k,$$

Por tanto

$$\begin{aligned} |(A + A) \cup A| &= |A + A| + |A| - |(A + A) \cap A| \\ &\geq k + k - 0 = 2k > N. \end{aligned}$$

Esto es una contradicción, ya que no puede haber un conjunto con más de N elementos en $\mathbb{Z}_N$. En consecuencia

$$GL\,(k) \geq 2k. \tag{2.4}$$

De (2.3) y (2.4) se tiene que

$$GL\,(k) = 2k.$$

■

Notación 2.1 *Sea N un número real cualquiera, en adelante se utiliza $\lfloor A \rfloor$ para denotar la parte entera de N.*

Teorema 2.2 *Para todo $N \in \mathbb{N}$, el máximo número de elementos de un conjunto libre de sumas módulo N es mayor o igual que $\left\lfloor \frac{N}{3} \right\rfloor$, esto es:*

$$LS\,(N) \geq \left\lfloor \frac{N}{3} \right\rfloor, \text{ para todo } N \in \mathbb{N}.$$

Demostración.

Por el teorema anterior el resultado es válido para todo N par. Supongamos que N es impar y consideremos sus posibles restos módulo 6.

Caso 1: Si $N \equiv 1\,(mód\ 6)$, es decir $N = 7, 13, 19, 25, 31, \ldots$;
Sea $k = \left\lfloor \frac{N}{6} \right\rfloor = \frac{N-1}{6}$; así $N = 6k + 1$.

Caso 2: Si $N \equiv 3\,(mód\ 6)$, es decir $N = 3, 9, 15, 21, 27, \ldots$;
Sea $k = \left\lfloor \frac{N}{6} \right\rfloor = \frac{N-3}{6}$; así $N = 6k + 3$.

Caso 3: Si $N \equiv 5\,(mód\ 6)$, es decir $N = 5, 11, 17, 23, 29, \ldots$;
Sea $k = \left\lfloor \frac{N}{6} \right\rfloor = \frac{N-5}{6}$; así $N = 6k + 5$.

En todos los casos, sean:

$$A_1 = \{2i - 1 : i = 1, 2, 3, .., k\},$$
$$A_2 = \{N - (2i - 1) : i = 1, 2, ..., k\};$$

probemos que $A = A_1 \cup A_2$ es libre de sumas, esto es

$$(A + A) \cap A = \emptyset.$$

Observemos que:

$$A + A = (A_1 + A_1) \cup (A_1 + A_2) \cup (A_2 + A_2),$$

además:

$$\begin{aligned}(A + A) \cap A &= [(A_1 + A_1) \cup (A_1 + A_2) \cup (A_2 + A_2)] \cap [A_1 \cup A_2] \\ &= [(A_1 + A_1) \cap A_1] \cup [(A_1 + A_1) \cap A_2] \cup [(A_1 + A_2) \cap A_1] \\ &\cup [(A_1 + A_2) \cap A_2] \cup [(A_2 + A_2) \cap A_1] \cup [(A_2 + A_2) \cap A_2]\end{aligned}$$

Ahora probemos que

$$\begin{aligned}(A_1 + A_1) \cap A_1 &= \emptyset, & (A_1 + A_1) \cap A_2 &= \emptyset, \\ (A_1 + A_2) \cap A_1 &= \emptyset, & (A_1 + A_2) \cap A_2 &= \emptyset, \\ (A_2 + A_2) \cap A_1 &= \emptyset, & (A_2 + A_2) \cap A_2 &= \emptyset.\end{aligned}$$

- Si $(A_1 + A_1) \cap A_1 \neq \emptyset$, entonces existen $i, j, l \in \{1, 2, 3, ..., k\}$, tal que:

$$(2i - 1) + (2j - 1) \equiv 2l - 1 \, (mód \ N)$$

luego N divide a $2i + 2j - 2l - 1$, que no es posible por que

$$0 < |2i + 2j - 2l - 1| < N.$$

Por lo tanto $(A_1 + A_1) \cap A_1 = \emptyset$.

- Si $(A_1 + A_1) \cap A_2 \neq \emptyset$, entonces existen $i, j, l \in \{1, 2, 3, ..., k\}$, tal que:

$$(2i - 1) + (2j - 1) \equiv N - (2l - 1) \, (mód \ N)$$

luego N divide a $2i + 2j + 2l - 3$, que no es posible por que

$$0 < |2i + 2j + 2l - 3| < N.$$

Por lo tanto $(A_1 + A_1) \cap A_2 = \emptyset$.

- Si $(A_1 + A_2) \cap A_1 \neq \emptyset$, entonces existen $i, j, l \in \{1, 2, 3, ..., k\}$, tal que:

$$(2i - 1) + (N - (2l - 1)) \equiv 2j - 1 \, (mód \ N)$$

luego N divide a $2i - 2j - 2l + 1$, que no es posible por que

$$0 < |2i - 2j - 2l + 1| < N.$$

Por lo tanto $(A_1 + A_2) \cap A_1 = \emptyset$.

- Si $(A_1 + A_2) \cap A_2 \neq \emptyset$, entonces existen $i, j, l \in \{1, 2, 3, ..., k\}$, tal que:

$$(2i - 1) + (N - (2j - 1)) \equiv N - 2l + 1 \, (mód \ N)$$

luego N divide a $2i - 2j + 2l - 1$, que no es posible por que

$$0 < |2i - 2j + 2l - 1| < N.$$

Por lo tanto $(A_1 + A_2) \cap A_2 = \emptyset$.

- Si $(A_2 + A_2) \cap A_1 \neq \emptyset$, entonces existen $i, j, l \in \{1, 2, 3, ..., k\}$, tal que:

$$(N - (2i - 1)) + (N - (2j - 1)) \equiv 2l - 1 \, (m\acute{o}d \ N)$$

luego N divide a $-2i - 2j - 2l + 3$, que no es posible por que

$$0 < |-2i - 2j - 2l + 3| < N.$$

Por lo tanto $(A_2 + A_2) \cap A_1 = \emptyset$.

- Si $(A_2 + A_2) \cap A_2 \neq \emptyset$, entonces existen $i, j, l \in \{1, 2, 3, ..., k\}$, tal que:

$$(N - (2i - 1)) + (N - (2j - 1)) \equiv N - 2l + 1 \, (m\acute{o}d \ N)$$

luego N divide a $-2i - 2j + 2l + 1$, que no es posible por que

$$0 < |-2i - 2j + 2l + 1| < N.$$

Por lo tanto $(A_2 + A_2) \cap A_2 = \emptyset$.

■

El siguiente ejemplo ilustra un conjunto libre de sumas que se ha construido a partir del Teorema 2.2.

Ejemplo 2.2 *Sea N=25, entonces* $\left\lfloor \frac{N}{3} \right\rfloor = 8$, *se toman los primeros cuatro impares* $\{1, 3, 5, 7\}$ *y los otros cuatro son el complemento* $\{24, 22, 20, 18\}$.

1	*3*	*5*	*7*	*18*	*20*	*22*	*24*
2	*4*	*6*	*8*	*19*	*21*	*23*	*0*
	6	*8*	*10*	*21*	*23*	*0*	*2*
		10	*12*	*23*	*0*	*2*	*4*
			14	*0*	*2*	*4*	*6*
				11	*13*	*15*	*17*
					15	*17*	*19*
						19	*21*
							23

Capítulo 3

Construcciones clásicas de conjuntos de Sidon módulo N

En este capítulo presentamos las tres construcciones clásicas de conjuntos de Sidon módulo N maximales para módulos de la forma q^2+q+1, q^2-1, p^2-p, donde p es un primo y q una potencia prima (*ver* [1], [2] *y* [5]).

Teorema 3.1 ***(Construcción de Bose)*** *Sean q una potencia prima y θ un elemento primitivo del campo finito con q^2 elementos, $\mathbb{F}_{q^2}$. El conjunto*

$$B = \{a \in \{1, 2, \dots q^2-1\} : \theta^a - \theta \in \mathbb{F}_q\}$$

es un conjunto de Sidon módulo q^2-1 con q elementos.

Demostración.

Es claro que B tiene q elementos, porque

$$\theta^a - \theta = \theta^b - \theta, \text{ con } a, b \in \{1, 2, 3, \dots q^2-1\},$$

es válido, si y solo si, $a = b$.

Probemos que B es un conjunto de Sidon módulo q^2-1. Supongamos que para $a, b, c, d \in B$ tenemos:

$$a + b \equiv c + d \, (mód \; q^2-1).$$

Entonces, en $\mathbb{F}_{q^2}$,

$$\begin{aligned} \theta^{a+b} &= \theta^{c+d}, \\ \theta^a\theta^b &= \theta^c\theta^d. \end{aligned} \tag{3.1}$$

Por definición de B, existen $\alpha, \beta, \gamma, \delta \in \mathbb{F}_q$ tales que

$$\theta^a = \theta + \alpha,\ \theta^b = \theta + \beta,\ \theta^c = \theta + \gamma,\ \theta^d = \theta + \delta.$$

Reemplazando en (3.1):

$$(\theta + \alpha)(\theta + \beta) = (\theta + \gamma)(\theta + \delta),$$

de donde

$$\theta^2 + (\alpha + \beta)\theta + \alpha\beta = \theta^2 + (\gamma + \delta)\theta + \gamma\delta,$$

y así

$$(\alpha + \beta - (\gamma + \delta))\theta + (\alpha\beta - \gamma\delta) = 0.$$

Note que

$$\alpha + \beta - (\gamma + \delta), \alpha\beta - \gamma\delta \in \mathbb{F}_q.$$

Como θ es de grado 2 sobre $\mathbb{F}_q$, esto es posible solo si

$$\alpha + \beta = \gamma + \delta \text{ y } \alpha\beta = \gamma\delta;$$

se sigue que:

$$\{\alpha, \beta\} = \{\gamma, \delta\},$$

luego

$$\left\{\theta^a, \theta^b\right\} = \left\{\theta^c, \theta^d\right\},$$

y de aquí,

$$\{a, b\} = \{c, d\}.$$

■

Observación 3.1 *Notemos que*

$$B = \{\log_\theta (\theta + x) : x \in \mathbb{F}_q\},$$

donde $\log_\theta$ *es la función logaritmo discreto definida como*

$$\begin{aligned} \log_\theta : \mathbb{F}_{q^2}^* = \langle\theta\rangle &\longrightarrow \mathbb{Z}_{q^2-1} \\ \theta^k &\longrightarrow k. \end{aligned}$$

El conjunto B *en esta forma, se utiliza en el capítulo 4 para la construcción de conjuntos de Sidon libres de sumas.*

Teorema 3.2 ***(Construcción de Ruzsa)*** *Sean* p *un primo y* α *una raiz prímitiva módulo* p*. Si para cada* i *con* $1 \leq i \leq p-1$*,* X_i *es la única solución módulo* $p(p-1)$ *del sistema de dos congruencias*

$$\begin{cases} X_i & \equiv i \,(mód\ p-1)\,, \\ X_i & \equiv \alpha^i \,(mód\ p)\,, \end{cases}$$

entonces el conjunto

$$R := \{X_1, X_2, ..., X_{p-1}\},$$

es un conjunto de Sidon módulo $p\,(p-1)$*, con* $p-1$ *elementos.*

Demostración.

Por la primera congruencia del sistema, claramente el conjunto R tiene $p-1$ elementos. Probemos ahora que R es un conjunto de Sidon módulo $p\,(p-1)$. Supongamos que existen i, j, k, l con $1 \leq i, j, k, l \leq p-1$ tales que

$$X_i + X_j \equiv X_k + X_l \,(mód\ p\,(p-1)).$$

Entonces

$$\begin{aligned} &X_i + X_j \equiv X_k + X_l \,(mód\ p-1) \quad \text{y} \\ &X_i + X_j \equiv X_k + X_l \,(mód\ p)\,. \end{aligned}$$

Luego, por definición,

$$i + j \equiv k + l \,(mód\ p-1) \quad \text{y} \tag{3.2}$$
$$\alpha^i + \alpha^j \equiv \alpha^k + \alpha^l \,(mód\ p)\,. \tag{3.3}$$

Ahora, de (3.2):

$$\alpha^{i+j} \equiv \alpha^{k+l} \,(mód\ p) \Leftrightarrow \alpha^i \alpha^j \equiv \alpha^k \alpha^l \,(mód\ p)\,. \tag{3.4}$$

De (3.3) *y* (3.4)

$$\alpha^i + \alpha^j \equiv \alpha^k + \alpha^l \,(mód\ p),$$
$$\alpha^i \alpha^j \equiv \alpha^k \alpha^l \,(mód\ p).$$

Como $\mathbb{Z}_p$ es un campo, tenemos que:

$$\{\alpha^i, \alpha^j\} = \{\alpha^k, \alpha^l\},$$

luego

$$\{i, j\} = \{k, j\},$$

y así

$$\{X_i, X_j\} = \{X_k, X_l\}.$$

■

Teorema 3.3 ***(Construcción de Singer)*** *Sean q una potencia prima y θ un elemento primitivo del campo finito con q^3 elementos, $\mathbb{F}_{q^3}$. El conjunto*

$$S = \{0\} \cup \{\log_\theta (\theta + x) \,(mód\ q^2 + q + 1) : x \in \mathbb{F}_q\},$$

es un conjunto de Sidon módulo $q^2 + q + 1$ con $q + 1$ elementos.

Nota 3.1 *La prueba de este resultado se hace en el capítulo siguiente.*

Observación 3.2 *En este caso la función logaritmo discreto se define como*

$$\log_\theta : \mathbb{F}_{q^3}^* = \langle\theta\rangle \longrightarrow \mathbb{Z}_{q^3-1}$$
$$\theta^k \longrightarrow k.$$

Esta función se utiliza en el capítulo 4 para la demostración del Teorema 4.1.

Capítulo 4

Conjuntos de Sidon Libres de Sumas Módulo N

4.1. Conceptos fundamentales

Mediante $S(\mathbb{Z}_N)$ denotamos la familia de los conjuntos de Sidon módulo N, es decir en el grupo $(\mathbb{Z}_N, +)$:

$$S(\mathbb{Z}_N) := \{A \subseteq \mathbb{Z}_N : A \text{ es conjunto de Sidon}\}.$$

Definición 4.1 ***(Función maximal)*** *La función maximal para los conjuntos de Sidon libres de sumas módulo N es:*

$$SLS(N) := \max\{|A| : A \in S(\mathbb{Z}_N) \cap LS(\mathbb{Z}_N)\}.$$

Así $SLS(N)$ es el máximo número de elementos que puede tener un conjunto de Sidon libre de sumas en $(\mathbb{Z}_N, +)$.

Definición 4.2 ***(Función mínima)*** *La función mínima para los conjuntos de Sidon libres de sumas módulo N esta dada por:*

$$GSL(k) := \min\{N \in \mathbb{N} : \text{existe } A \in S(\mathbb{Z}_N) \cap LS(\mathbb{Z}_N), |A| = k\}.$$

Así $GSL(k)$ es el mínimo módulo para el cual existe un conjunto de Sidon libre de sumas módulo N con k elementos.

4.2. Resultados Importantes

Como se observará en la prueba del siguiente teorema, la construcción de conjuntos de Sidon debida a Singer del capítulo anterior, sin el cero, nos proporciona un conjunto de Sidon libre de sumas maximal.

Teorema 4.1 *Sea q una potencia prima, entonces*

$$SLS\left(q^2+q+1\right)=q.$$

Demostración.

Sean q una potencia prima y θ un elemento primitivo de $\mathbb{F}_{q^3}$. Sabemos que θ es un generador del grupo multiplicativo de $\mathbb{F}_{q^3}$, el cual mediante el logaritmo discreto es isomorfo a $\mathbb{Z}_{q^3-1}$, es decir:

$$\langle\theta\rangle=\mathbb{F}_{q^3}^{*}\cong\mathbb{Z}_{q^3-1};$$

mientras que

$$\left\langle\theta^{q^2+q+1}\right\rangle=\mathbb{F}_{q}^{*}\cong\mathbb{Z}_{q-1}.$$

Sea S el siguiente conjunto:

$$S=:\left\{log_{\theta}\left(\theta+x\right)\left(m\acute{o}d\ q^2+q+1\right):x\in\mathbb{F}_q\right\}.$$

Probemos que S es un conjunto de Sidon. En efecto, supongamos que existen $a_i\in S$, $i=1,2,3,4$; tales que

$$a_1+a_2\equiv a_3+a_4\left(m\acute{o}d\ q^2+q+1\right).$$

Por definición de S existen $x_i\in\mathbb{F}_q$, $i=1,2,3,4$, tales que:

$$a_i\equiv\log_{\theta}\left(\theta+x_i\right)\left(m\acute{o}d\ q^2+q+1\right).$$

Luego

$$\log_{\theta}\left(\theta+x_1\right)+\log_{\theta}\left(\theta+x_2\right)\equiv\log_{\theta}\left(\theta+x_3\right)+\log_{\theta}\left(\theta+x_4\right)\left(m\acute{o}d\ q^2+q+1\right),$$

de donde

$$\log_{\theta}\left(\left(\theta+x_1\right)\left(\theta+x_2\right)\right)\equiv\log_{\theta}\left(\left(\theta+x_3\right)\left(\theta+x_4\right)\right)\left(m\acute{o}d\ q^2+q+1\right).$$

De ahí que

$$\log_\theta\left(\tfrac{(\theta+x_1)(\theta+x_2)}{(\theta+x_3)(\theta+x_4)}\right) \equiv 0\,(m\acute{o}d\ q^2+q+1),$$

esto es, existe $t \in \mathbb{Z}$ tal que

$$\log_\theta\left(\tfrac{(\theta+x_1)(\theta+x_2)}{(\theta+x_3)(\theta+x_4)}\right) = t\,(q^2+q+1);$$

entonces en $\mathbb{F}_{q^3}$;

$$\tfrac{(\theta+x_1)(\theta+x_2)}{(\theta+x_3)(\theta+x_4)} = \theta^{t\left(q^2+q+1\right)},$$

y así:

$$Y = \tfrac{(\theta+x_1)(\theta+x_2)}{(\theta+x_3)(\theta+x_4)} \in \mathbb{F}_q^*.$$

De donde,

$$\theta^2 + (x_1+x_2)\,\theta + x_1x_2 = Y\,(\theta^2 + (x_3+x_4)\,\theta + x_3x_4),$$

$$(1-Y)\,\theta^2 + (x_1+x_2-Yx_3-Yx_4)\,\theta + (x_1x_2 - Yx_3x_4) = 0.$$

Como los coeficiente de la ecuación anterior estan en $\mathbb{F}_q$ y el grado de θ sobre $\mathbb{F}_q$ es 3, se tiene que:

$$Y = 1,\ x_1+x_2 = x_3+x_4,\ x_1x_2 = x_3x_4,$$

entonces

$$\{x_1, x_2\} = \{x_3, x_4\},$$

así

$$\{\theta+x_1, \theta+x_2\} = \{\theta+x_3, \theta+x_4\},$$

luego

$$\{\log_\theta(\theta+x_1), \log_\theta(\theta+x_2)\} = \{\log_\theta(\theta+x_3), \log_\theta(\theta+x_4)\},$$

en consecuencia

$$\{a_1, a_2\} = \{a_3, a_4\}.$$

Por lo tanto S es un conjunto de Sidon.

Ahora, probemos que S es un conjunto libre de sumas, es decir que:

$$(S+S)\cap S=\emptyset.$$

Supongamos que existen $a_1,a_2,a_3\in S$, tal que

$$a_1+a_2\equiv a_3\,(m\acute{o}d\ q^2+q+1).$$

Entonces, por definición de S, existen $x_1,x_2,x_3\in\mathbb{F}_q$ tales que:

$$\log_\theta(\theta+x_1)+\log_\theta(\theta+x_2)\equiv\log_\theta(\theta+x_3)\,(m\acute{o}d\ q^2+q+1),$$

$$\log_\theta\left(\tfrac{(\theta+x_1)(\theta+x_2)}{(\theta+x_3)}\right)\equiv 0\,(m\acute{o}d\ q^2+q+1).$$

Luego, para algún $t\in\mathbb{Z}$, se tiene que:

$$\log_\theta\left(\tfrac{(\theta+x_1)(\theta+x_2)}{(\theta+x_3)}\right)=t\,(q^2+q+1),$$

y, como antes:

$$\tfrac{(\theta+x_1)(\theta+x_2)}{(\theta+x_3)}=\theta^{t\left(q^2+q+1\right)}.$$

Sea

$$Z=\tfrac{(\theta+x_1)(\theta+x_2)}{(\theta+x_3)}\in\mathbb{F}_q^*;$$

y así:

$$\theta^2+(x_1+x_2)\,\theta+x_1x_2=Z\,(\theta+x_3),$$

$$\theta^2+(x_1+x_2-Z)\,\theta+x_1x_2-Zx_3=0;$$

así θ satisface un polinomio mónico no nulo de grado 2 sobre $\mathbb{F}_q$, que no es posible. Por lo tanto S es un conjunto libre de sumas.

Probemos que S tiene q elementos. Si existen $x_1,x_2\in\mathbb{F}_q$, tales que

$$\log_\theta(\theta+x_1)\equiv\log_\theta(\theta+x_2)\,(m\acute{o}d\ q^2+q+1),$$

entonces

$$\log_\theta\left(\tfrac{(\theta+x_1)}{(\theta+x_2)}\right)\equiv 0\,(m\acute{o}d\ q^2+q+1),$$

entonces para algún entero t

$$log_\theta\left(\tfrac{(\theta+x_1)}{(\theta+x_2)}\right)=t\,(q^2+q+1),$$

luego,

$$\tfrac{(\theta+x_1)}{(\theta+x_2)} = \theta^{t\left(q^2+q+1\right)},$$

Sea

$$W = \tfrac{(\theta+x_1)}{(\theta+x_2)} \in \mathbb{F}_q^*;$$

así

$$(1-W)\,\theta + x_1 - Wx_2 = 0.$$

Como el grado de θ sobre $\mathbb{F}_q$ es 3, se tiene que:

$$W = 1,\ x_1 = x_2.$$

■

Observación 4.1 *Para la prueba del Teorema 3.3, notemos que*

$$S_0 = S \cup \{0\},$$

y

$$S_0 + S_0 = \{0\} \cup S \cup (S+S).$$

Como S es un conjunto de Sidon libre de sumas módulo q^2+q+1 con q elementos, de esta última ecuación se sigue que S_0 es un conjunto de Sidon módulo q^2+q+1 con $q+1$ elementos.

El siguiente ejemplo muestra un conjunto de Sidon libre de sumas módulo 57 con 7 elementos que se ha construido a partir del Teorema 4.1.

Ejemplo 4.1 *Sea $q = 7, q^2+q+1 = 57, S = \{1,4,12,14,30,37,52\}$*

1	*4*	*12*	*14*	*30*	*37*	*52*
2	*5*	*13*	*15*	*31*	*38*	*53*
	8	*16*	*18*	*34*	*41*	*56*
		24	*26*	*42*	*49*	*7*
			28	*54*	*4*	*9*
				3	*10*	*25*
					17	*32*
						47

En el ejemplo que se muestra a continuación se observa que al añadir el elemento 0 al conjunto S del ejemplo anterior no se tiene un conjunto libre de sumas, aunque si un conjunto de Sidon tipo Singer.

Ejemplo 4.2

0	*1*	*4*	*12*	*14*	*30*	*37*	*52*
0	*1*	*4*	*12*	*14*	*30*	*37*	*52*
	2	*5*	*13*	*15*	*31*	*38*	*53*
		8	*16*	*18*	*34*	*41*	*56*
			24	*26*	*42*	*49*	*7*
				28	*54*	*4*	*9*
					3	*10*	*25*
						17	*32*
							47

El siguiente teorema muestra que los conjuntos de Sidon obtenidos con la construcción de Ruzsa no se comportan tan bien como en el caso de los conjuntos de Sidon obtenidos con la construcción de Singer.

Teorema 4.2 *Sean p un primo impar y R el conjunto de Sidon módulo $p\,(p-1)$ obtenido en la construcción de Ruzsa. Entonces*

$$|(R+R)\cap R| = \frac{p-1}{2}.$$

Demostración.

Supongamos que existen $X_i, X_j, X_k \in R$, $1 \leq i, j, k \leq p-1$ tales que

$$X_i + X_j \equiv X_k \,(mód\ p\,(p-1)).$$

Por definición de R, si α es una raíz primitiva móduo p, tenemos que:

$$\begin{aligned} \alpha^i + \alpha^j &\equiv \alpha^k \,(mód\ p)\,, \qquad \text{y} \\ i + j &\equiv k \,(mód\ p-1)\,. \end{aligned} \tag{4.1}$$

$$\alpha^i \alpha^j = \alpha^{i+j} \equiv \alpha^k \,(mód\ p)\,. \tag{4.2}$$

Por lo tanto por (4.1) y (4.2)

$$\alpha^i + \alpha^j \equiv \alpha^i \alpha^j \ (m\acute{o}d\ p).$$

Sean $a = \alpha^i$ y $b = \alpha^j$, así entonces contar los elementos en $(R + R) \cap R$ es lo mismo que contar las soluciones de

$$a + b = ab, \ en\ \mathbb{F}_p^*. \tag{4.3}$$

Es fácil ver que $a, b \neq 1$. También que la única solución de (4.3) con $a = b$ es $(a, b) = (2, 2)$.
Ahora el número de soluciones para (4.3) es el número de valores de a con $3 \leq a \leq p - 1$, esto es $p - 3$, además (a, b) y (b, a) se cuentan como una sola solución cuando $a \neq b$, entonces hay $\dfrac{p-3}{2}$ soluciones distintas con $a \neq b$.
En total tenemos:

$$\frac{p-3}{2} + 1 = \frac{p-1}{2} \text{ soluciones.}$$

Luego

$$|(R + R) \cap R| = \frac{p-1}{2}.$$

Esto nos dice que para obtener un conjunto de Sidon libre de sumas módulo $p\,(p-1)$ hay que quitar los elementos de la intersección $(R + R) \cap R$ que son $\dfrac{p-1}{2}$ elementos.

■

A continución se muestra un ejemplo de un conjunto de Sidon tipo Ruzsa en el cual se resaltan los elementos que son comunes entre el conjunto de Sidon tipo Ruzsa y su conjunto suma asociado.

Ejemplo 4.3 *Sea p=13,* $\alpha = 2$ *y módulo* 156

10	*16*	*57*	*59*	*90*	*99*	*115*	*134*	*144*	*145*	*149*	*152*
20	*26*	*67*	*69*	*100*	*109*	*125*	*144*	*154*	*155*	*3*	*6*
	32	*73*	*75*	*106*	*115*	*131*	*150*	*4*	*5*	*9*	*12*
		114	*116*	*147*	*0*	*16*	*35*	*45*	*46*	*50*	*53*
			118	*149*	*2*	*18*	*37*	*47*	*48*	*52*	*55*
				24	*33*	*49*	*68*	*78*	*79*	*83*	*86*
					42	*58*	*77*	*87*	*88*	*92*	*95*
						74	*93*	*103*	*104*	*108*	*111*
							112	*122*	*123*	*127*	*130*
								132	*133*	*137*	*140*
									134	*138*	*141*
										142	*145*
											148

Observación 4.2 *Así necesitamos quitar los números (resaltados) en el ejemplo 4.3 para obtener un conjunto de Sidon libre de sumas, lo cual se puede observar en el ejemplo que se muestra a continuación.*

Ejemplo 4.4 .

10	*57*	*59*	*90*	*99*	*152*
20	*67*	*69*	*100*	*109*	*6*
	114	*116*	*147*	*0*	*53*
		118	*149*	*2*	*55*
			24	*33*	*86*
				42	*95*
					148

Recordemos que se quiere encontrar un conjunto de Sidon libre de sumas con el mayor número de elementos posible. El Teorema 4.2 nos dice que se deben quitar la mitad de los elementos del conjunto de Sidon tipo Ruzsa para obtener un conjunto de Sidon libre de sumas, pero al hacer algunas pruebas con algunos conjuntos de Sidon tipo Ruzsa se observa que no es necesario quitar tantos elementos, lo que da paso a la siguiente conjetura.

Conjetura 1.
Sea p un número primo y R un conjunto de Sidon tipo Ruzsa con $p-1$ elementos, entonces para obtener un conjunto de Sidon libre de sumas es suficiente quitar $\left\lfloor \frac{p}{4} \right\rfloor$ elementos.

El siguiente ejemplo toma el conjunto de Sidon tipo Ruzsa del ejemplo 4.3 para observar que se cumple la conjetura 1.

Ejemplo 4.5 *Sea p=13, entonces* $\left\lfloor \frac{p}{4} \right\rfloor$ *=3. Se quitarán los elementos* $\{115, 134, 149\}$ *y se obtiene un conjunto Sidon libre de sumas.*

10	*16*	*57*	*59*	*90*	*99*	*144*	*145*	*152*
20	*26*	*67*	*69*	*100*	*109*	*154*	*155*	*6*
	32	*73*	*75*	*106*	*115*	*4*	*5*	*12*
		114	*116*	*147*	*0*	*45*	*46*	*53*
			118	*149*	*2*	*47*	*48*	*55*
				24	*33*	*78*	*79*	*86*
					42	*87*	*88*	*95*
						132	*133*	*140*
							134	*141*
								148

Para el caso de la construcción del conjunto de Sidon tipo Bose, tenemos:

Problema 1. Sea B un conjunto tipo Bose y q una potencia prima, entonces

$$|(B+B) \cap B| = \frac{q+1}{2}.$$

A continución se muestran en los ejemplos 4.6 y 4.8 conjuntos de Sidon tipo Bose en los cuales se resaltan los elementos que son comunes entre el conjunto de Sidon tipo Bose y su conjunto suma asociado.

Ejemplo 4.6 *Sea* $q = 11$ *y módulo* 120.

1	*22*	*45*	*56*	*62*	*71*	*75*	*76*	*78*	*103*	*113*
2	*23*	*46*	*57*	*63*	*72*	*76*	*77*	*79*	*104*	*114*
	44	*67*	*78*	*84*	*93*	*97*	*98*	*100*	*5*	*15*
		90	*101*	*107*	*116*	*0*	*1*	*3*	*28*	*38*
			112	*118*	*7*	*11*	*12*	*14*	*39*	*49*
				4	*13*	*17*	*18*	*20*	*45*	*55*
					22	*26*	*27*	*29*	*54*	*64*
						30	*31*	*33*	*58*	*68*
							32	*34*	*59*	*69*
								36	*61*	*71*
									86	*96*
										106

Observación 4.3 *Así necesitamos quitar los números (resaltados) para obtener un conjunto de Sidon libre de sumas, lo cual se observa en el siguiente ejemplo.*

Ejemplo 4.7 .

56	*62*	*75*	*103*	*113*
112	*118*	*11*	*39*	*49*
	4	*17*	*45*	*55*
		30	*58*	*68*
			86	*96*
				106

Ejemplo 4.8 *Sea* $q = 9$ *y módulo* 80.

1	*22*	*36*	*37*	*44*	*49*	*53*	*55*	*78*
2	*23*	*37*	*38*	*45*	*50*	*54*	*56*	*79*
	44	*58*	*59*	*66*	*71*	*75*	*77*	*20*
		72	*73*	*0*	*5*	*9*	*11*	*34*
			74	*1*	*6*	*10*	*12*	*35*
				8	*13*	*17*	*19*	*42*
					18	*22*	*24*	*47*
						26	*28*	*51*
							30	*53*
								76

Observación 4.4 *Así necesitamos quitar los números (subrayados) para obtener un conjunto de Sidon libre de sumas, lo cual se observa en el siguiente ejemplo.*

Ejemplo 4.9 .

36	*49*	*55*	*78*
72	*5*	*11*	*34*
	18	*24*	*47*
		30	*53*
			76

Aunque el Problema 1 nos dice que hay que quitar $\frac{q+1}{2}$ elementos, para obtener un conjunto de Sidon libre de sumas, observando algunos conjuntos de Sidon tipo Bose se observa que no es necesario retirar tantos elementos, por lo que se obtiene la siguiente conjetura.

Conjetura 2.

Sea q una potencia prima y B un conjunto de Sidon tipo Bose con q elementos, entonces es suficiente dejar $\left\lfloor \frac{3(q-1)}{4} \right\rfloor$ elementos para obtener un conjunto de Sidon libre de sumas.

Ejemplo 4.10 *Así del ejemplo 4.8 con* $q = 9$ *y* $\left\lfloor \frac{3(q-1)}{4} \right\rfloor$*=6. Se quitarán los elementos* $\{1, 22, 53\}$ *y se obtiene un conjunto Sidon libre de sumas.*

36	*37*	*44*	*49*	*55*	*78*
72	*73*	*0*	*5*	*11*	*34*
	74	*1*	*6*	*12*	*35*
		8	*13*	*19*	*42*
			18	*24*	*47*
				30	*53*
					76

Conclusiones

En esta sección destacamos los resultados más importantes obtenidos durante el desarrollo de este trabajo de grado.

- En el capítulo 2 demostramos que el máximo número de elementos que puede tener un conjunto libre de sumas módulo $2N$ es igual a N; es decir,

  $$LS\,(2N) = N.$$

  Mientras que para todo N impar probamos que tal número máximal es mayor o igual que $\frac{N}{3}$, queda la pregunta

  $$\text{¿}\lim_{N\to\infty}\left[\frac{LS\,(N)}{N}\right] \text{ existe ?}$$

- En el capítulo 4 probamos que:
  Para toda potencia prima q, el máximo número de elementos que puede tener un conjunto de Sidon tipo Singer y libre de sumas módulo q^2+q+1 es q; es decir,

  $$SLS\,(q^2+q+1) = q.$$

  Para toda primo impar p, el máximo número de elementos que puede tener un conjunto de Sidon tipo Ruzsa y libre de sumas módulo p^2-p es mayor o igual que $\frac{p-1}{2}$.

$$SLS\left(p^2-p\right) \geq \frac{p-1}{2}.$$

Resta probar que para toda potencia prima q impar, el máximo número de elementos que puede tener un conjunto de Sidon tipo Bose y libre de sumas módulo q^2-1 es mayor o igual que $\frac{q-1}{2}$.

$$SLS\left(q^2-1\right) \geq \frac{q-1}{2}.$$

- Además conjeturamos que:

$$SLS\left(p^2-p\right) \geq \frac{3\left(p-1\right)}{4},$$

y

$$SLS\left(q^2-1\right) \geq \left[\frac{3\left(q-1\right)}{4}\right].$$

Queda por responder la existencia o no de los siguientes límites

$$\lim_{p\to\infty}\left[\frac{SLS\left(p^2-p\right)}{p}\right]$$

$$\lim_{q\to\infty}\left[\frac{SLS\left(q^2-1\right)}{q}\right]$$

Se diseñaron algoritmos para apoyar la busqueda de ejemplos en el estudio de las funciones extremas $LS\left(N\right)$ y $SLS\left(N\right)$. Con su ayuda identificamos el ejemplo que nos permitio probar los teoremas del capítulo 2 y las cotas inferiores para $SLS\left(p^2-p\right)$ y $SLS\left(q^2+q+1\right)$.

Apéndice A

Algoritmos

Los algoritmos que se presentan en este trabajo son un apoyo para analizar el comportamiento de las funciones extremas.

Algoritmo A.1 *Determina si el conjunto A es libre de sumas módulo m.*

$sinsum := proc(A, m)$
begin
$if\ (map(A + A,\ \_mod, m)\ intersect\ A) = \{\}\ then\ 1\ else\ 0;$
end_if;
end_proc;

Ejemplo A.1 *Sea $A = \{1, 3, 4, 7, 8\}$ un conjunto no libre de sumas mód 9 y $A = \{1, 3, 7, 12\}$ un conjunto libre de sumas mód 19.*

```
esb2mod({1,4,3,7,8},9)
 0
esb2mod({1,3,7,12},19)
 1
```

Figura A.1: A es libre de sumas módulo m.

Algoritmo A.2 *Produce un conjunto libre de sumas módulo N con k elementos, si existe.*

$LSNk := proc(N, k)$
local $Zn,\ L,\ G,\ A$;
begin
$Zn := \{\$0..N-1\}$
$G := combinat :: subsets :: generator(Zn, k); L := [\ ];$
while $((A := G())\ <>\ FAIL\ and\ L = [\ ])$ *do*
$if\ (sinsum(A, N) = 1)\ then\ L := [op(L), A];$
end_if;
end_while;
L;
end_proc;

Ejemplo A.2 *Si el conjunto existe nos dará un conjunto libre de sumas con k elementos, si no existe nos dará* [ ].

```
LSNk(27,7);
 [{1, 3, 5, 7, 9, 11, 13}]
LSNk(27,10);
 []
LSNk(18,8);
 [{1, 3, 5, 7, 9, 11, 13, 15}]
LSNk(29,9); LSNk(27,9); LSNk(25,9); LSNk(23,9);
 [{1, 3, 5, 7, 9, 11, 24, 26, 28}]
 [{1, 3, 5, 7, 9, 20, 22, 24, 26}]
 [{1, 4, 6, 9, 11, 14, 16, 19, 21}]
 []
```

Figura A.2: Conjunto libre de sumas con k elementos

Algoritmo A.3 *Calcula un conjunto libre de sumas módulo N con k elementos que tiene a S como subconjunto.*

$LSNks := proc(N, k, S)$
$local\ Zn,\ L,\ G,\ A;$
$begin$
$Zn := \{\$0..N-1\}\ \ minus\ S; k := k - nops(S);$
$G := combinat :: subsets :: generator(Zn, k);\ \ L := [\ ];$
$while\ ((A := G())\ \ <>\ \ FAIL\ and\ L = [\ ])\ do$
$A := A\ union\ S;\ \ if\ \ (sinsum(A, N) = 1)\ then\ L := [op(L), A];$
$end\_if;$
$end\_while;$
$L;$
$end\_proc;$

Ejemplo A.3 *Si el conjunto existe nos dará un conjunto libre de sumas con k elementos que contiene a S como subconjunto, si no existe nos dará [ ].*

```
LSNks(25,10,{1,24,4,21,6,19});
 [{1, 4, 6, 9, 11, 14, 16, 19, 21, 24}]

LSNks(39,13,{1,38,3,36,5,34,7,32,9,30});
 [{1, 3, 5, 7, 9, 11, 13, 28, 30, 32, 34, 36, 38}]

LSNks(39,14,{1,3,5,7,9,30,32,34,36,38});
 []

LSNks(33,11,{1,3,5,7,26,28,30,32});
 [{1, 3, 5, 7, 9, 11, 24, 26, 28, 30, 32}]
```

Figura A.3: Conjunto libre de sumas con S como subconjunto

Algoritmo A.4 *Dados un conjunto A y un entero positivo m, determinar si A es conjunto de Sidon módulo m.*

esb2mod := $proc(A, m)$
local S,k;
begin
$S := map(A + A, \_mod, m)$; $k := nops(A)$;
$if\ nops(S) = k * (k + 1)/2\ \ then\ 1\ else\ 0$;
end_if;
end_proc;

Ejemplo A.4 *Si A es Sidon módulo m entonces nos dara 1, si no 0.*

```
sinsum({2,5,7,9,13},6)
 0
sinsum({5,7,13,17,23},8)
 1
```

Figura A.4: A Conjunto Sidon

Algoritmo A.5 *Construcción de conjuntos de Sidon tipo Bose: $q = p^r$. ($Para\ Sidon\ h = 2$).*

boseh := $proc(p, r, h)$
local F, t, B, q, q1, s, i;
begin
$F := Dom :: GaloisField(p, r * h)$;
$t := F :: randomPrimitive()$;
$B := \{1\}; q := p^r; q1 := q - 1; s := (q^h - 1)/q1$;
for i from 1 to q1 do
$B := \{op(B), F :: ln(t + t\hat{}(i * s), t)\}$;
end_for;
end_proc;

Ejemplo A.5 *Nos proporciona conjuntos de Sidon tipo Bose.*

```
boseh(5,1,2);
 {1, 3, 16, 17, 20}
boseh(3,2,2);
 {1, 13, 35, 48, 49, 66, 72, 74, 77}
boseh(3,2,2);
 {1, 22, 36, 37, 44, 49, 53, 55, 78}
boseh(11,1,2);
 {1, 22, 45, 56, 62, 71, 75, 76, 78, 103, 113}
```

Figura A.5: Conjuntos de Sidon tipo Bose

Algoritmo A.6 *Construcción de conjunto de Sidon tipo Singer:* $q = p^r$. *(Para Sidon* $h = 2$*).*

singerh $:=$ *proc*(p, r, h)
local q,N,S;
begin
$q := p^r; N := (q\hat{}(h+1) - 1)/(q-1);$
$S :=$ *map*$(boseh(p, r, h+1), \_mod, N);$
$S :=$ *Sunion* $\{0\}$;
end_proc;

Ejemplo A.6 *Nos proporciona conjuntos de Sidon tipo Singer.*

```
singerh(5,1,2);
 {0, 1, 15, 20, 22, 28}
singerh(3,2,2);singerh(2,3,2);
 {0, 1, 37, 39, 51, 58, 66, 69, 82, 86}
 {0, 1, 12, 20, 26, 30, 33, 35, 57}
singerh(11,1,2);singerh(7,1,2);
 {0, 1, 8, 21, 39, 43, 48, 54, 73, 105, 117, 131}
 {0, 1, 6, 21, 28, 44, 46, 54}
```

Figura A.6: Conjuntos de Sidon tipo Singer

Algoritmo A.7 *Construcción de conjuntos Sidon tipo Ruzsa. Datos: p primo, r raíz primitiva módulo p, f cualquiera no cero, u unidad mód p − 1.*

$ruzsa := proc(p, r, f, u)$
local p1,m,A;
begin
$p1 := p - 1; m := p * p1; A := \{\}$;
for i from 1 to p1 do
$A := \{op(A), (p * f * i - u * p1 * (r \hat{} i)) mod\ m\}$;
end_for;
end_proc;

Ejemplo A.7 *Nos proporciona conjuntos de Sidon tipo Ruzsa.*

```
ruzsa(5,3,1,1);
 {7, 13, 14, 16}
ruzsa(5,3,2,1);
 {2, 4, 16, 18}
ruzsa(7,3,8,1);
 {6, 16, 32, 36, 38, 40}
ruzsa(17,5,3,1);
 {2, 4, 31, 57, 71, 94, 109, 113, 152, 197, 202, 243, 246, 256, 267, 268}
ruzsa(11,7,6,1);
 {10, 14, 26, 68, 72, 74, 82, 100, 106, 108}
ruzsa(13,3,1,1);
 {16, 27, 35, 55, 66, 74, 94, 105, 113, 133, 144, 152}
```

Figura A.7: Conjuntos de Sidon tipo Ruzsa

Algoritmo A.8 *Calcula el primer conjunto de Sidon libre de sumas módulo m con k elementos, si existe.*

$primslsmodmk := proc(k, m)$
local $Zm,\ L,\ G,\ A;$
begin
$Zm := \{\$0..m-1\}; G := combinat :: subsets :: generator(Zm, k); L := [\ ];$
$while\ ((A := G(\ )) <>\ FAIL\ and\ L = [\ ])\ do$
$if\ (esb2mod(A, m) = 1\ and\ sinsum(A, m) = 1)\ then\ L := [op(L), A];$
end_if;
end_while;
$L;$
end_proc;

Ejemplo A.8 *Si el conjunto con k elementos existe con el módulo m dado, se mostrará, sino existe se mostrará* [ ].

```
primslsmodmk(3,11);
 [{1, 3, 8}]
primslsmodmk(4,19);
 [{1, 3, 7, 12}]
primslsmodmk(5,30);
 [{1, 4, 13, 23, 29}]
primslsmodmk(6,43);
 [{1, 17, 26, 29, 37, 39}]
```

Figura A.8: Conjuntos de Sidon libres de Sumas

Apéndice B

Un Resultado General

El siguiente teorema muestra un resultado general sobre conjuntos libres de sumas, en el sentido que todo conjunto finito de enteros no cero contiene una tercera parte que es libre de sumas. Especificamente:

Teorema B.1 (*ver* [4]) *Si B es un conjunto con m enteros distintos de cero entonces contiene un subconjunto A libre de sumas con cardinal*

$$|A| > \frac{m}{3}.$$

Demostración. Sean $B = \{b_1, b_2, ..., b_m\}$ un conjunto de m enteros distintos de cero y $p = 3k + 2$ un primo con la propiedad que: $p > 1 + máx\ B$. Por lo tanto para todo b_i se tiene un residuo diferente módulo p y este residuo nunca es cero. En el grupo ciclico $\mathbb{Z}_p$ cuyos elementos son $0, 1, 2, 3, ..., 3k + 1$, podemos observar que el siguiente conjunto es libre de sumas:

$$C = \{k + 1, k + 2, ..., 2k + 1\},$$

por que:

$$C + C = \{2k + 2, ..., 4k + 2\} \equiv \{0, 1, ..., k, 2k + 2, 2k + 3, ..., 3k + 1\}\ (mód\ p)$$

Además C es un conjunto grande en $\mathbb{Z}_p$:

$$|C| = k + 1 > \tfrac{1}{3}\,(3k + 2).$$

Ahora, si se escoge al azar un número entero x $(1 \leq x \leq p)$, de acuerdo con la distribución uniforme en el conjunto $\{1, 2, ..., p-1\}$ y se define d_i por $d_i \equiv xb_i \,(mód\ p)$, podemos ver que si x recorre desde 1 hasta $p-1$ entonces d_i también, porque b_i es primo relativo con p. Por lo tanto la probabilidad que C contiene d_i es exactamente:

$$\frac{|C|}{p-1} = \frac{k+1}{3k+1} > \frac{1}{3}.$$

Además el número esperado de elementos b_i tal que $d_i \in C$ es mayor que $\frac{m}{3}$. Por lo tanto existe x, $(1 \leq x \leq p)$, tal que:

$$|\{xb_1, xb_2, ..., xb_m\} \cap C| > \tfrac{m}{3}.$$

Y denotemos los correspondiente b_i como $b_{i_1}, b_{i_2}, ..., b_{i_k}$ donde $k > \frac{m}{3}$.
Como C es un conjunto libre de sumas entonces $xb_{i_l} + xb_{i_t} \not\equiv xb_{i_s} \,(mód\ p)$ para todo $1 \leq l, s, t \leq k$, y encontramos un subconjunto libre de sumas de B con cardinal mayor que $\dfrac{m}{3}$.

■

Bibliografía

[1] R.C. Bose and S. Chowla, *"Theorems in the additive theory of Numbers"*, Comment. Math. Helv. 37 $(1962-63)$, $141-147$.

[2] C. Alexis Gómez R. y Carlos A. Trujillo S., *"Una nueva construcción de conjuntos B_h módulares"*. Matemáticas Enseñanza Universitaria (ERM), Vol. XIX, $N°1$, Junio 2011, 53-62.

[3] Richard K. Guy., *"Unsolved problems in Number Theory"*. Third Edition, Springer 2004. Ver secciones C9, C14, E28, E32.

[4] Márton Hablicsek, *"Sum-Free Sets"*. Master's Thesis, Eötvös Loránd University. Budapest 2009.

[5] I. Ruzsa, *"Solving a linear equation in a set of integers"*. I. Acta Arith. 65(1993), $N°3$, 259-282.