AGRA II: Aritmética, grupos y análisis
An ICTP-CIMPA Research School

Conjuntos de Sidon

Javier Cilleruelo

Universidad Autónoma de Madrid
Instituto de Ciencias Matemáticas (ICMAT)

franciscojavier.cilleruelo@uam.es

UNIVERSIDAD S. ANTONIO ABAD, CUSCO, PERÚ, del 8 al 22 de Agosto de 2015

Índice general

II

Prefacio

Uno de los temas favoritos de Paul Erdős y que mejor describe su gusto por los problemas aritméticos con sabor combinatorio, ha sido el de los conjuntos de Sidon. Corría el año 1932 cuando Simon Sidon, analista húngaro, le preguntó a Erdős sobre el crecimiento de sucesiones de enteros positivos con la propiedad de que todas las sumas de dos elementos de la sucesión son distintas.

Estos conjuntos, que Erdős llamaría más tarde conjuntos de Sidon, son el objeto de este curso. Aunque el interés de Sidon por estos conjuntos tenía que ver con cuestiones del análisis de Fourier, el problema cautivó a un joven Erdős por su vertiente aritmética y combinatoria y se convertiría en un tema recurrente en su investigación hasta que nos abandonara en 1998 en busca de "El Libro", ese libro virtual donde Erdős afirmaba que se encuentran las demostraciones más elegantes e ingeniosas que jamás hayan sido escritas.

Son muchos los problemas que nos podemos plantear acerca de los conjuntos de Sidon. Casi todos ellos tienen que ver con el tamaño máximo que pueden llegar a tener estos conjuntos en un intervalo o un grupo finito dado, y en el caso de las sucesiones infinitas, con la construcción de sucesiones infinitas de Sidon A cuya función contadora $A(x) = |A \cap [1, x]|$ crezca tanto como como sea posible. Estos dos problemas, tratados en el primero y en el segundo capítulo respectivamente, serán los objetivos principales del curso.

Hemos dedicado un último capítulo a problemas sin resolver sobre los conjuntos de Sidon donde hemos aprovechado para comentar otros problemas sobre conjuntos de Sidon no tratados en los dos primeros capítulos. Es posible que el lector más ambicioso no resista la tentación

de empezar por este capítulo y utilizar los capítulos anteriores y las referencias para ir completando información.

Los dos primeros capítulos están acompañados de ejercicios que ayudarán al lector a afianzar los contenidos del curso. Algunos son sencillos o consisten en completar algunos detalles de alguna demostración. Otros tienen mayor dificultad y permiten al lector explorar nuevos territorios.

Las notas de este curso son una parte del libro "Conjuntos de Sidon"[7], que fue escrito para el curso que con el mismo título, fue impartido en Mérida (Venezuela) en septiembre de 2014. El capítulo II del libro "Sequences"de Halberstam y Roth [37] es una referencia clásica sobre los conjuntos de Sidon hasta 1966. Erdős y R. Freud [28] escribieron un survey muy completo hasta 1991, pero en húngaro. "A complete annotated bibliography of work related to Sidon sequences", de Kevyn O'Bryant [52], es también una fuente de información valiosa sobre conjuntos de Sidon.

Javier Cilleruelo

Capítulo 1

Conjuntos de Sidon finitos

1.1. Los orígenes

Erdős solía contar la siguiente anécdota referida a Simon Sidon. Una de las tardes que él y su amigo Paul Turán fueron a visitar al analista húngaro, Sidon abrió bruscamente la puerta y les gritó: *vengan en otro momento y busquen a otra persona.* No sería esa tarde sino otra cuando Simon Sidon despertó el interés de Erdős al preguntarle por los conjuntos de enteros positivos con la propiedad de que todas las sumas de dos elementos de la sucesión son distintas.

Aunque el interés de Sidon por estos conjuntos tenía que ver con cuestiones del análisis de Fourier, el problema cautivó a un joven Erdős por su vertiente aritmética y combinatoria y se convertiría en un tema recurrente en su investigación hasta que nos abandonara en 1996 en busca de "El Libro", ese libro virtual donde Erdős afirmaba que se encuentran las demostraciones más ingeniosas y elegantes que jamás hayan sido escritas. Fue el propio Erdős quien bautizó con el nombre de conjuntos de Sidon a estos conjuntos. Una definición más formal y más general de un conjunto de Sidon es la siguiente.

Definición 1.1.1. *Sea G un grupo conmutativo. Un conjunto $A \subset G$ es un conjunto de Sidon si*

$$a + b = c + d \implies \{a, b\} = \{c, d\}$$

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

En otras palabras, A es un conjunto de Sidon si todas las sumas de dos elementos de A son distintas salvo por el orden de presentación de los sumandos.

Como $a+b=c+d$ si y sólo si $a-c=d-b$, los conjuntos de Sidon también se definen, indistintamente, como aquellos con la propiedad de que todas las diferencias no nulas de sus elementos son distintas.

Habitualmente utilizaremos el término conjunto de Sidon cuando nos refiramos a un conjunto finito y sucesión de Sidon cuando éste sea infinito. En este capítulo empezaremos estudiando los conjuntos de Sidon finitos y dejaremos para el siguiente las sucesiones de Sidon infinitas.

El conjunto siguiente es un conjunto de Sidon:

$$A=\{1,\ 2,\ 5,\ 10,\ 16,\ 23,\ 33,\ 35\}.$$

Una manera de organizar el cálculo de todas las diferencias positivas de dos elementos del conjunto para comprobar que efectivamente es un conjunto de Sidon, consiste en construir el triángulo de diferencias como se muestra a continuación. En la primera fila y en negrita hemos dispuesto los elementos del conjunto y en las filas inferiores todas las diferencias de dos elementos del conjunto que provienen de las elementos en negrita de las dos diagonales correspondientes. Nótese que todas las diferencias son distintas, así que el conjunto A es, efectivamente, un conjunto de Sidon. Más adelante veremos que es de tamaño maximal; es decir, el intervalo $[1,35]$ no contiene ningún conjunto de Sidon de 9 elementos.

1		**2**		**5**		**10**		**16**		**23**		**33**		**35**	
	1		3		5		6		7		10		2		
		4		8		11		13		17		12			
			9		14		18		23		19				
				15		21		28		25					
					22		31		30						
						32		33							
							34								

Parece totalmente improbable que exista una fórmula sencilla que nos proporcione, de manera exacta, el mayor tamaño de un conjunto de

Sidon en el intervalo $[1, n]$. Sin embargo sí que sabemos dar una respuesta asintótica a este problema. Se tratará en la siguiente sección pero antes dedicaremos unas pocas líneas a la notación que utilizaremos a lo largo del curso.

Se recuerda que $f(x) = O(g(x))$ significa que existe una constante positiva C tal que $f(x) < Cg(x)$ para x suficientemente grande. Se utiliza principalmente cuando en una estimación hay un término principal y un término de error del que sólo nos interesa el orden de magnitud. Algunas veces se utiliza también la notación $f(x) \ll g(x)$ para indicar lo mismo. Ésta última se utiliza sobre todo cuando del término principal sólo nos interesa el orden de magnitud.

La notación $f(x) = o(g(x))$ indica, por el contrario, que $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$. Así que, por ejemplo, los términos $o(1)$ se refieren siempre a cantidades que tienden a cero cuando x tiende a infinito.

1.2. Conjuntos de Sidon en intervalos

¿Cuál es el mayor número de elementos que puede tener un conjunto de Sidon en el intervalo $\{1, \ldots, n\}$?

Esta es una pregunta básica sobre los conjuntos de Sidon a la que se sabe dar una respuesta asintótica. Utilizaremos la notación clásica (ver [37], capítulo II)

$$F_2(n) = \max |A| : \ A \subset \{1, \ldots, n\}, \ A \text{ es Sidon.}$$

Un sencillo argumento de conteo proporciona una primera cota superior para esta cantidad. Como todas las diferencias positivas $a - a', \ a, a' \in A$ son distintas y menores que n y hay exactamente $\binom{|A|}{2}$ de esas diferencias, se tiene la desigualdad $\binom{|A|}{2} \leq n - 1$, de la que se sigue la cota trivial

$$F_2(n) < \sqrt{2n} + 1/2. \tag{1.1}$$

Esta cota superior ya permite ver que, como decíamos en la sección anterior, un conjunto de Sidon en el intervalo $[1, 35]$ no puede tener más de 8 elementos:

$$F_2(35) < \sqrt{70} + 1/2 = 8{,}866\ldots$$

La cota superior (1.1) está lejos de ser una cota óptima cuando n es grande. Pero se puede mejorar si en lugar de tener en cuenta todas las diferencias $a-a',\ a,a'\in A$, se consideran sólo las diferencias pequeñas. De esta manera Erdős y Turán [30] demostraron la desigualdad

$$F_2(n) < \sqrt{n} + O(n^{1/4}).$$

Años más tarde Lindström [44] precisó más el término de error con una demostración muy ingeniosa que reproducimos aquí.

Teorema 1.2.1 (Lindström)**.**

$$F_2(n) < n^{1/2} + n^{1/4} + 1.$$

Demostración. Sean $1 \le a_1 < \cdots < a_k \le n$ los elementos de un conjunto de Sidon en $[1,n]$. Dado un r, que elegiremos al final, las siguientes desigualdades son claras:

$$\begin{array}{rcl} (a_2-a_1)+(a_3-a_2)+\cdots+(a_k-a_{k-1}) & = & a_k-a_1<n \\ (a_3-a_1)+(a_4-a_2)+\cdots+(a_k-a_{k-2}) & = & a_k+a_{k-1}-(a_1+a_2)<2n \\ & & \cdots \\ (a_{r+1}-a_1)+(a_{r+2}-a_2)+\cdots+(a_k-a_{k-r}) & = & (a_k+\cdots+a_{k-(r+1)})-(a_1+\cdots+a_r)<rn \end{array} \tag{1.2}$$

En la parte izquierda aparecen exactamente

$$(k-1)+(k-2)+\cdots+(k-r) = rk-r(r+1)/2$$

diferencias positivas de la forma a_j-a_i y todas ellas son distintas por ser $\{a_1,\dots,a_k\}$ un conjunto de Sidon. Así que si $l=rk-r(r+1)/2$ y llamamos S_r a la suma de todas esas diferencias tenemos que

$$S_r = \sum_{\substack{i,j \\ 1\le i<j\le i+r}} (a_j-a_i) \ \ge \ \sum_{n=1}^{l} n > \frac{l^2}{2} = (rk-r(r+1)/2)^2/2.$$

Por otra parte, las desigualdades de la parte derecha en (1.2) implican que

$$S_r < n+(2n)+\cdots+(rn) = nr(r+1)/2.$$

De las dos desiguladades sobre S_r obtenemos que

$$\begin{array}{rcl} k & < & \sqrt{n(1+1/r)}+(r+1)/2 \\ & < & \sqrt{n}+\dfrac{\sqrt{n}}{2r}+\dfrac{r+1}{2}. \end{array}$$

La elección de $r=\lceil n^{1/4}\rceil$ finaliza la demostración. □

Vamos a dar otra demostración distinta, más moderna e inspiradora, que es esencialmente la que dio Ruzsa [54]. Antes de proceder vamos a introducir algunas definiciones y notaciones que son habituales en la teoría combinatoria de números.

Sea G un grupo conmutativo. Dados dos subconjuntos $A, B \subset G$, definimos el conjunto suma

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

y la función

$$r_{A+B}(x) = |\{(a, b) \in A \times B,\ a + b = x\}|,$$

que cuenta el número de representaciones de x como suma de un elemento de A y otro de B. A lo largo del curso haremos uso de las identidades triviales

$$r_{A-A}(0) = |A| \tag{1.3}$$

y

$$\sum_{x \in G} r_{A+B}(x) = |A||B|. \tag{1.4}$$

La cantidad

$$\sum_x r^2_{A+B}(x)$$

se denomina *energía aditiva* entre A y B y cuenta el número de soluciones de la ecuación $a + b = a' + b'$ con $a, a' \in A$ y $b, b' \in B$, que coincide con el número de soluciones de la ecuación $a - a' = b' - b$ con $a, a' \in A$ y $b, b' \in B$. Esta observación da lugar a la identidad

$$\sum_x r^2_{A+B}(x) = \sum_x r_{A-A}(x) r_{B-B}(x), \tag{1.5}$$

que aparecerá insistentemente a lo largo de este curso.

El siguiente lema se debe a Ruzsa [54].

Lema 1.2.1 (Ruzsa [54])**.** *Sea A un conjunto de Sidon en un grupo conmutativo G y sea B cualquier subconjunto de G. Entonces se tiene que*

$$|A|^2 \leq |A + B| \left(1 + \frac{|A| - 1}{|B|}\right). \tag{1.6}$$

Demostración. Haciendo uso de la identidad (1.4), de la desigualdad de Cauchy-Schwarz y de (1.5) obtenemos

$$\begin{aligned}(|A||B|)^2 &= \left(\sum_{x\in A+B} r_{A+B}(x)\right)^2 \\ &\le |A+B|\sum_x r_{A+B}^2(x) \\ &= |A+B|\sum_x r_{A-A}(x)r_{B-B}(x). \end{aligned} \tag{1.7}$$

Como $r_{A-A}(x)\le 1$ para $x\neq 0$, tenemos que

$$\begin{aligned}\sum_x r_{A-A}(x)r_{B-B}(x) &= r_{A-A}(0)r_{B-B}(0)+\sum_{x\neq 0} r_{A-A}(x)r_{B-B}(x) \\ &\le r_{A-A}(0)r_{B-B}(0)+\sum_{x\neq 0} r_{B-B}(x) \\ &= |A||B|+|B|^2-|B|. \end{aligned} \tag{1.8}$$

De (1.7) y (1.8) se sigue la desigualdad

$$(|A||B|)^2 \le |A+B|\left(|A||B|+|B|^2-|B|\right)$$

y la demostración del lema. □

El Lema 1.2.1 fue utilizado por Ruzsa para dar una demostración alternativa de la desigualdad de Lindström en el Teorema 1.2.1. Una pequeña modificación técnica permite una ligera mejora en la desigualdad.

Teorema 1.2.2 (Cilleruelo [10], Ruzsa [54])**.** *Si $A\subset[1,n]$ es un conjunto de Sidon, entonces*

$$|A| < n^{1/2}+n^{1/4}+1/2.$$

Demostración. Consideremos el conjunto $B=[0,l]\cap\mathbb{Z}$ donde

$$l=\lfloor\sqrt{n(|A|-1)}\rfloor.$$

Entonces $|A+B| \leq n+l$ y $|B| = l+1$. Así que el Lema 1.2.1 implica la desigualdad

$$\begin{aligned} |A|^2 &\leq (n+l)\left(1+\frac{|A|-1}{l+1}\right) \\ &< n+l+\frac{n(|A|-1)}{l+1}+|A|-1 \\ &\leq n+2\sqrt{n(|A|-1)}+|A|-1 \\ &= (\sqrt{n}+\sqrt{|A|-1})^2, \end{aligned}$$

que una sencilla manipulación conduce a la desigualdad

$$(|A|-\sqrt{n})^2 < |A|-1. \tag{1.9}$$

Escribiendo $|A| = \sqrt{n}+cn^{1/4}+1/2$ y sustituyendo esta expresión en (1.9) obtenemos

$$c^2n^{1/2}+cn^{1/4}+1/4 < n^{1/2}+cn^{1/4}-1/2,$$

que da lugar a una contradicción cuando $c \geq 1$. □

Ejercicio 1.2.1 (Cilleruelo [10])**.** *Demostrar que si $A \subset \{1,\dots,n\}$ es tal que $r_{A-A}(x) \leq g$ para todo $x \neq 0$, entonces*

$$|A| \leq (gn)^{1/2}+(gn)^{1/4}+1/2.$$

Es interesante observar que todas las demostraciones que se conocen de la estimación $F_2(n) < \sqrt{n}+O(n^{3/4})$ sólo utilizan el hecho de que todas las diferencias menores que $n^{3/4}$ son distintas. El siguiente ejercicio ilustra todavía mejor ese hecho.

Ejercicio 1.2.2. *Sea $\omega(x)$ una función que tiende a infinito y sea $A \subset [1,n]$ un conjunto de enteros positivos tal que $r_{A-A}(x) \leq 1$ para todo $x,\ 1 \leq x \leq \omega(n)\sqrt{n}$. Demostrar que entonces $|A| \leq (1+o(1))\sqrt{n}$.*

La cota superior

$$F_2(n) < n^{1/2}+n^{1/4}+1/2$$

parece ser el límite del método consistente en contar diferencias pequeñas. Aunque durante mucho tiempo Erdős conjeturó que $F_2(n) <$

$\sqrt{n}+O(1)$, acabó afirmando [27] que la conjetura era demasiado optimista y que la conjetura correcta debería ser $F_2(n) < \sqrt{n}+O(n^\epsilon)$ para todo $\epsilon > 0$. El Ejercicio 1.3.8 apoya también la creencia de que

$$\limsup_{n\to\infty}(F_2(n)-\sqrt{n}) = \infty, \tag{1.10}$$

pero todavía no se ha encontrado una demostración de este hecho.

El Teorema 1.2.2 también puede deducirse a partir de la siguiente desigualdad que tiene su propio interés.

Teorema 1.2.3. *Si $A \subset [1,n]$ entonces*

$$|A| < \sqrt{n} + \sqrt{|A|^2 - |A-A|}.$$

Dejamos al lector la demostración de este teorema en el siguiente ejercicio.

Ejercicio 1.2.3. *Sean A y B dos subconjuntos de un grupo conmutativo G. Demostrar que*

$$|A|^2 \le |A+B|\left(1+\frac{|A|^2-|A-A|}{|B|}\right).$$

y utilizar esta desigualdad para demostrar el Teorema 1.2.3.

Ejercicio 1.2.4. *Dar una demostración alternativa del Teorema 1.2.2 a partir del Teorema 1.2.3.*

Ejercicio 1.2.5. *Sea $A \subset [1,n]$ un conjunto de enteros positivos tal que $|A-A| = (1+o(1))|A|^2$. Demostrar que $|A| \le (1+o(1))\sqrt{n}$.*

El Ejercicio 1.2.5 muestra que la condición de ser de Sidon no es estrictamente necesaria para obtener la cota superior $|A| \le (1+o(1))\sqrt{n}$. Es suficiente con que $|A-A| \sim |A|^2$.

En contra de lo que se pudiera sospechar no se llega a la misma conclusión si asumimos que $|A+A| \sim |A|^2/2$. Erdős y Freud [28] construyeron, para cada n, un conjunto $A \subset [1,n]$ con $|A| \sim \frac{2}{\sqrt{3}}\sqrt{n} = (1{,}154\ldots)\sqrt{n}$ elementos y tal que $|A+A| \sim |A|^2/2$.

Consideraron un conjunto de Sidon B de tamaño máximo en $[1,n/3)$ que, como veremos en la próxima sección, tiene $\sim \sqrt{n/3}$ elementos. El

conjunto $A = B \cup (n - B)$ tiene entonces $\sim \frac{2}{\sqrt{3}}\sqrt{n}$ elementos y es fácil comprobar que todas las sumas de dos elementos de A con distintas excepto las $|B|$ sumas de la forma $b+(n-b)$. Dejamos los detalles como un ejercicio.

Ejercicio 1.2.6. *Demostrar que el conjunto $A \subset [1, n]$ construido por Erdős y Freud satisface que $|A + A| \sim |A|^2/2$ y tiene $|A| \sim \frac{2}{\sqrt{3}}\sqrt{n}$ elementos.*

El ejercicio siguiente da una estimación trivial en la otra dirección.

Ejercicio 1.2.7. *Sea $A \subset [1, n]$ un conjunto de enteros positivos tal que $|A + A| = (1 + o(1))|A|^2/2$. Demostrar que $|A| \leq (1 + o(1))2\sqrt{n}$.*

O. Pikhurko [53] ha demostrado que si $A \subset [1, n]$ es tal que $|A+A| = (1 + o(1))|A|^2/2$ entonces $|A| \leq (1{,}863\ldots)\sqrt{n}$.

1.3. Conjuntos de Sidon en grupos conmutativos finitos

Para obtener buenas cotas inferiores para $F_2(n)$ necesitamos construir conjuntos de Sidon en $\{1, \ldots, n\}$ tan grandes como sea posible. Las mejores construcciones conocidas provienen de construcciones algebraicas en grupos cíclicos. Es claro que si $A \subset \mathbb{Z}_n$ es un conjunto de Sidon en $\mathbb{Z}_n$ también lo es en el intervalo $[1, n]$. Sin embargo el recíproco no es cierto. Es sencillo comprobar que el conjunto $\{1, 2, 5, 10, 16, 23, 33, 35\}$, que era un conjunto de Sidon en el intervalo $[1, 35]$, no lo es, sin embargo, en $\mathbb{Z}_{35}$.

Sea A un conjunto de Sidon en un grupo conmutativo finito G. Como todas las diferencias $a - a',\ a \neq a' \in A$ son no nulas y distintas, se tiene la desigualdad trivial $|A|(|A| - 1) \leq |G| - 1$, que implica la cota superior

$$|A| \leq \sqrt{|G| - 3/4} + 1/2. \tag{1.11}$$

Es decir, si llamamos $F_2(G)$ al máximo cardinal de un conjunto de Sidon en G, siempre se tiene que

$$F_2(G) \leq \left\lfloor \sqrt{|G| - 3/4} + 1/2 \right\rfloor. \tag{1.12}$$

Esta cota superior es óptima para algunas familias infinitas de grupos finitos. El ejemplo más sencillo para el que se alcanza esta cota, y que es un caso particular del Ejemplo 1 que aparece más adelante, es la parábola en $\mathbb{Z}_p \times \mathbb{Z}_p$ cuando p es un primo impar:

$$A = \{(x, x^2) : \ x \in \mathbb{Z}_p\} \subset G = \mathbb{Z}_p \times \mathbb{Z}_p.$$

Ejercicio 1.3.1. *Sea q una potencia de un primo impar. Demostrar que el conjunto $A = \{(x, x^2) : \ x \in \mathbb{F}_q\}$ es un conjunto de Sidon en $\mathbb{F}_q \times \mathbb{F}_q$. Comprobar que para esta familia de grupos se alcanza la cota superior* (1.12).

Probablemente Erdős y Turán [30] se inspiraron en este conjunto para construir el primer ejemplo de un conjunto de Sidon A en $\{1, \dots, n\}$ con $|A| \gg \sqrt{n}$.

Ejercicio 1.3.2 (Erdős y Turán)**.** *Demostrar que para todo p primo, el conjunto*

$$A = \{(x^2)_p + 2xp : \ 0 \le x \le p-1\}$$

es un conjunto de Sidon en $\{1, \dots, 2p^2\}$ con p elementos. Deducir de esto que $F_2(n) \ge \sqrt{n/2}(1 + o(1))$.

A continuación describimos otras familias de conjuntos de Sidon de tamaño máximo en sus grupos ambientes correspondientes. En lo que sigue q indicará un primo o la potencia de un primo.

Ejemplo 1. *Sea q una potencia de un primo impar y sean $r(x), s(x) \in \mathbb{F}_q[X]$ polinomios de grado menor o igual que 2, linealmente independientes en $\mathbb{F}_q$. Entonces, el conjunto*

$$A = \{(r(x), s(x)) : \ x \in \mathbb{F}_q\}$$

es un conjunto de Sidon en $\mathbb{F}_q \times \mathbb{F}_q$ con q elementos.

Ejercicio 1.3.3. *Demostrar que los conjuntos del Ejemplo 1 son conjuntos de Sidon en $\mathbb{F}_q \times \mathbb{F}_q$.*

Ejercicio 1.3.4. *Sea $q = 2^n$. Demostrar que el conjunto*

$$A = \{(x, x^3) : \ x \in \mathbb{F}_q\}$$

es un conjunto de Sidon en $\mathbb{F}_q \times \mathbb{F}_q$.

Ejemplo 2. *Para todo generador g de $\mathbb{F}_q^*$, el conjunto*

$$A = \{(x, g^x) : \ x \in \mathbb{Z}_{q-1}\} \tag{1.13}$$

es un conjunto de Sidon en $\mathbb{Z}_{q-1} \times \mathbb{F}_q$ con $q-1$ elementos. Este conjunto también se puede describir de la forma

$$A = \{(\log x, x) : \ x \in \mathbb{F}_q^*\}$$

donde $\log x = \log_g x$ es el logaritmo discreto en base g.

Para probar que A es un conjunto de Sidon, tenemos que ver que dado un elemento $(a, b) \in \mathbb{Z}_{q-1} \times \mathbb{F}_q$, $(a, b) \neq (0, 0)$, la igualdad

$$(x, g^x) - (y, g^y) = (a, b) \tag{1.14}$$

determina los valores x, y. La igualdad (1.14) se puede escribir de la forma

$$\begin{aligned} x - y &\equiv a \pmod{q-1} \\ g^x - g^y &\equiv b \pmod{q}. \end{aligned}$$

De la primera ecuación se tiene que $g^x = g^{y+a}$, que sustituido en la segunda da lugar a la ecuación $g^y(g^a - 1) = b$. Si $a = 0$ entonces $b = 0$, en contra de lo supuesto. Si $a \neq 0$, entonces $g^a - 1 \neq 0$ y el valor de y queda determinado y a su vez el de x.

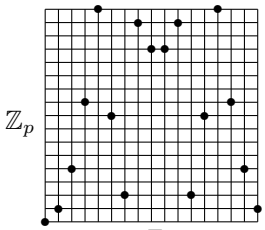
Ejemplo 3. *Dados dos generadores g_1, g_2 de $\mathbb{F}_q^*$, el conjunto*

$$A = \{(x, y) \in \mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1} : \ g_1^x + g_2^y = 1\} \tag{1.15}$$

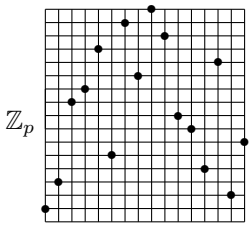
es un conjunto de Sidon en $\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}$ con $q-2$ elementos.

Ejercicio 1.3.5. *Demostrar que el conjunto del Ejemplo 3 es un conjunto de Sidon.*

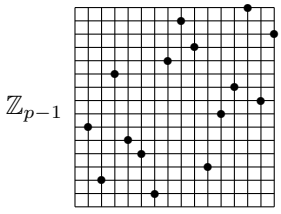
Cuando $q = p$ es un primo, podemos identificar $\mathbb{F}_p$ with $\mathbb{Z}_p$. Las figuras de abajo corresponden a los conjuntos de Sidon descritos para el caso $p = 17$.



Ejemplo 1



Ejemplo 2



Ejemplo 3

Observar que los conjuntos de Sidon de estos ejemplos, con q, $q-1$ y $q-2$ elementos respectivamente, tienen cardinal máximal (los dos primeros) o casi (el último).

Ejercicio 1.3.6. Sea $\phi : G \to G'$ un isomorfismo entre los grupos G y G'. Demostrar que si A es un conjunto de Sidon en G, entonces el conjunto $\phi(A) = \{\phi(a) : \ a \in A\}$ es un conjunto de Sidon en G'.

Como muestra el Ejercicio 1.3.6, los isomorfismos entre grupos preservan la propiedad de ser de Sidon. Así que la imagen del conjunto de Sidon descrito en el Ejemplo 2 por el isomorfismo natural entre $\mathbb{Z}_{p-1}\times\mathbb{Z}_p$ y $\mathbb{Z}_{p(p-1)}$ es un conjunto de Sidon en $\mathbb{Z}_{p(p-1)}$ de $p-1$ elementos. Esta observación se debe a Ruzsa [54] y proporciona la construcción más sencilla de conjuntos de Sidon de tamaño maximal en grupos cíclicos

Proposición 1.3.1 (Ruzsa)**.** *Sea g un generador de $\mathbb{F}_p^*$. El conjunto*

$$A = \{px - (p-1)(g^x)_p : \ 0 \le x \le p-2\}$$

es un conjunto de Sidon en $\mathbb{Z}_{p(p-1)}$.

Se deja al lector la demostración de la Proposición 1.3.1 en el siguiente ejercicio.

Ejercicio 1.3.7. *Demostrar que el conjunto A de la Proposición 1.3.1 es la imagen del conjunto del Ejemplo 2 bajo el isomorfismo natural entre $\mathbb{Z}_{p-1}\times\mathbb{Z}_p$ y $\mathbb{Z}_{(p-1)p}$, y que por lo tanto el conjunto A es un conjunto de Sidon en $\mathbb{Z}_{(p-1)p}$.*

La siguiente reflexión y el Ejercicio 1.3.8 invitan a pensar que la conjetura (1.10) debería ser cierta. Si se eligen al azar $p-1$ elementos de

$\mathbb{F}_p$ con repetición (un mismo elemento puede ser elegido varias veces), con alta probabilidad ocurriría que algunos elementos serían elegidos más de una vez, otros ninguna e incluso habría un intervalo de longitud aproximadamente $\log p$ cuyos elementos no habrían sido elegidos. Es decir, habría lagunas de longitud $\sim \log p$. Se piensa que la sucesión $g^x - x \pmod p,\ x = 1, \ldots, p-1$ se comporta como una sucesión aleatoria de este tipo, pero ni siquiera se ha podido demostrar la siguiente conjetura.

Conjetura 1.3.1. *Para todo M existe un primo p y un generador g de $\mathbb{F}_p^*$ tal que la sucesión $g^x - x \pmod p,\ x = 0, \ldots, p-1$ no contiene ningún elemento en algún intervalo I de longitud M.*

Ejercicio 1.3.8. *Utilizar el Teorema 1.3.1 para demostrar que la Conjetura 1.3.1 implicaría que*

$$\limsup_{n\to\infty}(F_2(n) - \sqrt{n}) = \infty.$$

Es decir, que la conjetura de Erdős, $F_2(n) < \sqrt{n} + O(1)$, no sería cierta.

Los conjuntos de Sidon construidos en la Proposición 1.3.1 permite obtener una buena cota inferior para $F_2(n)$.

Teorema 1.3.1. *Sea θ con la propiedad de que para todo m suficientemente grande, el intervalo $(m, m + m^\theta)$ contiene algún primo. Entonces*

$$F_2(n) \geq n^{1/2} + O(n^{\theta/2}).$$

Demostración. Dado n, sea p el mayor primo tal que $p(p-1) \leq n$. Si n es suficientemente grande podemos encontrar un tal primo p con $p > n^{1/2} - 2n^{\theta/2}$. Es claro que el conjunto construido en la Proposición 1.3.1 es, en particular, un conjunto de Sidon en $\{1, \ldots, p(p-1)\}$ y por lo tanto en $\{1, \ldots n\}$ □

Se conjetura que en el Teorema 1.3.1 es posible tomar cualquier $\theta > 0$ pero sólo se sabe cierto [4] para $\theta \geq 0{,}525$.

De los Teoremas 1.2.2 y 1.3.1 se deduce la estimación asintótica para $F_2(n)$.

Corolario 1.3.1. $F_2(n) \sim \sqrt{n}$.

Las conjeturas sobre las cotas superior y la cota inferior se pueden resumir en la siguiente.

Conjetura 1.3.2. *$F_2(n) = \sqrt{n} + O(n^\epsilon)$ para todo $\epsilon > 0$.*

Existen otras familias de grupos cíclicos que contienen conjuntos de Sidon que alcanzan la cota superior (1.12). La primera de ellas fue encontrada por Singer [61]. Utilizando geometría proyectiva finita construyó un conjunto de Sidon A de $q+1$ elementos en $\mathbb{Z}_{q^2+q+1}$. Nótese que el tamaño de su conjunto diferencia es $|A-A| = |A|^2-|A|+1 = q^2+q+1$. Es decir todo elemento no nulo del grupo se escribe, de manera única, como diferencia de dos elementos de A. Los conjuntos con esta propiedad se denominan conjuntos de diferencias perfectas y fue en este contexto donde este conjunto fue encontrado. Pasaron algunos años hasta que esta construcción fuera conocida por Erdős y popularizada en el mundo de los conjuntos de Sidon. Posteriormente Bose y Chowla [5] construyeron un conjunto de Sidon de q elementos en $\mathbb{Z}_{q^2-1}$. Estas construcciones, los Ejemplos 1,2, 3 y la cota superior en (1.11) prueban el valor exacto de $F_2(G)$ para algunas familias de grupos:

$$\begin{aligned} F_2(\mathbb{F}_q \times \mathbb{F}_q) &= q \\ F_2(\mathbb{F}_q \times \mathbb{Z}_{q-1}) &= q-1 \\ F_2(\mathbb{Z}_{q^2+q+1}) &= q+1 \\ F_2(\mathbb{Z}_{q^2-1}) &= q \\ F_2(\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}) &\in \{q-2, q-1\} \end{aligned}$$

Observar que si $q = p^n$, entonces el grupo aditivo en $\mathbb{F}_q$ es isomorfo a grupo $\mathbb{Z}_p \times \overbrace{\cdots}^{n} \times \mathbb{Z}_p$.

Se desconoce si $F_2(\mathbb{Z}_n)$ tiene comportamiento asintótico cuando $n \to \infty$. Lo único que se sabe se resume en el ejercicio siguiente.

Ejercicio 1.3.9. *Demostrar las siguientes desigualdades.*

$$\frac{1}{\sqrt{2}} \leq \liminf_{n\to\infty} \frac{F_2(\mathbb{Z}_n)}{\sqrt{n}} \leq \limsup_{n\to\infty} \frac{F_2(\mathbb{Z}_n)}{\sqrt{n}} = 1. \tag{1.16}$$

1.4. Conjuntos B_h

Los conjuntos B_h son una generalización natural de los conjuntos de Sidon en los que todas las sumas de h elementos del conjunto son distintas. De hecho, a los conjuntos de Sidon también se los denomina conjuntos B_2.

Definición 1.4.1. *Sea G un grupo conmutativo. Decimos que $A \subset G$ es un conjunto B_h si todas las sumas*

$$a_1 + \cdots + a_h, \quad a_1, \ldots, a_h \in A$$

son distintas salvo por el orden de presentación de los sumandos. En general decimos que A es un conjunto $B_h[g]$ si para todo $x \in G$ la ecuación

$$x = x_1 + \cdots + x_h, \ x_i \in A$$

tiene a lo más g soluciones distintas salvo por permutaciones de los sumandos.

Se define $F_h(n)$ como el mayor número de elementos que puede llegar a tener un conjunto B_h en $\{1, \ldots, n\}$. De manera análoga se define $F_h(G)$ como el mayor tamaño de un conjunto B_h en G.

Los conjuntos B_h son bastante más esquivos que los conjuntos de Sidon debido a que no tienen una caracterización natural en términos de diferencias. Eso hace que algunos resultados, análogos a los que son conocidos para los conjuntos de Sidon, no se hayan logrado demostrar para los conjuntos B_h. En particular se desconoce el comportamiento asintótico de $F_h(n)$, incluso se desconoce si dicho comportamiento asintótico existe. En cualquier caso no es difícil obtener una cota superior utilizando el resultado del problema siguiente.

Ejercicio 1.4.1. *Demostrar que el número de sumas de h elementos (no necesariamente distintos) de un conjunto A es a lo más $\binom{|A|+h-1}{h}$.*

Sea $A \subset [1, n]$ un conjunto B_h de enteros positivos. Como todas las sumas de h elementos de A son distintas y menores o iguales que hn, el resultado del ejercicio anterior implica que

$$\frac{|A|^h}{h!} < \binom{|A| + h - 1}{h} \leq hn \implies |A| < (h \cdot h! n)^{1/h}.$$

De manera análoga, en el caso de un grupo finito G con n elementos tenemos que

$$\frac{|A|^h}{h!} < \binom{|A|+h-1}{h} \leq n \implies |A| < (h!n)^{1/h}.$$

Es decir,

$$F_h(n) < (h \cdot h!n)^{1/h}$$

y

$$F_h(G) < (h!|G|)^{1/h}.$$

Por otro lado se conocen tres construcciones de conjuntos B_h en $\{1,\dots,n\}$ tamaño $\sim n^{1/h}$. Las dos primeras [6] son una generalización de los conjuntos de Sidon de Singer y Bose y la tercera es una generalización, obtenida por Carlos Alexis Gómez y Carlos Trujillo [34], que combina las ideas de la construcción de Ruzsa para $h=2$ con la de Bose-Chowla para $h \geq 2$. Estas construcciones prueban las siguientes cotas inferiores:

$$\begin{aligned} F_h(\mathbb{Z}_{q^h-1}) &\geq q \\ F_h(\mathbb{Z}_{q^h+\cdots+q+1}) &\geq q+1 \\ F_h(\mathbb{F}_{q^{h-1}} \times \mathbb{Z}_{q-1}) &\geq q-1. \end{aligned}$$

En [34] se da una presentación unificada de estas tres construcciones. Aquí seguimos [34] para exponer la construcción de Bose-Chowla, que es la más sencilla de todas ellas.

Teorema 1.4.1 (Bose-Chowla)**.** *Sea $\mathbb{F}_{q^h}$ un cuerpo de q^h elementos y sea θ un generador del grupo multiplicativo $\mathbb{F}_{q^h}^*$. Entonces el conjunto*

$$A = \{\log_\theta(\theta + a) : \ a \in \mathbb{F}_q\}$$

es un conjunto B_h en $\mathbb{Z}_{q^h-1}$.

Demostración. Por ser θ un generador de $\mathbb{F}_{q^h}$, su polinomio minimal tiene grado h. Como consecuencia de esto vamos a ver que el conjunto

$$\theta + \mathbb{F}_q = \{\theta + a : \ a \in \mathbb{F}_q\}$$

es un conjunto B_h multiplicativo en $\mathbb{F}_{q^h}^*$. Supongamos que no es así y que se da la igualdad entre dos productos de h elementos de $\theta + \mathbb{F}_q$:

$$\prod_{i=1}^{h} (\theta + a_i) = \prod_{i=1}^{h} \left(\theta + a_i'\right)$$

con $\{a_1, \ldots, a_h\} \neq \{a_1', \ldots, a_h'\}$. En ese caso el polinomio

$$\prod_{i=1}^{h} (X + a_i) - \prod_{i=1}^{h} \left(X + a_i'\right),$$

que es de grado menor que h, se anula en θ lo que contradice que el polinomio mínimo de θ es de grado h. Una vez visto que $\theta + \mathbb{F}_q$ es un conjunto de Sidon multiplicarico, es claro que el conjunto

$$A = \{\log_\theta(\theta + a) : \ a \in \mathbb{F}_q\}$$

es un conjunto B_h en $\mathbb{Z}_{q^h-1}$. □

Razonando de la misma manera que lo hicimos para obtener la cota inferior sobre $F_2(n)$ a partir de construcciones de conjuntos de Sidon en grupos cíclicos, tenemos que

$$n^{1/h}(1 + o(1)) \leq F_h(n) \leq (h \cdot h!)^{1/h}.$$

Con argumentos puramente combinatorios se puede mejorar la cota superior. Lindstrom [45] lo hizo por primera vez para sucesiones B_4 demostrando que $F_4(n) \leq (8n)^{1/4}(1 + o(1))$ y fue generalizado por otros autores [39, 24] para todo $h \geq 3$.

Teorema 1.4.2.

$$\begin{aligned} F_{2h-1}(n) &\leq (h!^2 n)^{1/(2h-1)}(1 + o(1)) \\ F_{2h}(n) &\leq (h \cdot h!^2 n)^{1/(2h)}(1 + o(1)). \end{aligned}$$

Una demostración más sencilla que las originales se puede obtener a partir de los dos ejercicios siguientes.

Ejercicio 1.4.2. *Demostrar que si $A \subset [1, n]$ es un conjunto B_{2h} entonces el conjunto $C = A + \overset{h}{\cdots} + A$ satisface que $|C - C| \sim |C|^2$.*

Ejercicio 1.4.3. *Combinar el ejercicio anterior y el Teorema 1.2.3 para demostrar que si $A \subset [1,n]$ es un conjunto B_{2h} entonces*

$$|A| \leq (1+o(1)) \left(h!^2 \cdot hn\right)^{1/(2h)}.$$

Todavía existen ligeras mejoras sobre estas cotas. Cuando h es grande, se puede sacar partido de que las sumas $a_1 + \cdots + a_h$ tenderán a estar concentradas sobre su media. Resultados en esta dirección aparecen en [26] y mejoras posteriores aparecen en [60, 11, 33]. Para h pequeño se puede utilizar análisis de Fourier para sacar partido del hecho de que los elementos de un conjunto suma $A+A$ no pueden estar bien distribuido en intervalos. Esta estrategia, basada en parte en las ideas de [19], aparecen en [11] y [33]. En particular Ben Green [33] ha demostrado que $F_4(n) \leq (7n)^{1/4}(1+o(1))$.

Capítulo 2

Sucesiones de Sidon infinitas

La manera de cuantificar el tamaño de una sucesión infinita A de enteros positivos es a través de su función contadora

$$A(x) = |A \cap [1, x]|,$$

que cuenta el número de términos de la sucesión menores o iguales que x. En lo que se refiere a sucesiones de Sidon infinitas, el principal objetivo consiste en construir sucesiones de Sidon infinitas que tengan una función contadora tan grande como sea posible.

Es fácil construir sucesiones infinitas de Sidon. Por ejemplo la sucesión de las potencias de 2 es una sucesión de Sidon porque todas las sumas de dos potencias de 2 son distintas. Pero esta sucesión no es muy interesante. Es muy poco densa, crece demasiado deprisa. Su función contadora es $A(x) \sim \log_2 x$.

La construcción más ingenua de un conjunto de Sidon con una función contadora decente es la generada por el algoritmo voraz. Consiste en empezar con $a_1 = 1,\ a_2 = 2$, y una vez construidos $a_1, ..., a_{n-1}$, añadir el menor entero positivo a_n que no viole la condición de ser de Sidon; es decir, el siguiente que no sea de la forma $a_i - a_j + a_k,\ 1 \leq i, j, k \leq n-1$. Los primeros términos de esta sucesión, introducida por Erdős

pero conocida como sucesión de Mian-Chowla, son los siguientes:

$$1, 2, 4, 8, 13, 21, 31, 45, 66, 81, 97, 123, 148, 182, 204, 252, 290, ...$$

Aunque se desconoce cómo crece realmente esta sucesión, como a lo más hay $(n-1)^3$ enteros prohibidos de la forma

$$a_i - a_j + a_k,\ 1 \le i, j, k \le n-1,$$

siempre es cierto que $a_n \le (n-1)^3 + 1$, lo que nos permite seleccionar un conjunto de Sidon en $\{1, ..., m\}$ con $m^{1/3}$ elementos por lo menos. Es decir la función contadora de la sucesión voraz de Sidon satisface $A(x) \gg x^{1/3}$.

Se desconoce cuál es el verdadero comportamiento de la función contadora de esta sucesión. Los datos computacionales sugieren que $A(x)/x^{1/3} \to \infty$ y de hecho existe un modelo heurístico bastante sólido [8] y avalado por los datos computacionales, que permite conjeturar que

$$A(x) \sim c(x \log x)^{1/3},$$

donde c es una constante explícita cuyo valor aproximado es $c = 1{,}7107\ldots$.

2.1. Crecimiento de las sucesiones de Sidon infinitas

Es claro que si A es una sucesión de Sidon infinita entonces el conjunto formado por elementos hasta x es un conjunto de Sidon finito en el intervalo $[1, x]$. De la cota superior trivial (1.1) para el máximo tamaño de un conjunto de Sidon en $[1, x]$ se obtiene:

$$A(x) \le \sqrt{2x} + 1/2. \tag{2.1}$$

En principio podríamos pensar que pudiera existir una sucesión de Sidon infinita con $A(x) \gg x^{1/2}$, de manera análoga a lo que ocurre en el caso finito. Sin embargo Erdős demostró que tal sucesión no puede existir. En [63] aparece el siguiente resultado.

Teorema 2.1.1 (Erdős)**.** *Si A es una sucesión de Sidon entonces*

$$\liminf_{x\to\infty} A(x) \left(\frac{\log x}{x}\right)^{1/2} \ll 1.$$

Demostración. Dividimos el intervalo $[1, N^2]$ en N intervalos de longitud N:

$$I_l = ((l-1)N + 1, lN], \qquad l = 1, \ldots, N$$

y llamamos

$$D_l = |A \cap I_l| = A(lN) - A((l-1)N)$$

al número de elementos de A en I_l. Contando las diferencias positivas de todas las parejas de dos elementos pertenecientes a un mismo intervalo tenemos que

$$\sum_{l=1}^{N} \binom{D_l}{2} \leq N$$

debido a que todas las diferencias que estamos contando son distintas y menores que N. Manipulando esta desigualdad y utilizando la estimación

$$A(N^2) \leq 2N + 1/2$$

vista en (2.1), llegamos a la desigualdad

$$\sum_{l=1}^{N} D_l^2 \leq 2N + 2\sum_{l=1}^{N} D_l = 2N + 2A(N^2) \leq 7N. \tag{2.2}$$

Aplicando la desigualdad de Cauchy-Schwarz y utilizando (2.2) y la parte derecha de la desigualdad

$$\log N \leq \sum_{l=1}^{N} \frac{1}{l} \leq 2 \log N \tag{2.3}$$

para $N \geq 3$, obtenemos

$$\sum_{l=1}^{N} \frac{D_l}{\sqrt{l}} \leq \left(\sum_{l=1}^{N} D_l^2\right)^{1/2} \left(\sum_{l=1}^{N} \frac{1}{l}\right)^{1/2} \leq \sqrt{14N \log N}. \tag{2.4}$$

Por otra parte, sumando por partes y utilizando la desigualdad

$$\frac{1}{\sqrt{l}} - \frac{1}{\sqrt{l+1}} \geq \frac{1}{4l^{3/2}}$$

para $l \geq 1$ obtenemos

$$\begin{aligned}\sum_{l=1}^{N} \frac{D_l}{\sqrt{l}} &= \sum_{l=1}^{N} \frac{A(lN) - A((l-1)N)}{\sqrt{l}} \\ &= \frac{A(N^2)}{\sqrt{N+1}} + \sum_{l=1}^{N} A(lN)\left(\frac{1}{\sqrt{l}} - \frac{1}{\sqrt{l+1}}\right) \\ &\geq \frac{1}{4}\sum_{l=1}^{N} \frac{A(lN)}{l^{3/2}}.\end{aligned}$$

Si definimos

$$\tau_N = \inf_{t \geq N} A(t)\left(\frac{\log t}{t}\right)^{1/2},$$

es claro que $A(lN) \geq \tau_N \left(\frac{lN}{\log(lN)}\right)^{1/2}$ para todo $l \geq 1$. Así que

$$\begin{aligned}\sum_{l=1}^{N} \frac{D_l}{\sqrt{l}} &\geq \tau_N \left(\frac{N}{\log(N^2)}\right)^{1/2} \frac{1}{4}\sum_{l=1}^{N} \frac{1}{l} \\ &\geq \tau_N \left(\frac{N}{\log N}\right)^{1/2} \frac{1}{4\sqrt{2}}\sum_{l=1}^{N} \frac{1}{l} \\ &\geq \tau_N \frac{(N\log N)^{1/2}}{4\sqrt{2}},\end{aligned}$$

donde en el último pase se ha utilizado la parte izquierda de la desigualdad 2.8. Esta desigualdad y (2.4) prueban que $\tau_N \leq 8\sqrt{7}$ por lo tanto que

$$\liminf_{x\to\infty} A(x)\left(\frac{\log x}{x}\right)^{1/2} \leq \lim_{N\to\infty} \tau_N \leq 8\sqrt{7}.$$

□

Ejercicio 2.1.1. *Refinar la demostración del Teorema 2.1.1 para demostrar que si A es una sucesión de Sidon infinita entonces*

$$\liminf_{x\to\infty} A(x)\left(\frac{\log x}{x}\right)^{1/2} \leq 4.$$

El siguiente ejercicio es interesante porque muestra que se puede llegar a una conclusión similar a la del Teorema 2.1.1 asumiendo solo que $|A_x - A_x| \sim |A_x|^2$. Curiosamente no sabemos si la conclusión también es cierta asumiendo que $|A_x + A_x| \sim |A_x|^2/2$.

Ejercicio 2.1.2. *Sea A una sucesión de enteros positivos y para cada x consideremos el conjunto $A_x = A \cap [1, x]$. Demostrar que si*

$$|A_x - A_x| \sim |A_x|^2$$

entonces

$$\liminf_{x\to\infty} \frac{|A_x|}{\sqrt{x}} = 0.$$

El Teorema 2.1.1 ha sido generalizado [23] para sucesiones B_{2h} combinando la estrategia del Teorema 2.1.1 con el hecho de que el conjunto $hA = A + \overset{h}{\cdots} + A$ es "casi" un conjunto de Sidon.

Teorema 2.1.2 (Chen)**.** *Si A es una sucesión B_{2h} entonces*

$$\liminf_{n\to\infty} A(n) \left(\frac{\log n}{n}\right)^{\frac{1}{2h}} \ll 1.$$

Se desconoce si $\liminf_{x\to\infty} A(x)/x^{1/h} = 0$ cuando A es una sucesión B_h y h es impar. En relación con este problema, Helm [38] ha demostrado que no existe ninguna sucesión B_3 infinita con comportamiento asintótico de la forma $A(x) \sim cx^{1/3}$.

Como contrapunto al Teorema 2.1.1 Erdős demostró que existe una sucesión infinita de Sidon con $\limsup_{x\to\infty} A(x)/\sqrt{x} = 1/2$. Este resultado fue mejorado por Krukenberger [42].

Teorema 2.1.3 (Krukenberger)**.** *Existe una sucesión infinita de Sidon A con*

$$\limsup_{x\to\infty} \frac{A(x)}{\sqrt{x}} \geq \frac{1}{\sqrt{2}}.$$

Demostración. Sea $m_j = 2^{4^j}$. Para cada intervalo

$$I_j = (m_j + 2m_{j-1}, 2m_j]$$

consideremos un conjunto de Sidon $A_j \subset I_j$ de tamaño maximal

$$|A_j| \sim (m_j - 2m_{j-1})^{1/2} \sim m_j^{1/2}.$$

La última estimación asintótica se debe a que $m_{j-1} = o(m_j)$. Al conjunto A_j le quitamos ahora todos los elementos a para los que exista un $a' \in A_j$ con $0 < a - a' \leq 2m_{j-1}$. Como A_j es de Sidon, existen a lo más $2m_{j-1}$ de estos elementos a. Así que el conjunto A_j^* resultante tendrá todavía

$$|A_j^*| \geq |A_j| - 2m_{j-1} \sim m_j^{1/2}$$

elementos porque de nuevo $m_{j-1} = o\left(m_j^{1/2}\right)$. Veamos que la sucesión infinita

$$A = \bigcup_j A_j^*$$

satisface las condiciones del teorema.

Veamos primero que A es un conjunt de Sidon. Supongamos que $a_1 + a_2 = a_1' + a_2'$ con $a_1 > a_1' \geq a_2' \geq a_2$ y todos ellos pertenecientes al conjunto A . Supongamos que $a_1 \in A_j^*$. Veamos que necesariamente $a_1' \in A_j^*$. Si no fuera así entonces

$$a_1 = a_1' + a_2' - a_2 \leq a_1' + a_2' \leq 2 \cdot 2m_{j-1} < m_j,$$

lo que contradice el hecho de que $a_1 \in A_j^*$.

Veamos que también $a_2' \in A_j^*$. Es claro que $a_2' = a_1 - a_1' + a_2 > a_1 - a_1' > 2m_{j-1}$, debido a que hemos destruido, por construcción, la posibilidad de que $a_1 - a_1' \leq 2m_{j-1}$. Eso implica que $a_2' \in A_j^*$.

Por último veamos que $a_2 \in A_j^*$. Escribimos

$$a_2 = a_1' + a_2' - a_1 > 2(m_j + 2m_{j-1}) - 2m_j = 4m_{j-1},$$

que en particular implica que $a_2 \in A_j^*$. Pero como A_j^* es un conjunto de Sidon, no es posible que los cuatro elementos de la identidad $a_1 + a_2 = a_1' + a_2'$ pertenezcan a A_j^*.

Una vez visto que A es de Sidon vayamos con el límite superior.

$$\frac{A(2m_j)}{(2m_j)^{1/2}} \geq \frac{|A_j^*|}{(2m_j)^{1/2}} \sim \frac{m_j^{1/2}}{(2m_j)^{1/2}} = \frac{1}{\sqrt{2}},$$

y por lo tanto,

$$\limsup_{x\to\infty} \frac{A(x)}{x^{1/2}} \geq \limsup_{j\to\infty} \frac{A(2m_j)}{(2m_j)^{1/2}} \geq \frac{1}{\sqrt{2}}.$$

□

Erdős se preguntaba si podría haber una sucesión infinita de Sidon tal que

$$\limsup_{x\to\infty} A(x)/\sqrt{x} = 1.$$

La constante 1 claramente no puede ser sustituida por una más grande porque, como hemos visto en el primer capítulo, siempre se tiene la cota superior $A(x) \leq \sqrt{x}(1 + o(1))$. Una respuesta afirmativa al siguiente problema de Erdős implicaría la existencia de una sucesión infinita de Sidon con $\limsup_{x\to\infty} A(x)/\sqrt{x} = 1$.

Problema (Erdős): Sean $b_1, \ldots, b_k$ enteros positivos que forman un conjunto de Sidon. ¿Existirán infinitos conjuntos de Sidon $A_n \subset [1, n]$ de tamaño $|A_n| \sim \sqrt{n}$ y que contengan a $b_1, \ldots, b_k$?

Ejercicio 2.1.3. *Demostrar que una respuesta afirmativa a la pregunta de Erdős implicaría la existencia de una sucesión infinita de Sidon A con* $\limsup_{x\to\infty} A(x)/\sqrt{x} = 1$.

2.2. Construcción de sucesiones de Sidon infinitas

La sucesión (a_n) generada por el algoritmo avaricioso (la sucesión de Mian-Chowla) es la construcción más sencilla de una sucesión de Sidon infinita. Ya vimos en el capítulo anterior que $a_n \leq (n-1)^3 + 1$, lo que implica que $A(x) \gg x^{1/3}$. Esta construcción fue durante 50 años la mejor de la que se disponía hasta que en 1981 Ajtai, Komlos y Szemerédi [2] demostraron la existencia de una sucesión infinita de Sidon con $A(x) \gg (x \log x)^{1/3}$.

Este resultado fue dramáticamente mejorado por Ruzsa [55] al demostrar la existencia de una sucesión infinita de Sidon con $A(x) =$

$x^{\sqrt{2}-1+o(1)}$. La demostración de Ruzsa es muy ingeniosa. Ruzsa observó que los primos forman una sucesión de Sidon multiplicativa y por lo tanto la sucesión $\{\log p\}$ es una sucesión de Sidon de números reales.

A grandes rasgos la demostración de Ruzsa es como sigue. Considera un parámetro $\alpha \in [1,2]$ y para cada α construye una sucesión $B_\alpha = \{b_p\}$ indexada en los primos donde cada b_p se construye a partir de los dígitos del desarrollo binario de $\alpha \log p$. Lo que Ruzsa demuestra es que para casi todo $\alpha \in [1,2]$ la sucesión B_α es "casi"de Sidon en el sentido de que podemos eliminar unos pocos términos de B_α para conseguir que la sucesión resultante sea de Sidon.

El siguiente ejercicio se puede considerar como la versión finita de la construcción de Ruzsa.

Ejercicio 2.2.1. Demostrar que el conjunto

$$A = \{\lfloor n \log(4p/\sqrt{n})\rfloor : \ \sqrt{n}/4 < p \leq \sqrt{n}/2\}$$

es un conjunto de Sidon en el intervalo $[1,n]$ de tamaño $|A| \gg \frac{\sqrt{n}}{\log n}$.

Una construcción similar a la de Ruzsa se puede hacer también utilizando los argumentos de los primos de Gauss en lugar de los logaritmos de los primos racionales.

Ejercicio 2.2.2. Sea $\phi(\mathbf{p})$ el argumento del primo Gaussiano $\mathbf{p} = |\mathbf{p}|e^{i\phi(\mathbf{p})}$. Demostrar que el conjunto

$$A = \{\lfloor 4n\phi(\mathbf{p})\rfloor : \ |\mathbf{p}| < \sqrt{n}, |\phi(\mathbf{p})| < \pi/4\}$$

es un conjunto de Sidon en el intervalo $[1,4n]$ de tamaño $|A| \gg \frac{\sqrt{n}}{\log n}$.

Volviendo a las sucesiones de Sidon infinitas, Erdős ofreció 1000 dólares por la resolución de la siguiente conjetura, que sigue sin estar resuelta.

Conjetura 2.2.1. *Para todo $\epsilon > 0$ existe una sucesión infinita de Sidon con $A(x) \gg x^{1/2-\epsilon}$.*

El Teorema 2.1.1 muestra que esta conjetura no es cierta para $\epsilon = 0$. Tanto las construcciones de Ajtai, Komlos y Szemerédi como la de Ruzsa son construcciones probabilísticas. No son explícitas. Recientemente Cilleruelo [13] ha encontrado una construcción explícita de una sucesión infinita de Sidon con función contadora similar a la de Ruzsa.

Teorema 2.2.1 (Cilleruelo [13])**.** *Existe una sucesión de Sidon infinita A, que puede ser descrita explícitamente, con función contadora*

$$A(x) = x^{\sqrt{2}-1+o(1)}. \tag{2.5}$$

En esta sección nos dedicaremos a demostrar el Teorema 2.2.1 construyendo, de manera explícita, la sucesión de Sidon infinita a la que hace referencia el teorema.

2.2.1. El método del logaritmo discreto

La principal dificultad para construir sucesiones de Sidon infinitas densas reside en que las construcciones finitas que se han visto en el primer capítulo, provienen todas ellas de construcciones algebraicas en grupos finitos y no se sabe cómo extenderlas a sucesiones infinitas. La siguiente construcción de un conjunto finito de Sidon (en general de un conjunto B_h) es una construcción que podemos denominar semialgebraica en el sentido de que, aunque el grupo ambiente es $\mathbb{Z}_{q-1}$ (la parte algebraica), los elementos se describen a partir de los primos racionales. El tamaño de estos conjuntos de Sidon es menor (por un factor logarítmico) que el de los conjuntos de Sidon de procedencia algebraica, pero éstos ofrecen una mayor flexibilidad a la hora de extenderlos a una sucesión infinita.

Teorema 2.2.2. *Sea q un primo y g un generador de $\mathbb{F}_q^*$. El conjunto*

$$A = \{x : \ g^x \equiv p \text{ para algún primo } p \leq q^{1/h}\}$$

es un conjunto B_h en $\mathbb{Z}_{q-1}$ con $\pi(q^{1/h})$ elementos.

Demostración. Supongamos que

$$x_1 + \cdots + x_h = y_1 + \cdots + y_h \pmod{q-1}$$

con $x_1, \ldots, x_h, y_1, \ldots, y_h \in A$. En ese caso tenemos que

$$g^{x_1} \cdots g^{x_h} \equiv g^{y_1} \cdots g^{y_h} \pmod{q}$$

y por construcción

$$p_1 \cdots p_h \equiv p_1' \cdots p_h' \pmod{q}.$$

Como tanto el lado derecho como el izquierdo son menores que q, la congruencia es en realidad una igualdad en enteros

$$p_1 \cdots p_h = p'_1 \cdots p'_h$$

y el teorema fundamental de la aritmética implica que $\{p_1, \ldots, p_h\} = \{p'_1, \ldots, p'_h\}$, que a su vez implica que $\{x_1, \ldots, x_h\} = \{y_1, \ldots, y_h\}$. □

El conjunto A también podía haber sido descrito de la forma

$$A = \{\log_g p : \ p \text{ primo }, \ p \leq q^{1/h}\},$$

donde $\log_g p$ es el logaritmo discreto de x en base g.

Esta construcción fue la que inspiró la construcción de la sucesión de Sidon infinita que pasamos a describir.

2.2.2. Bases generalizadas

La manera de representar los números en una base dada (normalmente la base 10) es algo bien conocido por todos. Este hecho se puede generalizar de la manera siguiente.

Dada una sucesión de enteros positivos $2 \leq b_1 \leq \cdots \leq b_j \leq \ldots$ (la base), todo entero no negativo se puede escribir de manera única de la forma

$$a = x_1 + x_2 b_1 + \cdots + x_j b_1 \cdots b_{j-1} + \cdots$$

donde los x_i (los dígitos) son enteros tales que $0 \leq x_i < b_i$.

Ejercicio 2.2.3. *Utilizar el algoritmo de Euclides para demostrar la afirmación anterior sobre las bases generalizadas.*

La base en la que expresaremos los elementos de nuestra sucesión será de la forma

$$\overline{q} := 4q_1, \ldots, 4q_i, \ldots$$

donde los q_i son primos que satisfacen la desigualdad

$$2^{2i-1} < q_i \leq 2^{2i+1}.$$

Es claro que todo entero positivo a se puede expresar, de manera única de la forma

$$a = x_1 + x_2(4q_1) + \cdots + x_i(4q_1 \cdots 4q_{i-1}) + \cdots$$

donde los x_i (los dígitos) son enteros tales que $0 \leq x_i < 4q_i$. El factor 4 aparece en los elementos de la base por razones técnicas que se verán más adelante.

Fijada la base, representamos cada entero a mediante sus dígitos:

$$a := \cdots x_k \cdots x_1.$$

La ventaja de representar los enteros mediante dígitos es que podemos ver los enteros como si fueran vectores. Este hecho había sido utilizado anteriormente por otros autores.

Una observación importante es la siguiente. Supongamos que los dígitos de los enteros de nuestra sucesión satisfacen la desigualdad

$$q_i < x_i < 2q_i \tag{2.6}$$

y sean a, a' dos elementos de dicha sucesión, con dígitos

$$\begin{aligned} a &= x_k \ldots\ldots x_1 \\ a' &= \quad x'_j \ldots x'_1. \end{aligned}$$

Como $x_i + x'_i < 4q_i$ para todo i, los dígitos de $a + a'$ en la base $\overline{q} := 4q_1, \ldots, 4q_i, \ldots$ se pueden calcular sumando los dos dígitos de cada posición:

$$a + a' = (x_k + 0) \ldots (x_{j+1} + 0)(x_j + x'_j) \ldots (x_1 + x'_1) \tag{2.7}$$

Observar además que los dígitos en las posiciones $1, \ldots, j$ son todos mayores que $2q_i$ y que el resto son menores que $2q_i$. Es decir, los dígitos de $a+a'$ determinan el número de dígitos de a y a' cuando éstos satisfacen (2.6).

Vamos a describir los elementos de nuestra sucesión en una base como la descrita y de tal manera que los dígitos de los elementos van a satisfacer la desigualdad $q_i < x_i < 2q_i$. De esta manera podremos sacar ventaja de la observación que acabamos de hacer.

2.2.3. La distribución de los números primos

La sucesión que vamos a construir va a estar indexada con la sucesión de los números primos. Por esa razón es conveniente recordar cómo se distribuyen los números primos en la sucesión de los enteros. La función $\pi(x)$ es la que cuenta el número de primos menores o iguales que x.

Uno de los teoremas fundamentales de la teoría de números es el teorema de los números primos que nos habla del comportamiento asintótico de la función $\pi(x)$.

Teorema 2.2.3 (Teorema de los números primos)**.** *Cuando $x \to \infty$ se tiene que*

$$\pi(x) \sim \frac{x}{\log x}.$$

El teorema de los números primos, pronosticado por matemáticos como Gauss y Riemann, fue demostrado independientemente por Jacques Hadamard y Charles-Jean de la Vallée Poussin en 1896.

2.2.4. Una sucesión de Sidon infinita explícita

Empezaremos la construcción de la sucesión A del Teorema 2.2.1 indicando en qué base vamos a expresar sus elementos:

La base. Fijamos una sucesión de primos (q_i) con

$$2^{2i-1} < q_i < 2^{2i+1} \tag{2.8}$$

y consideramos la base generalizada

$$\overline{q} := 4q_1, \dots, 4q_i, \dots$$

Es esta base la que utilizaremos para describir, mediante sus dígitos, los elementos de la sucesión infinita de Sidon A del Teorema 2.2.1.

Por comodidad utilizaremos la notación

$$Q_k = \prod_{i=1}^{k} q_i$$

para indicar el producto de los primeros k primos de esa sucesión. Por (2.8) es claro que

$$2^{k^2} < Q_k < 2^{(k+1)^2}. \tag{2.9}$$

El conjunto de índices: Vamos a enumerar los elementos de nuestra sucesión utilizando el conjunto de los primos $\mathcal{P}$ como conjunto de índices.

$$A = (a_p)_{p\in\mathcal{P}}$$

y representaremos cada elemento mediante sus dígitos en la base $\overline{q}$:

$$a_p = \cdots x_k(p)\cdots x_1(p).$$

La función contadora: Para determinar el número de dígitos de cada elemento, que será lo que a su vez determine el crecimiento de la sucesión, fijamos un número real $c,\ 0 < c < 1/2$ (que acabará siendo el exponente en la función contadora de A), y consideramos la siguiente partición de los números primos:

$$\mathcal{P} = \bigcup_{k\geq 2} \mathcal{P}_k,$$

donde

$$\mathcal{P}_k = \left\{ p \text{ primo} : \ \frac{Q_{k-1}^c}{k-1} < p \leq \frac{Q_k^c}{k} \right\}.$$

En la sucesión que construiremos los elementos a_p con $p \in \mathcal{P}_k$ tendrán exactamente k dígitos. El cálculo del número de elementos de $\mathcal{P}_k$ lo dejamos como ejercicio.

Ejercicio 2.2.4. *Demostrar que*

$$|\mathcal{P}_k| \asymp \frac{Q_k^c}{k^3}. \tag{2.10}$$

Al final de la demostración tomaremos $c = \sqrt{2} - 1$, pero ahora preferimos escribir simplemente c para que se aprecie en la demostración por qué no es posible tomar otro valor mayor.

Lema 2.2.1. *Sea $A = (a_p)$ una sucesión indexada con los primos. Supongamos que todos los elementos a_p con $p \in \mathcal{P}_k$ tienen exactamente k dígitos. Entonces*

$$A(x) = x^{c+o(1)}.$$

Demostración. Consideremos, para cada x, el entero k tal que

$$4^k Q_k < x \leq 4^{k+1} Q_{k+1}. \tag{2.11}$$

De (2.9) se sigue que fácilmente que

$$x = 2^{k^2(1+o(1))}. \tag{2.12}$$

Observemos que si $p \leq \frac{Q_k^c}{k}$ entonces $p \in \mathcal{P}_j$ para algún $j \leq k$. Eso quiere decir que

$$a_p = x_1 + x_2(4q_1) + \cdots + x_j(4q_1 \cdots 4q_{j-1})$$

para algunos $0 \leq x_i \leq q_i - 1,\ 1 \leq i \leq j$. En particular

$$a_p \leq (4q_1)\cdots(4q_j) \leq (4q_1)\cdots(4q_k) = 4^k Q_k < x$$

y por lo tanto $A(x) \geq \pi(Q_k^c/k)$. Finalmente el teorema de los números primos y (2.12) implican la desigualdad

$$\pi(Q_k^c/k) \geq \pi(2^{ck^2}/k) \gg 2^{ck^2}/k^3 = 2^{ck^2(1+o(1))} = x^{c+o(1)}.$$

Para la cota superior observemos que si $p > \frac{Q_{k+1}^c}{k+1}$ entonces $p \in \mathcal{P}_j$ para algún $j \geq k+2$ y entonces

$$a_p > (4q_1)\cdots(4q_{j-1}) \geq (4q_1)\cdots(4q_{k+1}) = 4^{k+1}Q_{k+1} \geq x.$$

Es decir, $A(x) \leq \pi\left(Q_{k+2}^c/(k+2)\right)$. De nuevo tenemos

$$\pi(Q_{k+2}^c/(k+2)) \leq Q_{k+2}^c = 2^{k^2(1+o(1))} = x^{c+o(1)}.$$

□

Los dígitos: Para terminar de describir nuestra sucesión

$$A = (a_p)_{p\in\mathcal{P}}$$

tenemos que decir quiénes son los dígitos de cada elemento a_p en nuestra base $\overline{q}$.

Cada entero a_p con $p \in P_k$ va a ser un entero $a_p = x_k \ldots x_1$ con exactamente k dígitos en nuestra base, lo que garantiza, gracias al Lema 2.2.1 que la función contadora de la sucesión satisface $A(x) = x^{c+o(1)}$.

El dígito $x_i(p)$, para $i \leq k$, es la solución de la congruencia

$$g_i^{x_i(p)} \equiv p \pmod{q_i}, \qquad q_i + 1 \leq x_i(p) \leq 2q_i - 1 \tag{2.13}$$

donde g_i es un generador del grupo multiplicativo $\mathbb{F}_{q_i}^*$, que habremos fijado previamente para cada q_i. Definimos $x_i(p) = 0$ for $i > k$.

Es decir, si $p \in \mathcal{P}_k$, los dígitos de a_p en la base $\overline{q} := 4q_1, \ldots, 4q_i, \ldots$ son

$$a_p = x_k x_{k-1} \cdots x_2 x_1,$$

donde los $x_i = x_i(p),\ i = 1, \ldots, k$ han sido definidos en (2.13).

Utilizaremos la notación A_c para designar a nuestra sucesión y enfatizar la dependencia de c. La siguiente proposición concierne a las propiedades de Sidon de la sucesión A_c.

Proposición 2.2.1. *Supongamos que existen $a_{p_1}, a_{p_2}, a_{p_1'}, a_{p_2'} \in A_c$ con $a_{p_1} > a_{p_1'} \geq a_{p_2'} > a_{p_2}$ y tales que*

$$a_{p_1} + a_{p_2} = a_{p_1'} + a_{p_2'}.$$

Entonces tenemos que:

i) existen $j, k,\ j \leq k$ tales que $p_1, p_1' \in \mathcal{P}_k,\ p_2, p_2' \in \mathcal{P}_j$.

ii) $p_1 p_2 \equiv p_1' p_2'$ (mód Q_j)

iii) $p_1 \equiv p_1'$ (mód Q_k/Q_j).

iv) $Q_k^{1-c} < Q_j < Q_k^{\frac{c}{1-c}}$.

Demostración. Como $0 \leq x_j(p_1) + x_j(p_2) < 4q_j$ para todo j, la igualdad $a_{p_1} + a_{p_2} = a_{p_1'} + a_{p_2'}$ implica que los dígitos de ambas sumas son iguales:

$$x_j(p_1) + x_j(p_2) = x_j(p_1') + x_j(p_2') \tag{2.14}$$

para todo j. Por construcción y la observación (2.7) podemos ver que $p_1 \in \mathcal{P}_k$ y $p_2 \in \mathcal{P}_j$ donde k es el mayor entero para el que

$$x_k(p_1) + x_k(p_2) \geq q_k + 1$$

y j es el mayor para el que

$$x_j(p_1) + x_j(p_2) \geq 2q_j + 2.$$

Esta observación prueba la parte i). Para probar ii) y iii) observemos que (2.14) implica que para todo i tenemos

$$g_i^{x_i(p_1)+x_i(p_2)} \equiv g_i^{x_i(p_1')+x_i(p_2')} \pmod{q_i}.$$

También sabemos que si $p \in \mathcal{P}_k$, entonces

$$g_i^{x_i(p)} \equiv p \pmod{q_i},\ i \le k \tag{2.15}$$

$$g_i^{x_i(p)} \equiv 1 \pmod{q_i},\ i > k. \tag{2.16}$$

Así que $p_1p_2 \equiv p_1'p_2'$ (mód q_i) para todo $i \le j$. Esta observación y el teorema chino del resto implica la congruencia en ii)

$$p_1p_2 \equiv p_1'p_2' \pmod{Q_j}.$$

Como $p_1p_2 \neq p_1'p_2'$, entonces $|p_1p_2 - p_1'p_2'| \ge Q_j$. Por otra parte, como $p_1, p_1' \in \mathcal{P}_k$ y $p_2, p_2' \in \mathcal{P}_j$ tenemos que $p_1p_2 \le Q_k^cQ_j^c$ y tenemos la desigualdad

$$Q_k^cQ_j^c > |p_1p_2 - p_1'p_2'| \ge Q_j \Longrightarrow Q_j < Q_k^{\frac{c}{1-c}}. \tag{2.17}$$

En particular se tiene que $j < k$ porque $c < 1/2$. Las congruencias (2.15) implican que $p_1 \equiv p_1'$ (mód q_i) para todo i con $j+1 \le i \le k$. El teorema chino del resto implica la congruencia

$$p_1 \equiv p_1' \pmod{Q_k/Q_j}.$$

Procediendo como antes obtenemos la desigualdad

$$Q_k^c > |p_1 - p_1'| \ge Q_k/Q_j \Longrightarrow Q_j > Q_k^{1-c}. \tag{2.18}$$

Las desigualdades (2.17) y (2.18) implican iv). □

Observemos que si hubiera sumas repetidas, entonces la proposición 3.4.3, iv) implicaría $1 - c < \frac{c}{1-c}$, lo cual no es cierto para $c = \frac{3-\sqrt{5}}{2} =$ 0,38... Así que la sucesuón A_c es una sucesión de Sidon para este valor de c, que es mayor que $1/3$. Esta observación nos proporciona el siguiente corolario.

Corolario 2.2.1. *La sucesión $A = A_c$ con $c = \frac{3-\sqrt{5}}{2}$ es una sucesión infinita de Sidon con función contadora $A(x) = x^{\frac{3-\sqrt{5}}{2}+o(1)}$.*

Si $c > \frac{3-\sqrt{5}}{2}$ ya no es cierto que A_c vaya a ser una sucesión de Sidon. Aparecerán infinitas sumas que se repiten. Pero si aparecen con poca frecuencia podemos eliminar los elementos de A_c involucrados en esas sumas para así obtener una verdadera sucesión de Sidon. Por supuesto hay que controlar que los elementos que vamos a descartar no sean demasiados para que eso no afecte demasiado al orden de la función contadora de la nueva sucesión. Eso lo vamos a poder hacer para todo $c \leq \sqrt{2}-1$ y esa es la estrategia que seguiremos para demostrar el Teorema 2.2.1.

Consideremos la sucesión

$$A_c^* = (a_p)_{p\in\mathcal{P}^*}$$

donde los números a_p se definen como antes pero ahora $\mathcal{P}^*$ es el conjunto de los primos que quedan después de eliminar de cada $\mathcal{P}_k$ un subconjunto $\mathcal{R}_k$ con el propósito de evitar la presencia de algunas sumas repetidas que pudieran aparecer. Para que no parezca extraña la definición de los conjuntos $\mathcal{R}_k$, esperaremos a que la propia demostración nos diga quiénes tienen que ser estos conjuntos. En cualquier caso sea

$$\mathcal{P}^* = \bigcup_k (\mathcal{P}_k \setminus \mathcal{R}_k)$$

donde los conjuntos de primos eliminados $\mathcal{R}_k$ los definiremos más adelante.

Vamos a demostrar que para $c = \sqrt{2}-1$, la sucesión $A_c^* = \{a_p\}_{p\in\mathcal{P}^*}$ es una sucesión infinita de Sidon con $A_c^*(x) = x^{\sqrt{2}-1+o(1)}$.

Para ver que A_c^* es una sucesión de Sidon, supongamos que

$$a_{p_1} + a_{p_2} = a_{p_1'} + a_{p_2'}$$

con $a_{p_1} > a_{p_1'} \geq a_{p_2'} > a_{p_2}$ y $p_1, p_1', p_2, p_2' \in \mathcal{P}^*$. La Proposition 2.2.1 implica que

$$p_1, p_1' \in \mathcal{P}_k \setminus \mathcal{R}_k \quad \text{y} \quad p_2, p_2' \in \mathcal{P}_j \setminus \mathcal{R}_j$$

para algún par de índices j, k que satisface $Q_j < Q_k^{\frac{c}{1-c}}$. Esta última restricción es consecuencia de la Proposición 3.4.3, iv).

Seguidamente observemos que gracias a las partes ii) and iii) de la Proposition 3.4.3 podemos escribir

$$p_1(p_2 - p_2') = s_1 Q_j + s_2 Q_k / Q_j$$

para los enteros no nulos

$$s_1 = \frac{p_1p_2 - p_1'p_2'}{Q_j}, \qquad s_2 = \frac{(p_1' - p_1)p_2'}{Q_k/Q_j},$$

los cuales satisfacen las desigualdades

$$1 \le |s_1| \le \frac{Q_j^c Q_k^c}{jkQ_j}, \quad 1 \le |s_2| \le \frac{Q_j^c Q_k^c Q_j}{jkQ_k}.$$

Esto implica que p_1 es un primo de $\mathcal{P}_k$ que divide a algún elemento s de alguno de los conjuntos

$$S_{j,k} = \left\{ s = s_1Q_j + s_2Q_k/Q_j : \ 1 \le |s_1| \le \frac{Q_j^c Q_k^c}{jkQ_j}, \ 1 \le |s_2| \le \frac{Q_j^c Q_k^c Q_j}{jkQ_k} \right\}$$

para algún j tal que $Q_j < Q_k^{\frac{c}{1-c}}$.

Ahora parece más claro cómo deberíamos definir el conjunto $\mathcal{R}_k$ al que hemos aludido al principio de la demostración. El conjunto $\mathcal{R}_k$ es el conjunto de los primos p_1 en $\mathcal{P}_k$ que dividen a algún elemento de algún $S_{j,k}$ para algún j tal que $Q_j < Q_k^{\frac{c}{1-c}}$.

De esta manera es claro que la sucesión A_c^* es de Sidon. Si hubiera una suma repetida $a_{p_1} + a_{p_2} = a_{p_1'} + a_{p_2'}$ con $p_1, p_1' \in \mathcal{P}_k$, $p_2, p_2' \in \mathcal{P}_j$ entonces tendríamos que $p_1 \in \mathcal{R}_k$ y por tanto $a_{p_1} \notin A_c^*$.

Para demostrar que $A_{q,c}^*(x) = x^{c+o(1)}$ sólo necesitamos probar que $|\mathcal{R}_k| = o(|\mathcal{P}_k|)$.

Primero veamos que para cada $s \in S_{j,k}$ y k suficientemente grande, existe a lo más un $p \in \mathcal{P}_k$ dividiendo a s. Si $p, p' \mid s$ tendríamos que

$$\frac{Q_{k-1}^{2c}}{(k-1)^2} < pp' \le |s| \le 2 \cdot \frac{Q_j^c Q_k^c}{jk} < \frac{Q_k^{\frac{c}{1-c}}}{k},$$

lo cual no puede ser cierto para k grande porque $2c > \frac{c}{1-c}$ para $c < 1/2$. Por lo tanto,

$$|S_{j,k}| \le \left(2 \cdot \frac{Q_j^c Q_k^c}{jkQ_j}\right)\left(\frac{Q_j^c Q_k^c Q_j}{jkQ_k}\right) \le 2\frac{Q_j^{2c} Q_k^{2c-1}}{j^2k^2}. \tag{2.19}$$

Utilizando (2.19), la identidad

$$\frac{2c^2}{1-c} + 2c - 1 = c$$

para $c = \sqrt{2} - 1$ y la estimación (2.10) en el último paso, tenemos, para k suficientemente grande, la estimación requerida,

$$\begin{aligned} |\mathcal{R}_k| &\leq \sum_{Q_j < Q_k^{\frac{c}{1-c}}} |S_{j,k}| \ll \sum_{Q_j < Q_k^{\frac{c}{1-c}}} \frac{Q_j^{2c} Q_k^{2c}}{j^2 k^2 Q_k} \\ &\ll \frac{Q_k^{\frac{2c^2}{1-c}+2c-1}}{k^4} = \frac{Q_k^c}{k^4} = o\left(|\mathcal{P}_k|\right). \end{aligned}$$

El último paso es consecuencia del Ejercicio 2.10. Precisamente el valor $c = \sqrt{2} - 1$ sale de la igualdad $\frac{2c^2}{1-c} + 2c - 1 = c$.

2.3. Sucesiones B_h infinitas

Ejercicio 2.3.1. Sea A_h la sucesión B_h construida con el algoritmo avaricioso. Demostrar que $A_h(x) \gg x^{\frac{1}{2h-1}}$.

Como ya comentamos en el capítulo anterior, el exponente $1/(2h-1)$ que se obtiene con el algoritmo voraz fue mejorado por Ruzsa para el caso $h = 2$. Recientemente [18] se ha utilizado una variante del método de Ruzsa que permite mejorar dicho exponente en los casos $h = 3$ y $h = 4$. Sin embargo el método de Ruzsa se extiende mal para valores más grandes de h.

Para valores mayores de h adaptaremos el método utilizado en la construcción de la sucesión que aparece en el Teorema 2.2.1 y le combinareos con un argumento probabilístico para demostrar la existencia de sucesiones B_h que mejoran el exponente $\frac{1}{2h-1}$ para todo h.

Teorema 2.3.1 (Cilleruelo [13])**.** *Para todo $h \geq 3$ existe una sucesión B_h, $\mathcal{B}$, con*

$$\mathcal{B}(x) = x^{\sqrt{(h-1)^2+1}-(h-1)+o(1)}.$$

Demostración. Fijemos

$$c = \sqrt{(h-1)^2+1} - (h-1)$$

y consideremos la función $f(t) = ct^2 - t^2/\sqrt{\log t}$. Sea

$$\mathcal{P} = \bigcup_{k\geq 3} \mathcal{P}_k$$

donde

$$\mathcal{P}_k = \left\{ p \text{ prime } : \ e^{f(k-1)} < p \leq e^{f(k)} \right\}.$$

Sea $\overline{q} := q_1 < q_2 < \cdots$ una sucesión de primos con

$$e^{2j-1} < q_j \leq e^{2j+1}$$

y sea g_j un generador de $\mathbb{F}_{q_j}^*$. Para cada $p \in \mathcal{P}_k$ definimos el entero

$$b_p = x_1(p) + \sum_{2\leq j\leq k} x_j(p)(h^2 q_1)\cdots(h^2 q_{j-1}),$$

donde $x_j(p)$ es la solución de la congruencia

$$g_j^{x_j(p)} \equiv p \pmod{q_j}, \qquad (h-1)q_j + 1 \leq x_j(p) \leq hq_j - 1.$$

Definimos $x_j(p) = 0$ para $j > k$.

Es claro que la sucesión $\mathcal{B}_{\overline{q},c} = \{b_p\}$ será una sucesión B_h si y sólo si para todo $l,\ 2 \leq l \leq h$ no existe una suma repetida de la forma

$$\begin{array}{rcl} b_{p_1} + \cdots + b_{p_l} & = & b_{p'_1} + \cdots + b_{p'_l} \\ \{b_{p_1}, \ldots, b_{p_l}\} & \cap & \{b_{p'_1}, \ldots, b_{p'_l}\} = \emptyset \\ b_{p_1} \geq & \cdots & \geq b_{p_l} \\ b_{p'_1} \geq & \cdots & \geq b_{p'_l}. \end{array} \tag{2.20}$$

La siguiente proposición es una generalización de la Proposition 3.4.3.

Proposición 2.3.1. *Supongamos que existen* $p_1, \ldots, p_l, p'_1, \ldots, p'_l \in \mathcal{B}_{\overline{q},c}$ *satisfaciendo* (2.20). *Entonces se tiene que:*

i) $p_i, p'_i \in \mathcal{P}_{k_i},\ i = 1, \ldots, l$ *for some* $k_l \leq \cdots \leq k_1$.

$$p_1 \cdots p_l \equiv p'_1 \cdots p'_l \pmod{Q_{k_l}}$$

ii)
$$\begin{array}{lll} p_1 \cdots p_{l-1} \equiv p'_1 \cdots p'_{l-1} & (\text{mód } Q_{k_{l-1}}/Q_{k_l}) & \text{if } k_l < k_{l-1} \\ \cdots \qquad\qquad \cdots & & \\ p_1 \equiv p'_1 & (\text{mód } Q_{k_1}/Q_{k_2}) & \text{if } k_2 < k_1. \end{array}$$

iii) $k_l^2 < \frac{c}{1-c}\left(k_1^2 + \cdots + k_{l-1}^2\right).$

iv) $q_1 \cdots q_{k_1} \mid \prod_{i=1}^{l} (p_1 \cdots p_i - p'_1 \cdots p'_i).$

Demostración. La demostración es similar a la de la Proposición 3.4.3: En este caso k_i es el j más grande tal que

$$x_j(p_1) + \cdots + x_j(p_l) \geq i((h-1)q_j + 1).$$

La parte iii) es consecuencia de la primera congruencia de ii). La parte iv) es también una consecuencia obvia de la parte ii). □

La sucesión $\mathcal{B}_{\overline{q},c}$ definida al principio de esta sección puede no ser una sucesión B_h para el valor de c que hemos fijado. El plan de la demostración es quitar de $\mathcal{B}_{\overline{q},c} = (b_p)_{p\in\mathcal{P}}$ el mayor elemento que aparezca en cada repetición para obtener una verdadera sucesión B_h.

Más precisamente, definimos $\mathcal{P}^* = \mathcal{P}^*(\overline{q})$ como el conjunto

$$\mathcal{P}^* = \bigcup_k (\mathcal{P}_k \setminus \mathcal{R}_k(\overline{q}))$$

donde $\mathcal{R}_k(\overline{q}) = \{p \in \mathcal{P}_k : b_p \text{ es el mayor elemento en alguna ecuación (2.20)}\}$.

Al haber eliminado todas las posibles sumas repetidas es claro que la sucesión

$$\mathcal{B}^*_{\overline{q},c} = (b_p)_{p\in\mathcal{P}^*}$$

es una sucesión B_h.

Recordemos que en el Lema 2.2.1 demostrábamos que $\mathcal{B}_{\overline{q},c}(x) = x^{c+o(1)}$. Y si, $|\mathcal{R}_k(\overline{q})| = o(|\mathcal{P}_k|)$, tenemos que

$$\mathcal{B}^*_{\overline{q},c}(x) \sim \mathcal{B}_{\overline{q},c}(x) = x^{c+o(1)}.$$

Así que la demostración del Teorema 2.3.1 se completará si probamos que existe una sucesión $\overline{q}$ tal que $|\mathcal{R}_k(\overline{q})| = o(|\mathcal{P}_k|)$ cuando $k \to \infty$.

Para $2 \le l \le h$ escribimos

$$\mathrm{Bad}_l(\overline{q}, k_l, \dots, k_1) = \{(p_1, \dots, p_l') : \ p_i, p_i' \in \mathcal{P}_{k_i}, \ i = 1, \dots, l \text{ satisfying } (2.20)\}.$$

Observemos que cada $p \in \mathcal{R}_k(\overline{q})$ proviene de alguna $2l$-tupla

$$(p_1, \dots, p_l') \in \mathrm{Bad}_l(\overline{q}, k_l, \dots, k_1),$$

con $2 \le l \le h, \ k_l \le \cdots \le k_1 = k$. Entonces,

$$\begin{aligned} |\mathcal{R}_k(\overline{q})| &\le \sum_{l=2}^{h} \sum_{k_l \le \cdots \le k_1 = k} |\mathrm{Bad}_l(\overline{q}, k_l, \dots, k_1)| \qquad (2.21) \\ &\le h k^{h-1} \max_{\substack{2 \le l \le h \\ k_l \le \cdots \le k_1 = k}} |\mathrm{Bad}_l(\overline{q}, k_l, \dots, k_1)|. \end{aligned}$$

Sucede que no sabemos dar una buena cota superior para $|\mathrm{Bad}_l(\overline{q}, k_l, \dots, k_1)|$ para una sucesión concreta de primos $\overline{q} := q_1 < q_2 < \cdots$, pero lo sabemos hacer en media y es aquí donde introducimos el argumento probabilístico. Si el lector está familiarizado con el trabajo de Ruzsa, la sucesión $\overline{q}$ jugará el mismo papel que el parámetro α en la construcción de Ruzsa.

Consideremos el espacio probabilístico de las sucesiones $\overline{q} := q_1 < q_2 \cdots$ donde cada q_j se elige uniformemente entre todos los primos en el intervalo $(e^{2j-1}, e^{2^j+1}]$. Usaremos que

$$\pi(e^{2k+1}) - \pi(e^{2k-1}) \gg e^{2k}/k = e^{2k+O(\log k)}$$

para deducir que dados $q_1 < \cdots < q_{k_1}$ satisfaciendo

$$e^{2j-1} < q_j \le e^{2j+1}$$

tenemos que

$$\begin{aligned} \mathbb{P}(q_1, \dots, q_{k_1} \in \overline{q}) &= \prod_{k=1}^{k_1} \frac{1}{\pi(e^{2k+1}) - \pi(e^{2k-1})} \\ &\le e^{-k_1^2 + O(k_1 \log k_1)}. \end{aligned}$$

Entonces, para una $2l-$tupla dada $(p_1,\dots,p_l')$, usamos la Proposición2.3.1, iv) y la estimación $\tau(n)=n^{O(1/\log\log n)}$ para la función divisor para deducir que

$$\begin{aligned}\mathbb{P}((p_1,\dots,p_l')\in \mathrm{Bad}_l(\overline{q},k_l,\dots,k_1)) & \\ \leq & \sum_{\substack{q_1,\dots,q_{k_1}\\ q_1\cdots q_{k_1}\mid\prod_{i=1}^{l}(p_1\cdots p_i-p_1'\cdots p_i')}} \mathbb{P}(q_1,\dots,q_{k_1}\in\overline{q})\\ \leq & \ \tau\left(\prod_{i=1}^{l}(p_1\cdots p_i-p_1'\cdots p_i')\right)e^{-k_1^2+O(k_1\log k_1)}\\ \leq & \ e^{-k_1^2+O(k_1^2/\log k_1)}.\end{aligned}$$

Usando la Proposition 2.3.1 iii) en la última desigualdad tenemos que:

$$\begin{aligned}\mathbb{E}(|\{(p_1,\dots,p_l') \ : \ & p_i,p_i'\in\mathcal{P}_{k_i},\ i=1,\dots,l \text{ satisfying (2.20)}\}|)\\ \leq & \ e^{-k_1^2+O(k_1^2/\log k_1)}|\{(p_1,\dots,p_l') : \ p_i,p_i'\in\mathcal{P}_{k_i}\}|\\ \leq & \ e^{-k_1^2+O(k_1^2/\log k_1)}|\mathcal{P}_{k_1}|^2\cdots|\mathcal{P}_{k_l}|^2\\ \leq & \ e^{-k_1^2+O(k_1^2/\log k_1)}\cdot e^{2f(k_1)+\cdots+2f(k_l)}\\ \leq & \ e^{-k_1^2+\frac{2c}{1-c}\left(k_1^2+\cdots+k_{l-1}^2\right)-(2c+o(1))k_1^2/\sqrt{\log k_1}}\\ \leq & \ e^{\left(-1+\frac{2c(l-1)}{1-c}\right)k_1^2-(2c+o(1))k_1^2/\sqrt{\log k_1}}.\end{aligned}$$

Y usando (2.21) obtenemos

$$\mathbb{E}(|\mathcal{R}_k(\overline{q})|)\leq e^{\left(-1+\frac{2c(h-1)}{1-c}\right)k^2-(2c+o(1))k^2/\sqrt{\log k}}.$$

Finalmente usamos la identidad $-1+\frac{2c(h-1)}{1-c}-c=0$ para $c=\sqrt{(h-1)^2+1}-(h-1)$ para obtener

$$\begin{aligned}\mathbb{E}\left(\sum_k\frac{|\mathcal{R}_k(\overline{q})|}{|\mathcal{P}_k|}\right) & \leq \sum_k k^2 e^{\left(-1+\frac{2c(h-1)}{1-c}-c\right)k^2-(c+o(1))k^2/\sqrt{\log k}}\\ & \leq \sum_k k^2 e^{-(c+o(1))k^2/\sqrt{\log k}}.\end{aligned}$$

Como la serie es convergente tenemos que para casi toda sucesión $\overline{q}$ la serie

$$\sum_k\frac{|\mathcal{R}_k(\overline{q})|}{|\mathcal{P}_k|}$$

es convergente. Así que, para cualqueira de estas sucesiones $\overline{q}$ tenemos que $|\mathcal{R}_k(\overline{q})| = o(|\mathcal{P}_K|)$, que es lo que pretendíamos probar. $\square$

Capítulo 3

Problemas sin resolver sobre conjuntos de Sidon

Este capítulo está dedicado a aquellos problemas sobre los conjuntos de Sidon a los que todavía no se sabe dar respuesta. Muchos de ellos ya han aparecido en los dos capítulos anteriores. Gran parte de ellos fueron propuestos por Erdős hace muchos años y son, presumiblemente, muy difíciles. Pero hay otros más recientes que quizás no se hayan pensado lo suficiente y sean más asequibles. Nuestra intención es que esta colección de problemas pueda servir de fuente de inspiración para jóvenes investigadores.

3.1. Conjuntos de Sidon en intervalos

Erdős y Turan [30] demostraron que si $A \subset [1, n]$ es un conjunto de Sidon entonces $|A| < n^{1/2} + O(n^{1/4})$. Lindström [44] y Ruzsa [55] obtuvieron demostraciones más limpias que dan lugar a la cota $|A| < n^{1/2} + n^{1/4} + 1$. Esta estimación lleva 54 años sin mejorarse salvo por la insignificante mejora [10] (que ya estaba implícita en [55]) y que supone la cota $|A| < n^{1/2} + n^{1/4} + 1/2$. Mejorar esta cota superior (incluso eliminar el $1/2$ para n grande) es un problema que se resiste.

Durante mucho tiempo Erdős estuvo convencido de que las cotas anteriores se podían sustituir por $|A| \leq \sqrt{n} + O(1)$. Pero, según afirma

el propio Erdős en [27], Ruzsa y H. Talylor le convencieron de que había razones que sugerían que podía no ser cierto. La conjetura más plausible es la siguiente.

Conjetura 3.1.1 (Erdős)**.** *Para todo $\epsilon > 0$, si $A \subset \{1, \dots, n\}$ es un conjunto de Sidon, entonces $|A| \leq \sqrt{n} + O(n^{\epsilon})$.*

Como ya hemos comentado, se cree que la conjetura anterior no es cierta para $\epsilon = 0$. De otra manera:

Conjetura 3.1.2. *Para todo M existe un n y un conjunto de Sidon $A \subset [1, n]$ con $|A| > \sqrt{n} + M$.*

Los resultados computacionales avalan esta última conjetura. Pero también existen argumentos heurísticos sólidos a su favor. Uno de ellos está relatado en el Ejercicio 1.3.8. Otro resultado que apoya esta conjetura es que la conjetura análoga en dimensión 2 sí se sabe cierta [10].

Si seguimos con detalle cualquiera de los argumentos que proporcionan la cota superior $|A| < \sqrt{n} + O(n^{1/4})$ cuando A es un conjunto de Sidon en $[1, n]$ observamos que sólo se utiliza el hecho de que todas las diferencias positivas $a - a'$ menores que $n^{3/4}$ son distintas. Sería interesante estudiar si bajo estas condiciones, menos restrictivas que las de ser conjunto de Sidon, la cota superior está más cerca de lo mejor posible. Un primer paso sería demostrar la siguiente conjetura, previsiblemente más sencilla.

Conjetura 3.1.3. *Para todo M existe un n conjunto $A \subset [1, n]$ con $|A| > \sqrt{n} + M$ y con la propiedad de que todas las diferencias $a - a'$, $a, a' \in A$ con $0 < a - a' < n^{1/2}$ son distintas.*

3.2. Conjuntos de Sidon en dimensiones superiores

Conjetura 3.2.1. *Para todo $\epsilon > 0$, si $A \subset [1, n]^d$ es un conjunto de Sidon, entonces $|A| \leq n^{d/2} + O(n^{\epsilon})$.*

Si esta conjetura es cierta es sin duda muy difícil de demostrar, al menos en dimensión $d = 2$. La razón es que en ese caso daría una respuesta

positiva a una antigua conjetura de Vinogradov sobre el menor residuo no cuadrático módulo p: para todo $\epsilon > 0$ y p primo suficientemente grande existe un residuo no cuadrático menor que p^{ϵ}.

Conjetura 3.2.2. *Para todo $d \geq 1$ y para todo M existe un conjunto de Sidon en $[1, n]^d$ con $|A| > n^{d/2} + M$.*

Como hemos comentado anteriormente, se sabe que es cierto para $d = 2$. Quizás los casos $d \geq 3$ no se hayan intentado lo suficiente.

3.3. Conjuntos de Sidon en grupos finitos

¿Cuál es el mayor tamaño de un conjunto de Sidon en $\mathbb{Z}_n$? Si n es de la forma $n = p(p-1)$, $n = q^2 + q + 1$ o $n = q^2 - 1$, donde q es la potencia de un primo, entonces $\mathbb{Z}_n$ contiene un conjunto de Sidon de tamaño $\sqrt{n} + O(1)$. Cualquier de estas familias implica que

$$\limsup_{n\to\infty} \frac{F_2(\mathbb{Z}_n)}{\sqrt{n}} = 1.$$

Estas construcciones obedecen a ciertos milagros algebraicos que no tienen que ocurrir para todo n. Por otra parte es claro que cualquier conjunto de Sidon en el intervalo $[1, n/2]$ es en particular un conjunto de Sidon en $\mathbb{Z}_n$. Este argumento implica que $\liminf_{n\to\infty} \frac{F_2(\mathbb{Z}_n)}{\sqrt{n}} \geq 1/\sqrt{2}$. Aunque creemos que el valor de este límite es $1/\sqrt{2}$, no siquiera sabemos demostrar la siguiente conjetura.

Conjetura 3.3.1.

$$\liminf_{n\to\infty} \frac{F_2(\mathbb{Z}_n)}{\sqrt{n}} < 1.$$

Los conjuntos de la forma

$$A = \{(f(x), g(x)) : \ x \in \mathbb{Z}_p\} \subset \mathbb{Z}_p \times \mathbb{Z}_p \tag{3.1}$$

donde f y g son polinomios independientes de grados $1 \leq \deg f, \deg g \leq 2$ son conjuntos de Sidon con p elementos. La demostración de la siguiente conjetura sería el primer resultado inverso cobre conjuntos de Sidon.

Conjetura 3.3.2. *Todos los conjuntos de Sidon en $\mathbb{Z}_p \times \mathbb{Z}_p$ con p elementos son de la forma descrita en* (3.1).

Se sabe que si $A = \{(x, g(x)) : \ x \in \mathbb{Z}_p\}$ es un conjunto de Sidon en $\mathbb{Z}_p \times \mathbb{Z}_p$ entonces g es un polinomio cuadrático.

3.4. Sucesiones infinitas de Sidon

Al sucesión avariciosa de Sidon (la sucesión de Mian-Chowla) es aquella que empezando en $a_1 = 1$, el término a_n es el menor entero positivo que se puede elegir de tal manera que $\{a_1, \dots, a_n\}$ sea un conjunto de Sidon. Mientras que un argumento sencillo muestra que $A(x) \geq x^{1/3}$, se desconoce cuál es el verdadero orden de magnitud de $A(x)$.

Conjetura 3.4.1. *La función contadora de la sucesión de Mian-Chowla satisface que*

$$\frac{A(x)}{x^{1/3}} \to \infty.$$

De hecho, argumentos heurísticos y computacionales sugieren que $A(x)$ debería tener un comportamiento asintótico de la forma

$$A(x) \sim c(x \log x)^{1/3}.$$

Sin embargo se desconoce siquiera que $A(x) \ll x^{1/2-\epsilon}$ para algún $\epsilon > 0$.

Los n primeros términos de la sucesión de Mian-Chowla forman una sucesión maximal en el sentido de que no es posible añadir un elemento entre 1 y a_n sin que se destruya la propiedad de ser de Sidon. Sea $M(n)$ el menor tamaño de un conjunto de Sidon en $[1, n]$ con la propiedadde ser maximal. Se desconoce cuál es el orden de magnitud de $M(n)$. Es claro que $M(n) \geq n^{1/3}$ y por otra parte Ruzsa [56] ha demostrado que $M(n) \ll (n \log n)^{1/3}$.

Problema 3.4.1. *¿Es cierto que $M(n)/n^{1/3} \to \infty$?*

Una respuesta afirmativa a este problema implicaría inmediatamente la Conjetura 3.4.1.

La siguiente conjetura aparece insistentemente en varios artículos de Erdős.

Conjetura 3.4.2 (Erdős). *Para todo $\alpha < 1/2$ existe una sucesión infinita de Sidon A con $A(x) \gg x^{\alpha}$.*

Ruzsa demostró la existencia de una sucesión de Sidon A con $A(x) = x^{\sqrt{2}-1+o(1)}$. Una construcción explícita con la misma función contadora fue dada por Cilleruelo. Ver el capítulo 2 para más detalles.

El propio Erdős demostró que la conjetura anterior no es cierta para $\alpha = 1/2$ pero demostró la existencia de una sucesión infinita de Sidon con

$$\limsup_{x\to\infty} \frac{A(x)}{\sqrt{x}} \geq c$$

con $c = 1/2$. Posteriormente Kruckeberg [42] lo demostró para $c = 1/\sqrt{2}$.

Conjetura 3.4.3 (Erdős). *Existe una sucesión infinita de Sidon con*

$$\limsup_{x\to\infty} \frac{A(x)}{\sqrt{x}} = 1.$$

Erdős también observó que la conjetura 3.4.3 seguiría de la siguiente.

Conjetura 3.4.4 (Erdős). *Dados $a_1, \ldots, a_k$ elementos de un conjunto de Sidon, existe para todo n un conjunto de Sidon $A \subset [1, n]$ con $|A| \sim \sqrt{n}$ que les contiene.*

Es posible que ninguna de estas dos conjeturas sea cierta.

Sea $A_x = A \cap [1, x]$. En el Ejercicio 2.1.2 se pide demostrar que si A es una sucesión infinita con $|A_x - A_x| \sim |A_x|^2$ entonces $\liminf_{x\to\infty} \frac{A(x)}{\sqrt{x}} = 0$. Sería interesante saber si se puede conseguir la misma conclusión asumiendo una hipótesis análoga para $A_x + A_x$.

Problema 3.4.2. *Sea A una sucesión infinita con $|A_x + A_x| \sim |A_x|^2/2$. ¿Es cierto que $\liminf_{x\to\infty} \frac{A(x)}{\sqrt{x}} = 0$?*

3.5. Sucesiones B_h y $B_2[g]$

La diferencia esencial entre las sucesiones de Sidon (sucesiones B_2) y las sucesiones B_h con $h \geq 3$, radica que, a diferencia de las primeras,

las sucesiones B_h con $h \geq 3$ no se pueden caracterizar en términos de sus diferencias. Eso hace que muchos resultados, que son conocidos para $h = 2$, se desconozcan para $h \geq 3$. El primero de ellos se refiere al máximo tamaño de un conjunto B_h en $[1, n]$. Mientras que es bien conocido que $F_2(n) \sim \sqrt{n}$, se desconoce el comportamiento asintótico de $F_n(n)$. Ni siquiera se sabe si tiene.

Problema 3.5.1. *Hallar el valor asintótico de $F_h(n)$ para $h \geq 3$.*

Hay construcciones que demuestran que $F_h(n) \geq n^{1/h}(1+o(1))$, pero las cotas superiores son bastante peores. Por ejemplo para $h = 4$, la mejor cota superior se debe a Ben Green: $F_4(n) \leq (7n)^{1/4}(1 + o(1))$. Probablemente, $F_h(n) \sim n^{1/h}$.

Respecto a las sucesiones B_h infinitas sucede algo parecido. Si A es una sucesión B_h con h par, entonces $B = A+\cdots+A$ es casi una sucesión de Sidon en el sentido de que $|B-B| \sim |B|^2$ y se puede demostrar que en ese caso $\liminf_{x\to\infty} \frac{A(x)}{x^{1/h}} = 0$. Sin embargo si h es impar ese argumento no funciona y el resultado análogo se desconoce.

Conjetura 3.5.1. *Si A es una sucesión B_h infinita entonces*

$$\liminf_{x\to\infty} A(x)/x^{1/h} = 0.$$

La conjetura se ha demostrado para h par.

3.6. Conjuntos de Sidon con condiciones adicionales

Erdős consideró conjuntos A que no eran de Sidon pero que $|A+A| \sim |A|^2/2$. A estos conjuntos los llamó conjuntos quasi-Sidon.

Problema 3.6.1. *Dar estimaciones no triviales de*

$$Q(n) = \max |A| : \ A \subset [1, n], \ A \text{ es quasi-Sidon.}$$

Se sabe que

$$1{,}154\ldots \frac{2}{\sqrt{3}}(1+o(1)) \leq \frac{Q(n)}{\sqrt{n}} \leq \left(\frac{1}{4} + \frac{1}{(\pi+2)^2}\right)(1+o(1)) = 1{,}863\ldots.$$

La cota inferior se debe a una construcción de Erdős y Freud [28] y la cota superior a Pikhurko[53].

Conjetura 3.6.1. *Demostrar que si $A \subset \{1, \dots, n\}$ es de Sidon y convexo, entonces $|A| = o(\sqrt{n})$.*

Esta interesante conjetura la escuché (creo que a Ruzsa) en el workshop que Ruzsa organizó en Budapest en el año 2000. Se dice que una sucesión es convexa si las diferencias entre dos términos consecutivos de la sucesión son crecientes. Por ejemplo, la sucesión de los cuadrados es una sucesión convexa.

Problema 3.6.2. *Construir un conjunto, lo más grande posible, $A \subset \{1, \dots, n\}$ que sea de Sidon y convexo.*

No es difícil demostrar que si $A \subset [1, n]$ es una sucesión de Sidon formada por cuadrados entonces $|A| = o(\sqrt{n})$.

Problema 3.6.3. *¿ Es cierto que para todo $\epsilon > 0$ existe un conjunto de Sidon en $[1, n]$ formado por cuadrados y de tamaño $|A| \gg n^{1/2-\epsilon}$?*

No es difícil demostrar que existe uno de tamaño $|A| \geq n^{1/3-o(1)}$. Bastante más complicado, aunque se sabe cierto, es la demostración de que existe un conjunto de Sidon de cuadrados $A \subset [1, n]$ tal que $|A| \gg n^{1/3}$. Probablemente no se pueda mejorar el exponente $1/3$. La razón para sospechar esto es un trabajo reciente de Saxton and Thomason [59]. Uno de sus corolarios es que si elegimos un conjunto de $\sqrt{n}$ elementos al azar en $[1, n]$, con probabilidad tendiendo a 1, el mayor conjunto de Sidon que contiene tiene tamaño $n^{1/3+o(1)}$. Si los cuadrados en $[1, n]$ se comportan como un conjunto aleatorio para este problema entonces no se debería esperar que contuvieran un conjunto de Sidon de tamaño $n^{1/3+\epsilon}$.

Komlós, Sulyok y Szemerédi [41] demostraron que cualquier conjunto de n elementos contiene un conjunto de Sidon de tamaño $|A| \gg \sqrt{n}$. Erdős hizo la siguiente conjetura cn respecto a este problema.

Conjetura 3.6.2 (Erdős)**.** *Todo conjunto de enteros de n elementos contiene un conjunto de sidon con $\sim \sqrt{n}$ elementos.*

Mi opinión es que esta conjetura es falsa.

3.7. Bases y sucesiones de Sidon

Una de las conjeturas más importantes de la teoría combinatoria de números es la que se conoce como Conjetura de Erdős-Turan.

Conjetura 3.7.1. *Si A es una base asintótica de orden 2 entonces su función de representación no está acotada.*

La siguiente conjetura, conocida como conjetura fuerte de Erdős Turan, implica la anterior porque si A es una base de orden 2 entonces $A(x) \gg x^{1/2}$.

Conjetura 3.7.2. *Si $A(x) \gg x^{1/2}$ entonces su función de representación no está acotada.*

En la otra dirección una Erdős conjeturó lo siguiente.

Conjetura 3.7.3 (Erdős)**.** *Existe alguna sucesión de Sidon que es base asintótica de orden 3.*

Esta conjetura parece difícil pero recientemente se ha demostrado [9] que para todo $\epsilon > 0$ existe una sucesión de Sidon A tal que todo n suficientemente grande se puede escribir de la forma $n = a_1+a_2+a_3+a_4$ con $a_1, a_2, a_3, a_4 \in A$ y $a_4 < n^{\epsilon}$.

Bibliografía

[1] Aliev, Iskander, *Siegel's lemma and sum-distinct sets*. Discrete Comput. Geom. 39 (2008), no. 1-3, 59–66.

[2] M. Ajtai, J. Komlós, and E. Szemerédi, *A dense infinite Sidon sequence*, European J. Combin. 2 (1981), 1–11.

[3] N. Alon and Spencer, The probabilistic method,

[4] R. C. Baker, G. Harman, G. Pintz y J Pintz (2001). *The difference between consecutive primes, II.* Proceedings of the London Mathematical Society 83 (3): 532–5-62

[5] R. C. Bose, *An afine analogue of Singer's theorem*, J. Indian Math. Soc. (N.S.) 6 (1942), 1–15.

[6] R. C. Bose and S. Chowla, *Theorems in the additive theory of numbers*, Comment. Math. Helv. 37 (1962/1963), 141–147.

[7] J. Cilleruelo, *Conjuntos de Sidon*, EMALCA 2014.

[8] J. Cilleruelo, *The greedy Sidon sequence*, en preparación.

[9] J. Cilleruelo, *Sidon basis*. Preprint in Arxiv.

[10] J. Cilleruelo, *Sidon sets in* $\mathbb{N}^d$. J. Combin. Theory Ser. A 117 (2010), no. 7, 857–871.

[11] J. Cilleruelo, *New upper bounds for finite* B_h *sequences*, Adv. Math. 159 (2001), 1–17.

[12] J. Cilleruelo, *Probabilistic constructions of* $B_2[g]$ *sequences*, Acta Mathematica Sinica vol 26, nº7 (2010)

[13] J. Cilleruelo, *Infinite Sidon sequences*, *Advances in Mathematics*, vol 255 (2014)

[14] J. Cilleruelo, *An upper bound for $B_2[2]$ sequences,* J. Combin. Theory Ser. A 89 (2000), no. 1, 141–144.

[15] J. Cilleruelo y J. Jiménez, *$B_h[g]$ sequences*, Mathematika, vol 47, nº1-2 (2000).

[16] J. Cilleruelo y M. Nathanson, *Perfect difference sets constructed from Sidon sets*, Combinatorica, vol 28, nº4 (2008)

[17] J. Cilleruelo and C. Vinuesa, *$B_2[g]$ sets and a conjecture of Schinzel and Schmidt,* Combinatorics, Probability and Computing, vol 17, nº6 (2008)

[18] J. Cilleruelo and R. Tesoro, *Dense infinite B_h sequences*. Preprint in Arxiv.

[19] J. Cilleruelo, I. Ruzsa and C. Trujillo, *Upper and lower bounds for finite $B_h[g]$ sequences*, J. Number Theory 97 (2002), 26–34.

[20] J. Cilleruelo, I. Ruzsa and C. Vinuesa, *Generalized Sidon sets*. Adv. Math. 225 (2010), no. 5, 2786–2807.

[21] J. Cilleruelo, S. Kiss, I. Ruzsa and C. Vinuesa, *Generalization of a theorem of Erdos and Renyi on Sidon sets* Random Structures and Algorithms, vol 37, nº4 (2010)

[22] J. Cilleruelo and J. Rué, *On a question on Sarkozy and Sos for bilinear forms*, Bulletin of the London Mathematical Society, vol 41, nº2 (2009)

[23] S. Chen, *On Sidon sequences of even orders*, Acta Arith. 64 (1993), 325–330.

[24] S. Chen, *On the size of finite Sidon sequences*. Proc. Amer. Math. Soc. 121 (1994), no. 2, 353–356.

[25] G. A. Dirac, *Note on a Problem in Additive Number Theory*, J. London Math. Soc. 26 (1951) pp. 312–313.

[26] A. G. Doyachkov and V. V. Rykov, *B_s-sequences*, Mat. Zametki 36 (1984), 593–601, English trans- lation: Math. Notes 36 (1984), no. 3-4, 794–799.

[27] P. Erdős, *Some Problems and Results on Combinatorial Number Theory.*

[28] P. Erdős and R. Freud, *On Sidon sequences and related problems*, Mat. Lapok 1 (1991), 1-44

[29] P. Erdős and A. Renyi, *Additive properties of random sequences of positive integers,* Acta Arith. 6 (1960), 83–110.

[30] Erdős, P and Turan, P. *On a problem of Sidon in additive number theory, and on some related problems*, J. London Math. Soc. 16 (1941), 212–215.

[31] M. Z. Garaev, The sum-product estimate for large subsets of prime fields. *Proc. Amer. Math. Soc.* 136 (2008) n.8, 2735-2739.

[32] M. Z. Garaev and C. Shen, On the size of the set $A(A+1)$, *Mathematische Zeitschrift*, 265 (2010) n.1, 125-132.

[33] B. Green, *The number of squares and $B_h[g]$ sets*, Acta Arith. 100 (2001), 365–390.

[34] C. A. Gómez Ruiz y C. A. Trujillo Solarte, *A new construction of modular Bh-sequences.* (Spanish) Mat. Enseñ. Univ. (N. S.) 19 (2011), no. 1, 53–62.

[35] T. Gowers, Some unsolved problems in additive/combinatorial number theory.

[36] S.W. Graham and C. J. Ringrove, *Lower bounds for least quadratic nonresidues*, Progress in Math. **85**, (1990).

[37] Halberstam and Roth, *Sequences*, Clarendon Press 1966

[38] M. Helm, *On B_3-sequences*, Analytic Number Theory, Vol. 2 (Allerton Park, IL, 1995), Progr. Math., vol. 139, Birkhauser Boston, Boston, MA, 1996, pp. 465–469.

[39] X.-D. Jia, *On finite Sidon sequences*, J. Number Theory 44 (1993), 84–92.

[40] M. Kolountzakis, *The density of $B_h[g]$ sequences and the minimum of dense cosine sums*, J. Number Theory 56 (1996), 4–11.

[41] J. Komlós, M. Sulyok, and E. Szemerédi, *Linear problems in combinatorial number theory*, Acta Math. Acad. Sci. Hungar. 26 (1975), 113—121

[42] F. Kruckeberg, *B_2-Folgen und verwandte Zahlenfolgen*, J. Reine Angew. Math. 206 (1961), 53–60.

[43] H. Lefmann and Torsten Thiele, Point sets with distinct distances, Combinatorica 15 (1995), 379–408.

[44] B. Lindström, *An inequality for B_2-sequences*, J. Combinatorial Theory 6 (1969), 211–212.

[45] B. Lindström, *A remark on B_4-sequences*, J. Combinatorial Theory 7 (1969), 276–277.

[46] B. Lindström, *On B_2-sequences of vectors*, J. Number Theory 4 (1972), 261–265.

[47] Maldonado López, Juan Pablo A remark on infinite Sidon sets. (Spanish) Rev. Colombiana Mat. 45 (2011), no. 2, 113–127.

[48] G. Martin, K. O'Bryant, *Constructions of Generalized Sidon Sets*. Journal of Combinatorial Theory, Series A, Volume 113, Issue 4, 591-607 (2006).

[49] G. Martin, K. O'Bryant, *The Symmetric Subset Problem in Continuous Ramsey Theory*. Experiment. Math., Volume 16, no 2, 145-166 (2007).

[50] M. Matolcsi and C. Vinuesa, *Improved bounds on the supremum of autoconvolutions*. J. Math. Anal. Appl. 372 (2010), no. 2, 439–447

[51] L. Moser, *An Application of Generating Series*, Mathematics Magazine (1) 35 (1962) 37–38.

[52] K. O'Bryant, *A complete annotated bibliography of work related to Sidon sequences* The Electronic Journal of Combinatorics, (2004) Volume: DS11.

[53] O. Pikhurko, *Dense edge-magic graphs and thin additive bases.* Discrete Math. 306 (2006), no. 17, 2097–2107.

[54] I. Ruzsa, *Solving a linear equation in a set of integers.* I. Acta Arith. 65 (1993), no. 3, 259–282.

[55] I. Ruzsa, *An infinite Sidon sequence.* J. Number Theory 68 (1998), no. 1, 63–71.

[56] I. Ruzsa, *A small maximal Sidon set.* The Ramanujan Journal 2 (1998), 55–58.

[57] L. Rackman y P. Sarka, B_h *Sequences in Higher Dimensions*, The Electronic Journal of Combinatorics, 17 (2010), #35

[58] C. Sandor, *A note on a conjecture of Erdős-Turan*, Integers 8 (2008), A30, 4 pp.

[59] D. Saxton and A. Thomason, *Hypergraph containers*, Preprint.

[60] I. Shparlinski, *On* B_s*-sequences*, Combinatorial Analysis, No. 7 (Russian), Moskov. Gos. Univ., Moscow, 1986, pp. 42–45, 163.

[61] J. Singer, *A theorem infinite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. 43 (1938), 377–385.

[62] J. Solymosi, *Bounding multiplicative energy by the sumset*, Adv. in Math. 222 (2009), 402–408.

[63] A. Stohr, *Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe. I, II* , J. Reine Angew. Math. 194 (1955), 40–65, 111–140.

[64] C. Trujillo, Sucesiones de Sidon, *Ph. D thesis*, (1998) Universidad Politécnica de Madrid.

[65] L. Vinh, *The Szemerédi–Trotter type theorem and the sum-product estimate in finite fields*, European Journal of Combinatorics Volume 32, Issue 8, November 2011, Pages 1177—1181.

[66] V. H. Vu, *On a refinement of Waring's problem*, Duke Math. J. 105, (2000), no 1, 107-134.

[67] G. Yu, *An upper bound for $B_2[g]$ sets.* J. Number Theory 122, no. 1, 211-220 (2007).