Conjuntos de Sidon Libres de Sumas

Santiago Carlosama, Fabian Muñoz, Carlos Trujillo

Universidad del Cauca

ALTENCOA6-2014
San Juan de Pasto, Colombia
12 de agosto de 2014

Conjunto de Sidon

Sean $(G, +)$ un grupo conmutativo, notado aditivamente, y A un subconjunto de G.
A se llama un conjunto de Sidon (en G) si todas las sumas de dos elementos de A son distintas. Es decir, si para todo $x \in G$ se tiene que:

$$|A \cap (x - A)| \leq 2,$$

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

Conjunto Libre de Sumas

Sea $A \neq \Phi$, A se llama un conjunto libre de sumas(en G) si la ecuación $x + y = z$ no tiene soluciones con $x, y, z \in A$. Es decir, si

$$(A + A) \cap A = \Phi,$$

donde $\quad A + A = \{a + b : a, b \in A\}$, donde Φ es el conjunto vacio.

Conjuntos de Sidon: Construccion de Singer

Si $m = p^n$(p primo), entonces podemos encontrar $m+1$ enteros $d_0, d_1, \ldots, d_m$ tales que las m^2+m diferencias $d_i - d_j \,(i \neq j)\,, i, j = 0, 1, \ldots, m$ cuando se reducen modulo $\left(m^2+m+1\right)$ son todos los diferentes enteros no cero menores que $\left(m^2+m+1\right)$.

Conjuntos de Sidon: Construccion de Singer

Corolario 1

Si $m = p^n$(p primo), entonces podemos encontrar $m+1$ enteros $d_0, d_1, \ldots, d_m$ tales que las sumas $d_i + d_j \ (i \neq j), i, j = 0, 1, \ldots, m$ cuando se reducen modulo $\left(m^2 + m + 1\right)$ son todas los diferentes.

Conjunto Diferencia Perfecto

Se llama un conjunto diferencia perfecto a un conjunto $D \subseteq \mathbb{Z}_m, |D| = k$, talque todo elemento no cero tiene exactamente λ representaciones de la forma $x = d - d^*$; $d, d^* \in D$. Se representa por (m, k, λ).

Ejemplo

Sea $m = 5, m^2 + m + 1 = 31, S = \{0, 1, 3, 10, 14, 26\}, |S| = 6$

0	1	3	10	14	26
0	1	3	10	14	26
30	0	2	9	13	25
28	29	0	7	11	23
21	22	24	0	4	16
17	18	20	27	0	12
5	6	8	15	19	0

Estas son todas las diferencias, son todas distintas luego $S \ominus S = \mathbb{Z}_{31} - \{0\}$

Resultados Importantes

Teorema 1

Sea S un conjunto Singer, si $S^* = S - \{0\}$ entonces S^* es libre de sumas, es decir

$$x + y = z$$

no tiene solución en S^*.

Resultados Importantes

Demostración

Si existen $x_0, y_0, z_0 \in S^*$ tales que

$$x_0 + y_0 = z_0 \left(\text{mód } m^2 + m + 1\right)$$

entonces

$$x_0 - z_0 = -y_0$$

y esto no es posible, ya que, $S^* \ominus S^* = \mathbb{Z}_{m^2+m+1} - \{S^* \cup (-S^*)\}$.

Por lo tanto S^* es libre de sumas.

Resultados Importantes

Ejemplo

Sea $m = 5, m^2 + m + 1 = 31, S^* = \{1, 3, 10, 14, 26\}, |S^*| = 5$

1	3	10	14	26
2	4	11	15	27
	6	13	17	29
		20	24	5
			28	9
				21

Luego S^* es un conjunto libre de sumas.

Resultados Importantes

El reciproco del teorema anterior no es valido.

Ejemplo

Sea $S^* = \{1, 3, 7, 12\}\,(\acute{m}\acute{o}d\ 19)$, miremos que es libre de sumas y que S no es un conjunto tipo Singer.

$$\begin{array}{cccc}
1 & 3 & 7 & 12 \\
\hline
2 & 4 & 8 & 13 \\
 & 6 & 10 & 15 \\
 & & 14 & 0 \\
 & & & 5
\end{array}$$

Luego S^* es un conjunto libre de sumas.

Resultados Importantes

0	1	3	7	12
0	1	3	7	12
18	0	2	6	11
16	17	0	4	9
12	13	15	0	5
7	8	10	14	0

Luego S no es un conjunto tipo Singer.

Resultados Importantes

Notación

$$B_2(\textit{mód}\ \ N) := \{A \subseteq \mathbb{Z}_N : A\ \ es\ \ Sidon\}$$

$$LS(\textit{mód}\ \ N) := \{A \subseteq \mathbb{Z}_N : A\ \ es\ \ Libre\ \ de\ \ Sumas\}$$

$$S\,(\textit{mód}\ \ N) := \text{máx}\,\{|A| : A \in B_2\,(\textit{mód}\ \ N)\}$$

$$SL\,(\textit{mód}\ \ N) := \text{máx}\,\{|A| : A \in B_2\,(\textit{mód}\ \ N) \cap LS(\textit{mód}\ \ N)\}$$

Resultados Importantes

Observaciones

Sea m una potencia prima, entonces:

$$S\left(\text{mód } m^2+m+1\right)=m+1$$

$$SL\left(\text{mód } m^2+m+1\right)\geq m$$

Teorema 2

$$SL\left(\acute{mod}\ m^2+m+1\right)=m$$

Demostración

Tenemos que $SL\left(\acute{mod}\ m^2+m+1\right)\geq m$

Ahora sea $A\in B_2\left(\acute{mod}\ m^2+m+1\right), |A|\leq m+1$, por ser Sidon

Si $|A|=k$

$A\ominus A\subseteq\mathbb{Z}_{m^2+m+1}-\{A\cup(-A)\}\cup\{0\}$

$|A\ominus A|\leq m^2+m+1-1-|A\cup(-A)|$

$k\,(k-1)\leq m^2+m-k$

$k^2\leq m^2+m=m\,(m+1)$

Esto es $k\leq m$

Por lo tanto $SL\left(\acute{mod}\ m^2+m+1\right)=m$.

Ejemplo

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

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

GRACIAS