XXVII ESCUELA VENEZOLANA DE MATEMÁTICAS
EMALCA-VENEZUELA 2014

CONJUNTOS DE SIDON

Javier Cilleruelo

MÉRIDA, VENEZUELA, 31 de agosto al 5 de septiembre de 2014

XXVII ESCUELA VENEZOLANA DE MATEMÁTICAS
EMALCA - VENEZUELA 2014

Conjuntos de Sidon

Javier Cilleruelo

Universidad Autónoma de Madrid
Instituto de Ciencias Matemáticas (ICMAT)

franciscojavier.cilleruelo@uam.es

MÉRIDA, VENEZUELA, 31 DE AGOSTO AL 5 DE SEPTIEMBRE DE 2014

XXVII ESCUELA VENEZOLANA DE MATEMÁTICAS

La Escuela Venezolana de Matemáticas es una actividad de los postgrados en matemáticas de las instituciones siguientes: Centro de Estudios Avanzados del Instituto Venezolano de Investigaciones Científicas, Facultad de Ciencias de la Universidad Central de Venezuela, Facultad de Ciencias de la Universidad de Los Andes, Universidad Simón Bolívar, Universidad Centroccidental Lisandro Alvarado y Universidad de Oriente, y se realiza bajo el auspicio de la Asociación Matemática Venezolana. La XXVII Escuela Venezolana de Matemáticas recibió financiamiento de la Academia de Ciencias Físicas, Matemáticas y Naturales de Venezuela, el Banco Central de Venezuela, el Fondo Nacional de Ciencia, Tecnología e Innovación (FONACIT), el Instituto Venezolano de Investigaciones Científicas (Centro de Estudios Avanzados, Departamento de Matemáticas y Ediciones IVIC), la Universidad de los Andes (CEP, CDCHT, Departamento de Matemáticas de la Facultad de Ciencias, Decanato de Ciencias y Vicerrectorado Administrativo), Unión Matemática de América Latina y el Caribe (UMALCA) y Centre International de Mathematiques Pures et Appliquees (CIMPA).

2010 Mathematics Subject Classication: 11B83 (11B30)

Instituto Venezolano de Investigaciones Científicas
Rif: G-20004206-0

Conjuntos de Sidon

Javier Cilleruelo

Diseño y edición: Escuela Venezolana de Matemáticas
Preprensa e impresión: Gráficas Lauki C.A.
Deposito legal: If66020145102247
ISBN: 978-980-261-154-6
Caracas, Venezuela
2014

Para Estrella y Carlos

Índice general

Prefacio

Uno de los temas favoritos de Paul Erdős y que mejor describe su gusto por los problemas aritméticos con sabor conbinatorio, 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 construir sucesiones infinitas de Sidon A cuya función contadora $A(x) = |A \cap [1, x]|$ sea tan grande como sea posible.

Los conjuntos de Sidon admiten varias generalizaciones naturales, como los conjuntos B_h donde todas las sumas de h elementos de conjuntos son distintas o, más en general, las sucesiones $B_h[g]$, aquellas que tienen la propiedad de que todo elemento admite a lo más g representaciones como suma de h elementos del conjunto.

Hay un capítulo dedicado al método probabilístico, que es especial-

mente eficaz para demostrar la existencia de conjuntos de enteros o sucesiones infinitas que satisfacen ciertas propiedades dadas cuando no se saben construir explícitamente.

Los conjuntos de Sidon en grupos finitos aparecen también de manera natural al estudiar otros problemas aritmeticos y combinatorios. Permiten obtener demostraciones elementales de algunos resultados clásicos, como el último teorema de Fermat en cuerpos finitos, o resultados más recientes, como las estimaciones suma-producto en cuerpos finitos.

Hemos dedicado un último capítulo a problemas sin resolver sobre los conjuntos de Sidon. Es posible que el lector más ambicioso no resista la tentación de empezar por este capítulo y utilizar el resto del libro para ir completando información.

Todos los 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 exporar nuevos territorios.

El capítulo II del libro "Sequences"de Halberstam y Roth [36] es una referencia clásica sobre los conjuntos de Sidon hasta 1966. Erdős y R. Freud [27] escribieron un survey muy completo hasta 1991, pero en húngaro. "A complete annotated bibliography of work related to Sidon sequences", de Kevyn O'Bryant [51], 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 Turan fueron a visitar al analísta 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 estudando 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				10				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 se sabe 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 [36], 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 primera sección, 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 Turan [29] demostraron la desigualdad

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

Años más tarde Lindström [43] 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:

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

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 llamamos $l = rk-r(r+1)/2$ y S_r a la suma de todas esas diferencias tenemos que

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

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

$$\begin{aligned}
k &< \sqrt{n(1+1/r)} + (r+1)/2 \\
&< \sqrt{n} + \frac{\sqrt{n}}{2r} + \frac{r+1}{2}.
\end{aligned}$$

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 [53]. 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 lemma se debe a Ruzsa [53].

Lema 1.2.1 (Ruzsa [53])**.** *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 Lemma 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 [9], Ruzsa [53])**.** *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

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

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

Ejercicio 1.2.1 (Cilleruelo [9]). *Demostrar que si $A \subset \{1,\ldots,n\}$ 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 [26] 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 los ejercicios 1.2.3 y 1.2.4.

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

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

Ejercicio 1.2.4. *Utilizar el resultado del Ejercicio 1.2.3 para demostrar el Teorema 1.2.3.*

Ejercicio 1.2.5. *Dar una demostración alternativa del Teorema 1.2.2 a partir del Teorema 1.2.3.*

El Teorema 1.2.3 (ver Ejercicio 1.2.6) muestra que la condición de ser de Sidon no es estrictamente necesaria para obtener la cota superior $|A| \le \sqrt{n}(1 + o(1))$. Es suficiente con que $|A - A| \sim |A|^2$.

Ejercicio 1.2.6. *Sea $A \subset [1, n]$ un conjunto de enteros positivos tal que $|A - A| = (1 + o(1))|A|^2$. Demostrar que $|A| \le (1 + o(1))\sqrt{n}$.*

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 [27] 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 maximal 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 1.2.7. *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 1.2.8. *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 [52] 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 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 Turan [29] 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 Turan)**.** *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 maximal 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

$$\begin{aligned} x - y &\equiv a \pmod{q-1} \\ g^x - g^y &= b \quad (\text{ en } \mathbb{F}_q). \end{aligned}$$

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.

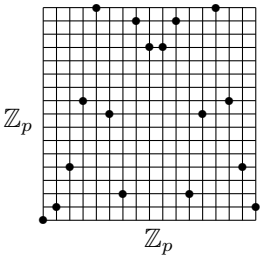
Ejemplo 3. *Dados dos generadores g_1, g_2 de $\mathbb{F}_q^*$, el conjunto*

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

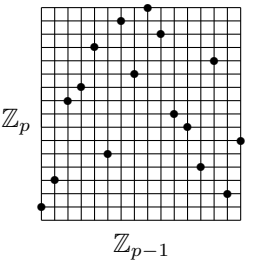
es un conjunto de Sidon en $\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}$ con $q-2$ elementos.

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

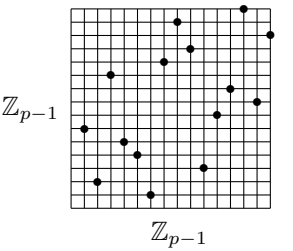
Cuando $q = p$ es un primo, podemos identificar $\mathbb{F}_p$ with $\mathbb{Z}_p$. Las figuras de abajo corresponden a los conjuntos de Sidon descritos para el caso $p = 17$.



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 [53] 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 (1.10) debería ser cierto. 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 [60]. 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 entorno 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 commportamiento 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 [33], 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 [33] se da una presentación unificada de estas tres construcciones. Aquí seguimos [33] 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 [44] 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 [38, 23] 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 [25] y mejoras posteriores aparecen en [59, 10, 32]. 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 [18], aparecen en [10] y [32]. En particular Ben Green [32] 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 infinita, 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 algorito 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 co-

nocida 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 [7] 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 [62] 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 últio pase se ha utilizado la parte izquierda de la desigualdad 2.7. 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 se sabe 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 [22] 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 [37] 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 [41].

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

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. 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 [54] 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 $|A| \gg \frac{\sqrt{n}}{\log n}$.

La 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 la 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 [12] ha encontrado una construcción explícita de una sucesión infinita de Sidon con función contadora similar a la de Ruzsa.

Teorema 2.2.1 (Cilleruelo [12])**.** *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 una sucesión infinita. 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 también de los primos racionales. El tamaño de los conjuntos de Sidon que se obtienen es menor (por un factor logarítmico) que el de los conjuntos de Sidon de procedencia algebrica, pero ofrece 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 $\{x_1, \ldots, x_h\} = \{y_1, \ldots, y_h\}$. □

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 $0 \leq x_i < b_{i-1}$.

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_j son primos que satisfacen la desigualdad

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

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

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

donde los x_i (los dígitos) son enteros tales que $0 \leq x_i < 4q_i$. El factor 4 en los elementos de la base no es estrictamente necesario pero es conveniente ponerlo por razones técnicas que se verán más adelaante.

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 ha sido utilizado en diferentes problemas y es muy interesante tenerlo en cuenta.

Una observación importamte 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:

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

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 consptruir 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. Demostración del Teorema 2.2.1

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_j) con

$$2^{2j-1} < q_j \leq 2^{2j+1} \tag{2.7}$$

y consideramos la base generalizada

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

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 (2.7) es claro que

$$2^{k^2} < Q_k < 2^{(k+1)^2}. \tag{2.8}$$

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 dl número de elementos de $\mathcal{P}_k$ lo dejamoscomo ejercicio.

Ejercicio 2.2.4. *Demostrar que*

$$|\mathcal{P}_k| \gg \frac{Q_k^c}{k^3}. \tag{2.9}$$

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

$$4^k Q_k < x \leq 4^{k+1} Q_{k+1}. \tag{2.10}$$

De (2.8) se sigue que fácilmente que

$$x = 2^{k^2(1+o(1))}. \tag{2.11}$$

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 $0 \leq x_i \leq q_i - 1$. 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 (2.11) 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 $p \in Pp_k$ 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

$$g_i^{x_i(p)} \equiv p \pmod{q_i}, \qquad q_i + 1 \leq x_i(p) \leq 2q_i - 1 \tag{2.12}$$

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 (2.12).

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) $p_1 p_2 \equiv p_1' p_2' \pmod{Q_j}$

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

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:

$$x_j(p_1) + x_j(p_2) = x_j(p_1') + x_j(p_2') \tag{2.13}$$

para todo j. Por construcción 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 (2.13) 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

$$\begin{aligned} g_j^{x_i(p)} &\equiv p \pmod{q_i},\ i \leq k \\ g_i^{x_i(p)} &\equiv 1 \pmod{q_i},\ i > k. \end{aligned}$$

Así que $p_1p_2 \equiv p_1'p_2' \pmod{q_i}$ para todo $i \leq j$ y por lo tanto,

$$\begin{aligned} p_1p_2 &\equiv p_1'p_2' \pmod{Q_j} \\ p_1 &\equiv p_1' \pmod{Q_k/Q_j}. \end{aligned}$$

Para probar iv) observemos que las desigualdades sobre los primos p_1, p_2, p_1', p_2', aquellas sobre los q_i y lo demostrado en ii) implican

$$Q_k^c Q_j^c > |p_1p_2 - p_1'p_2'| \geq Q_j \Longrightarrow Q_j < Q_k^{\frac{c}{1-c}}. \tag{2.14}$$

En particular se tiene que $j < k$ y podemos aplicar la parte iii), que implica la desigualdad

$$Q_k^c > |p_1 - p_1'| \geq Q_k/Q_j \Longrightarrow Q_j > Q_k^{1-c}. \tag{2.15}$$

Las desigualdades (2.14) y (2.15) implican iv). □

Observemos que si hubiera sumas repetidas, entonces la proposición 7.0.10, 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 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 7.0.10 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 7.0.10, iv).

Seguidamente observemos que gracias a las partes ii) and iii) de la Proposition 7.0.10 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 $A_{\overline{q},c}^*(x) = x^{c+o(1)}$ 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

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

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

$$|S_{j,k}| \le \left(2 \cdot \frac{Q_j^c Q_k^c}{jkQ_j}\right)\left(\frac{Q_j^c Q_k^c Q_j}{jkQ_k}\right) \le 2\frac{Q_j^{2c} Q_k^{2c-1}}{j^2k^2}. \tag{2.16}$$

Utilizando (2.16), la identidad

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

para $c = \sqrt{2} - 1$ y la estimación (2.9) en el último paso, tenemos, para k suficientemente grande, la estimación requerida,

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

Precisamente el valor $c = \sqrt{2} - 1$ sale de la igualdad $\frac{2c^2}{1-c} + 2c - 1 = c$.

2.2.5. Sucesiones B_h infinitas

Ejercicio 2.2.5. 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 [17] 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.

Aconsejamos a quienes no estén familiarizados con el método probabilístico que pospongan esta lectura hasta después del capítulo 4.

Teorema 2.2.4 (Cilleruelo [12])**.** *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

$$\begin{array}{rcl} b_{p_1} + \cdots + b_{p_l} & = & b_{p'_1} + \cdots + b_{p'_l} \\ \{b_{p_1}, \ldots, b_{p_l}\} & \cap & \{b_{p'_1}, \ldots, b_{p'_l}\} = \emptyset \\ b_{p_1} \geq & \cdots & \geq b_{p_l} \\ b_{p'_1} \geq & \cdots & \geq b_{p'_l}. \end{array} \tag{2.17}$$

La siguiente proposición es una generalización de la Proposition 7.0.10.

Proposición 2.2.2. *Supongamos que existen* $p_1, \ldots, p_l, p'_1, \ldots, p'_l \in \mathcal{B}_{\overline{q},c}$ *satisfaciendo* (2.17)*. Entonces se tiene que:*

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

$$p_1 \cdots p_l \equiv p'_1 \cdots p'_l \qquad (\text{mód } Q_{k_l})$$

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

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 7.0.10: 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 $\mathcal{R}_k(\overline{q}) = \{p \in \mathcal{P}_k : b_p \text{ es el mayor elemento en alguna ecuación (2.17)}\}$.

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 2.2.4 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

$$\mathrm{Bad}_l(\overline{q}, k_l, \dots, k_1) = \{(p_1, \dots, p_l') : \ p_i, p_i' \in \mathcal{P}_{k_i}, \ i = 1, \dots, l \text{ satisfying (2.17)}\}.$$

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,

$$\begin{aligned} |\mathcal{R}_k(\overline{q})| &\le \sum_{l=2}^{h} \sum_{k_l \le \cdots \le k_1 = k} |\mathrm{Bad}_l(\overline{q}, k_l, \dots, k_1)| \qquad (2.18) \\ &\le h k^{h-1} \max_{\substack{2 \le l \le h \\ k_l \le \cdots \le k_1 = k}} |\mathrm{Bad}_l(\overline{q}, k_l, \dots, k_1)|. \end{aligned}$$

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 Proposición2.2.2, 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 2.2.2 iii) en la última desigualdad tenemos que:

$$\begin{aligned}\mathbb{E}(|\{(p_1,\dots,p_l') \ : \ & p_i,p_i'\in\mathcal{P}_{k_i},\ i=1,\dots,l \text{ satisfying (2.17)}\}|)\\ \leq & \ e^{-k_1^2+O(k_1^2/\log k_1)}|\{(p_1,\dots,p_l'):\ p_i,p_i'\in\mathcal{P}_{k_i}\}|\\ \leq & \ e^{-k_1^2+O(k_1^2/\log k_1)}|\mathcal{P}_{k_1}|^2\cdots|\mathcal{P}_{k_l}|^2\\ \leq & \ e^{-k_1^2+O(k_1^2/\log k_1)}\cdot e^{2f(k_1)+\cdots+2f(k_l)}\\ \leq & \ e^{-k_1^2+\frac{2c}{1-c}\left(k_1^2+\cdots+k_{l-1}^2\right)-(2c+o(1))k_1^2/\sqrt{\log k_1}}\\ \leq & \ e^{\left(-1+\frac{2c(l-1)}{1-c}\right)k_1^2-(2c+o(1))k_1^2/\sqrt{\log k_1}}.\end{aligned}$$

Y usando (2.18) 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

Sucesiones con función de representación acotada

3.1. Sucesiones $B_2[g]$ finitas

Los conjuntos de Sidon tienen una generalización muy natural cuando permitimos que cada elemento del conjunto tenga a lo más g representaciones distintas como suma de dos elementos del conjunto, salvo por el orden de los sumandos. Para clarificar la definición llamaremos $r_A(x)$ a la función

$$r_A(x) = |\{\{a, a'\} : \ x = a + a', \ a, a' \in A\}|$$

que es distinta de la función de representación de A que se define de la forma

$$r_{A+A}(x) = |\{(a, a') : \ n = a + a', \ a, a' \in A\}|$$

Definición 3.1.1. *Sea G un grupo conmutativo. Un conjunto $A \subset G$ es un conjunto $B_2[g]$ si $r_A(x) \leq g$ para todo $x \in G$.*

Observemos que si A es un conjunto $B_2[g]$ entonces

$$r_{A+A}(x) \leq 2r_A(x) \leq 2g$$

para todo $x \in G$. Los conjuntos $B_2[1]$ son simplemente los conjuntos de Sidon.

Definimos $F_2(g;n)$ como el mayor cardinal que puede tener un conjunto $B_2[g]$ en $\{1,\dots,n\}$:

$$F_2(g;n) = \text{máx}\{|A| :\ A \subset \{1,\dots,n\},\ A \text{ es } B_2[g]\}.$$

El siguiente argumento permite obtener una cota superior para $F_2(g;n)$.

$$|A|^2 = \sum_{2\le x\le 2n} r_{A+A}(x) \le 4gn \implies |A| \le 2\sqrt{gn}.$$

Y con un argumento más refinado (ver [9] o [13]) podemos mejorarlo un poco más todavía.

Teorema 3.1.1.

$$F_2(g;n) \le 2\sqrt{(g-1/2)n} + 1.$$

Demostración. Por brevedad escribimos $r(x) = r_{A+A}(x)$ y $d(x) = r_{A-A}(x)$. Como A es una sucesión $B_2[g]$, tenemos que $r(x) \le 2g$ para todo x. Utilizaremos las identidades

$$\begin{aligned} \sum_x r(x) &= \sum_x d(x) = |A|^2 \\ d(0) &= |A| \\ \sum_x r^2(x) &= \sum_x d^2(x) \end{aligned}$$

que ya fueron comentadas el el capítulo 1. Entonces

$$\begin{aligned} \sum_{x\neq 0} d^2(x) &= \sum_x d^2(x) - |A|^2 \\ &= \sum_x r^2(x) - |A|^2 \\ &\le \sum_x r(x)(r(x)-2g) + 2g\sum_x r(x) - |A|^2 \\ &\le (2g-1)|A|^2. \end{aligned} \tag{3.1}$$

Por otro lado,

$$\sum_{x\neq 0} d^2(x) = \sum_{1\le|x|\le n} d^2(x) \ge \frac{\left(\sum_{x\neq 0} d(x)\right)^2}{2n} = \frac{\left(|A|^2-|A|\right)^2}{2n}. \tag{3.2}$$

De (3.1) y (3.2) se obtiene la desigualdad del teorema. □

Cuando g es grande esta cota no es mucho mejor que la trivial pero la constante 2 en la cota superior se puede mejorar con un método más sofisticado. Se logró por primera vez en [18] y fue el resultado principal de la tesis doctoral de Carlos Trujillo [63]. Esta mejora y otras posteriores quedan reflejadas en la siguiente tabla que refleja el valor de C para el cual se tiene que $F_2(g,N) \leq C\sqrt{gN}(1+o(1))$:

$C = 2$ (trivial)
$C = 1{,}864...$ (J. Cilleruelo - I. Z. Ruzsa - C. Trujillo, [18])
$C = 1{,}844...$ (B. Green, [32])
$C = 1{,}839...$ (G. Martin - K. O'Bryant, [48])
$C = 1{,}7888...$ (G. Yu, [66])
$C = 1{,}7802...$ (G. Martin - K. O'Bryant, [**?**])

Una manera de construir conjuntos $B_2[g]$ consiste en pegar conjuntos de Sidon adecuadamente; es decir, añadir traslaciones de un conjunto de Sidon en un grupo cíclico. En la tabla siguiente quedan reflejadas las sucesivas cotas inferiores de la forma $F_2(g,N) \geq c\sqrt{gN}(1+o(1))$ que se fueron consiguiendo de esta forma:

$c = 1$ (P. Erdős, M. Kolountzakis [39])
$c = 1{,}06...$ (J. Cilleruelo - I. Z. Ruzsa - C. Trujillo, [18])
$c = 1{,}121...$ (B. Green, [32])
$c = 1{,}128...$ (J. Cilleruelo - C. Vinuesa, [16])

No se conoce el comportamiento asintótico de $F_2(g;n)$ cuando $n \to \infty$ excepto cuando $g = 1$, donde ya hemos visto que $F_2(1;n) \sim \sqrt{n}$. De hecho ni siquiera se sabe si existe un comportamiento asintótico (aunque se cree que sí). Sin embargo en [18] se introdujeron nuevas ideas que permitieron dar una respuesta bastante satisfactoria a este problema. La demostración es demasiado compleja para ser incluida en este curso.

Teorema 3.1.2. *Para todo g existen $\underline{\sigma}_g$ y $\overline{\sigma}_g$ tales que*

$$\underline{\sigma}_g\sqrt{gN}(1+o(1)) \leq F_2(g,N) \leq \overline{\sigma}_g\sqrt{gN}(1+o(1))$$

y

$$\lim_{g\to\infty} \underline{\sigma}_g = \lim_{g\to\infty} \overline{\sigma}_g = \sigma$$

donde

$$\sigma = \sup_f \int_0^1 f(x)dx$$

y el supremo se toma sobre todas las funciones positivas integrables f tales que

$$\int f(y)f(x-y)dx \leq 2$$

para todo x.

La constante σ del Teorema 3.1.2 es difícil de calcular. Durante mucho tiempo se pensó que $\sigma = \sqrt{8/\pi}$ y que la función $f(x) = \sqrt{\frac{2}{\pi}}\frac{1}{\sqrt{x}}$ en $x \in [0,1]$ y $f(x) = 0$ cuando $x \notin [0,1]$ era la función para la que se alcanzaba el supremo. Pero recientemente M. Matolcsi y C.Vinuesa [49] han construido otra función que muestra que σ es mayor que esa cantidad y han demostrado que $1{,}6276\cdots \leq \sigma \leq 1{,}7713\ldots$.

3.1.1. Conjuntos $B_2[g]$ en grupos cíclicos

Si definimos $F_2(g;G) = \max\{|A|,\ A \subset G,\ A \text{ es } B_2[g]\}$, es claro que

$$\binom{|A|+1}{2} \leq g|G| \implies |A| \leq \sqrt{2g}\sqrt{|G|}. \tag{3.3}$$

La demostración del Teorema 3.1.1 se puede adaptar para refinar la cota superior anterior:

$$|A| \leq \sqrt{2g-1}\sqrt{|G|} + 1. \tag{3.4}$$

El valor asintótico de $F_2(g;G)$ se desconoce en general, incluso para $g = 1$. En ese caso, como ya vimos en el capítulo 1, se conoce para algunas familias de grupos. De hecho, si definimos

$$\alpha_g = \limsup_{m\to\infty} \frac{F_2(g;\mathbb{Z}_m)}{\sqrt{m}},$$

de las construcciones de conjuntos de Sidon en grupos cíclicos que vimos se deduce que $\alpha_1 = 1$. Para $g = k^2$, Martin y O'Bryant [47] demostraron que $\alpha_g \geq \sqrt{g}$. Observemos que (3.4) implica que $\alpha_g \leq \sqrt{2g-1}$. No es tan fácil, sin embargo, obtener una buena cota inferior para α_g.

Un ingrediente clave en la demostración del Teorema 3.1.2 fue la siguiente estimación asintótica de α_g. Al lector interesado en su demostración le remitimos a [18].

Teorema 3.1.3. $\alpha_g = \sqrt{2g} + O(g^{3/10})$.

Ejercicio 3.1.1. *Demostrar que* $F_2(g, G) \leq \sqrt{2g-1}\sqrt{n} + 1$ *para cualquier grupo conmutativo de* n *elementos.*

3.2. Sucesiones $B_h[g]$ infinitas

Como ya comentamos en el capítulo anterior, Erdős conjeturó que para todo $\epsilon > 0$ existe una sucesión de Sidon infinita A tal que $A(x) \gg x^{1/2-\epsilon}$. En general conjeturó que existe una sucesión B_h infinita A con $A(x) \gg x^{1/h-\epsilon}$. En apoyo a esta conjetura, sí que se sabe que es cierto si relajamos la condición de ser de B_h a ser $B_h[g]$ para un $g = g(h, \epsilon)$. Más concretamente:

Teorema 3.2.1. *Para todo* $h \geq 2$ *y para todo* $\epsilon > 0$ *existe un* $g = g(h, \epsilon)$ *y una sucesión* $B_h[g]$ *con función contadora* $A(x) \gg x^{1/h-\epsilon}$.

Este resultado fue demostrado por Erdős y Renyi para $h = 2$ con el método probabilístico. Se comentará después y se verá su demostración en el capítulo 4. Aunque ellos afirmaron que su demostración se generalizaba fácilmente para $h \geq 3$, lo cierto es que no tuvieron en cuenta las dificultades que surgen al tratar con sucesos que no son independientes. Años antes, en el survey que Erdős y Freud [27] escribieron sobre los conjuntos de Sidon aparece un esbozo de una construcción explícita de Ruzsa que apareció publicada con todo detalle y bastantes años más tarde en [20]. Así que la primera demostración correcta del Teorema 1.4.1 hay que atribuírsela a Ruzsa. Esa es la demostración que ofrecemos aquí.

Demostración del Teorema 1.4.1. Dados h y ϵ, vamos a construir una sucesión A con $r_{h,A}(n)$ acotada y probaremos que $A(n) > n^{1/h-\varepsilon}$ para n suficientemente grande, que implica el Teorema 3.2.1.

Dada una sucesión en enteros positivos $q_1, q_2, \ldots,$ (la base) todo número natural x puede ser expresado de manera única de la forma

$$x = b_0 + b_1 q_1 + b_2 q_1 q_2 + \cdots + b_s q_1 \cdots q_s + \cdots,$$

donde $0 \le b_i < q_{i+1}$. Los b_i's son los "digitos" de x en la base dada.

Sea $l \ge 2$, un entero positivo suficientemente grande que será fijado más tarde. Fijamos los conjutos $0 \in A_i \subset \left[0, \frac{q_i}{h}\right)$ tales que los A_i's son conjutos maxiales con la condición $r_{h,A_i}(n) \le 1$ para todo n. Sabemos (ver por ejemplo Teorema 1.4.1) que si p es primo, hay un conjunto B_h en $[0, p^h - 2]$ con p elementos. Combinando este resultado con el Postulado de Bertrand podemos asumir que

$$|A_i| > \frac{1}{2}\left(\frac{q_i}{h}\right)^{1/h}. \tag{3.5}$$

Sea A el conjunto de aquellos números naturales n con las ds propiedades siguientes:

i) Cada dígito b_i of n satisface $b_i \in A_{i+1}$.

ii) Existe un entero m tal que $b_i = 0$ para $i \notin [m+1, \dots, m+l]$.

Primero demostrareos que $r_{h,A}(n) < (h!)^{lh}$. Sumemos h elementos de A: a_1, a_2, $\dots$, a_h.

Como el dígito j de cada sumando está en $\left[0, \frac{q_j}{h}\right)$, el dígito j de la suma será la suma de los dígitos j de $a_1, \dots, a_h$. (en otras palabras, no nos llevamos ninguna al sumar).

Y como el dígito j de cada suamando esta en un conjunto B_h, el dígito j de la suma sólo se puede obtener de una manera como suma de h dígitos. Observemos que los h números tienen $h!$ permutaciones, así que para cada dígito de la suma podríamos tener los h sumandos distribuidos a lo más de $h!$ maneras diferentes.

Finalmente, observar que los dígitos no nulos de la suma de h elementos de A son a lo más hl. Por lo tanto tenemos que $r_{h,A}(n) \le (h!)^{lh}$ para todo n.

Ahora daremos una estimación del valor de $A(n)$. Dado n, sabemos que existe j tal que

$$q_1 q_2 \cdots q_j \le n < q_1 q_2 \cdots q_{j+1}. \tag{3.6}$$

Es claro que los enteros con dígitos

$$b_i \in A_{i+1}, \quad i = j-l, \dots, j-1,$$

y $b_i = 0$ en otro caso están en A. Sea N el número de estos enteros. Definnios $r = \dfrac{\log_2 l}{l}$ y, para $i \geq 1$,

$$q_i = \lfloor e^{(1+r)^{i-1}} \rfloor. \tag{3.7}$$

Como $\frac{e^{(1+r)^{i-1}}}{2} \leq q_i \leq e^{(1+r)^{i-1}}$ y $2(2h)^{1/h} \leq 2e^{2/e} < e^2$, la desigualdad (3.5) implica

$$|A_i| > \frac{1}{2}\left(\frac{e^{(1+r)^{i-1}}}{2h}\right)^{1/h} > e^{\frac{(1+r)^{i-1}}{h}-2}. \tag{3.8}$$

Primero daremos una cota para $\log n$. De (3.6) y (3.7) se sigue que

$$\log n < \log(q_1 \cdots q_{j+1}) \leq 1 + (1+r) + \cdots + (1+r)^j < \frac{(1+r)^{j+1}}{r}. \tag{3.9}$$

Seguidamente daremos una estimación inferior para $\log N$. Aplicando (3.8) tenemos

$$\begin{aligned} \log N = \sum_{i=j-l+1}^{j} \log|A_i| &> \frac{(1+r)^{j-l} + \cdots + (1+r)^{j-1}}{h} - 2l \\ &= \frac{(1+r)^j}{hr}(1-(1+r)^{-l}) - 2l. \end{aligned} \tag{3.10}$$

Por (3.9) y (3.10) tenemos

$$\begin{aligned} \frac{h\log N}{\log n} &> \frac{(1+r)^j(1-(1+r)^{-l})}{(1+r)^{j+1}} - \frac{2lrh}{(1+r)^{j+1}} \\ &= \frac{1-(1+r)^{-l}}{1+r} - \frac{2lrh}{(1+r)^{j+1}}. \end{aligned} \tag{3.11}$$

Usando que $\frac{1}{1+r} > 1-r$ y que $\left(1+\frac{\log_2 l}{l}\right)^{\frac{l}{\log_2 l}} \geq 2$ para todo $l \geq 2$, tenemos

$$\begin{aligned} \frac{1-(1+r)^{-l}}{1+r} &> 1 - r - (1+r)^{-l} = 1 - \frac{\log_2 l}{l} - \left(1+\frac{\log_2 l}{l}\right)^{-l} \\ &> 1 - \frac{\log_2 l}{l} - \frac{1}{l} > 1 - \frac{2\log_2 l}{l}. \end{aligned} \tag{3.12}$$

Por otro lado, como $\lim_{j\to\infty} \frac{2lrh}{(1+r)^{j+1}} = 0$ tenemos que, para j suficientemente garnde,

$$\frac{2lrh}{(1+r)^{j+1}} < \frac{\log_2 l}{l}. \tag{3.13}$$

Finalmente, de (3.11), (3.12) y (3.13) tenemos que

$$\frac{h\log N}{\log n} > 1 - \frac{3\log_2 l}{l},$$

para n suficientemente grande.

Terminamos la demostración del Teorema 3.2.1 tomando, para un $\epsilon > 0$ dado, un entero l, suficientemente grande tale que $\frac{3\log_2 l}{l} < h\epsilon$, porque entonces $\log N > \left(\frac{1}{h} - \epsilon\right)\log n$, i. e. $N > n^{1/h-\epsilon}$.

□

Un pequeño comentario acerca de la the dependencia de g sen función de ϵ. Observemos que nuestro g es $(h!)^{lh}$ y que, dado ϵ, necesitamos elegir un valor grande de l, digamos $l \gg \epsilon^{-1}\log\epsilon^{-1}$. Esto hace que la dependencia de g en función de ϵ sea muy mala. El valor de g que se consigue con la construcción anterior depende de ϵ^{-1} más que exponentialmente.

Volviendo a la demostración probabilística de Erdős y Renyi, la dependencia que se obtiene es nucho mejor y queda reflejada en el siguiente teorema.

Teorema 3.2.2. *Para todo g y para todo $\beta < \frac{1}{2} - \frac{1}{2(g+1)}$ existe una sucesión $B_2[g]$ con función contadora $A(x) \gg x^\beta$.*

Posponemos la demostración al capítulo siguiente dedicado íntegramente al método probabilístico.

En [11] se demuestra que el teorema anterior también es cierto para todo $\beta < \frac{1}{2} - \frac{1}{4g+2}$ utilizando el método de alteración. Es decir, no es cierto que para estos valores de β casi toda sucesión es $B_2[g]$, pero sí que es cierto que el número de enteros n en cada intervalo diádico que tienen más de g representaciones como suma de dos elementos son suficientemente excasos como para poder destruir esas representaciones malas eliminando pocos elementos de la sucesión.

Para $h \geq 3$, Vu [65] dio una demostración probabilística del Teorema 3.2.1 donde $g \ll \epsilon^{-h}$. En [20] se da otra demostración probabilística diferente con $g \ll_h \epsilon^{-1}$.

Ejercicio 3.2.1. *Demostrar que si* $F_2(g;n) \geq c\sqrt{gn}(1+o(1))$ *entonces existe una sucesión* $B_2[g]$ *infinita* A *tal que*

$$\limsup_{N\to\infty} \frac{A(N)}{\sqrt{N}} \geq c\sqrt{g/2}.$$

3.2.1. La conjetura de Erdős-Turan

En el Teorema 2.1.1 se demostraba que no existe ninguna sucesión infinita de Sidon A tal que $A(x) \gg x^{1/2}$. Erdős y Turan conjeturaron que la misma conclusión debería ser cierta para sucesiones $B_2[g]$ infinitas.

Conjetura 3.2.1 (Conjetura fuerte de Erdős-Turan)**.** *Si* A *es una sucesión* $B_2[g]$ *entonces* $\liminf_{x\to\infty} A(x)/\sqrt{x} = 0$.

Esta conjetura está considerada como uno de los problemas abiertos más importantes en la Teoría Combinatoria de Números. El hecho de que las sucesiones $B_2[g]$ no puedan caracterizarse bien en términos de diferencias (como pasaba con los conjuntos de Sidon) es el que impide utilizar la misma estrategia que se usó en el Teorema 2.1.1. El Problema 3.2.2 ilustra bien este hecho.

El adjetivo "conjetura fuerte"se debe a que es más fuerte que otra conjetura, más conocida pero menos natural, que también propusieron Erdős y Turan.

Conjetura 3.2.2 (Conjetura de Erdős- Turan)**.** *No existe ninguna sucesión infinita* A *para la que exista una constante* g *con la propiedad de que* $1 \leq r_A(n) \leq g$ *para todo* n *suficientemente grande.*

Es decir, que una sucesión $B_2[g]$ no puede ser una base asintótica.

Ejercicio 3.2.2. Demuestrar que la Conjetura de Erdős Turan es cierta si sustituimos $r_A(n)$ por $d_A(n) = \{(a,a') : \ a,a' \in A, \ a-a' = n\}$.

Ejercicio 3.2.3. *Demostrar que existe una sucesión de enteros positivos* A *con* $A(x) \gg x^{1/3}$ *y con la propiedad de que todo entero distinto de cero*

se puede escribir, de manera única, como diferencia de dos elementos de la sucesión.

En [15] se demuestra que dada una sucesión infinita de Sidon A, existe una sucesión de enteros positivos B con $B(x) \gg A(x/3)$ y con la propiedad de que todo entero distinto de cero se puede escribir, de manera única, como diferencia de dos elementos de la sucesión. En particular existe tal sucesión B con $B(x) \gg x^{\sqrt{2}-1+o(1)}$.

3.3. Bases

Definición 3.3.1. *Se dice que una sucesión de enteros no negativos A es una base (asintótica) de orden h si todo entero no negativo (suficientemente grande) se puede escribir como suma de h elementos de A.*

Por ejemplo, un resultado clásico de Lagrange dice que la sucesión de los cuadrados es una base de orden 4. Más en general, Hilbert demostró el problema de Waring: para todo $k \geq 1$, existe una constante g_k de talmanera que la sucesión $\{n^k : \ n \geq 0\}$ es una base de orden g_k.

Otro ejemplo notable es la sucesiónd de los primos, que después del teorema de Harald Helfggot sabemos que son una base de orden 3 para los impares mayores que 5. La conjetura de Goldbach afrima que la sucesión de los primos es una base de orden 2 para los pares mayores que 2.

Es claro que cuanto más densa sea una sucesión más fácil es que sea una base. Por el contrario, si la sucesión es muy densa, más difícil es que sea una sucesiónd e Sidon o una sucesión B_h. Otra manera de enunciar la conjetura de Erdős Turan es diciendo que no puede existir una sucesión $B_2[g]$ que sea una base asintótica de orden 2.

Si A es una base de orden h entonces, para todo n, cualquier entero menor o igual que n se escribe como suma de h elementos de A menores o iguales que n. Como el número de h-tuplas $(a_1, \ldots, a_h),\ a_1 \leq \cdots \leq a_h \leq n,\ a_i \in A$ es $\binom{A(n)+h-1}{h} \geq n$, tenemos la desigualdad trivial

$$\binom{A(n)+h-1}{h} \geq n,$$

de donde

$$A(n) \geq (h!n)^{1/h}(1 + o(1).$$

Por otro lado es fácil construir bases de orden h con función contadora $A(n) \ll n^{1/h}$. Considerése por ejemplo la sucesión

$$A = \bigcup_{k=0}^{h-1} A_k \tag{3.14}$$

donde

$$A_k = \left\{ \sum_{s \equiv k \pmod h,\ s \geq 0} \epsilon_s 2^s : \ \epsilon_s \in \{0, 1\} \right\}.$$

Para ver que A es una base de orden h observemos que todo entero positivo n puede escribirse de la forma

$$n = \sum_{s \geq 0} \epsilon_s 2^s, \ \epsilon_s \in \{0, 1\}.$$

Por lo tanto podeos escribir n como suma de h elementos:

$$n = n_1 + \cdots + n_h$$

donde

$$n_k = \sum_{\substack{s \geq 0 \\ s \equiv k \pmod h}} \epsilon_s 2^s \in A_k \subset A.$$

Dejamos como ejercicio la estimación del orden de magnitud de $A(x)$.

Ejercicio 3.3.1. *Demostrar que la función contadora de la sucesión A descrita en* (3.14) *satisface $A(x) \gg x^{1/h}$.*

No es difícil demostrar que una sucesión de Sidon no puede ser una base asintótica de orden 2. Una conjetura famosa de Erdős afirma que la exitencia de una sucesión de Sidon que es base asintótica de orden 3.

Conjetura 3.3.1 (Erdős)**.** *Existen sucesiones de Sidon que son bases asintóticas de orden* 3*.*

Recientemente ha habido importantes avances en esta dirección. Alain Plagne y Jean Marc Deshouillers construyeron de manera explícita una sucesión de Sidon que es base asintótica de orden 7 y posteriormene Sandor Kiss rebajo el orden a 5. En el capítulo 4 se prueba este teorema. De hecho el orden se ha rebajado a 4 e incluso a $3+\epsilon$ para todo $\epsilon > 0$. Explicaremos que queremos decir con esto.

Definición 3.3.2. *Decimos que A es una base asintótica de orden $h+\epsilon$ si todo entero n suficientemente grande se puede escribir de la forma*

$$n = a_1 + \cdots + a_h + a_{h+1}, \quad a_{h+1} \leq n^{\epsilon},\ a_1, \ldots, a_{h+1} \in A.$$

En [8] se ha demostrado el siguiente teorema.

Teorema 3.3.1. *Para todo $\epsilon > 0$ existe una sucesiónde Sidon que es una base asintótica de orden $3+\epsilon$.*

La demostración es demasiado complicada para ser incluida en este curso pero uno de los ingredientes de la demostración es la existencia de conjuntos de Sidon en grupos cíclicos $\mathbb{Z}_n$ que son bases de orden 3. Aunque en [8] se demuestra la existencia de dichos conjuntos para todo n suficientemente grande, aquí nos conformaremos deostrándolo para infinitos valores de n.

Teorema 3.3.2. *Existen infinitos grupos cíclicos Z_n que contienen conjuntos de Sidon que son bases de orden 3.*

Demostración. Ya hemos visto que para todo primo p y para todo g, generador de $\mathbb{F}_p^*$, el conjunto

$$S = \{(x, g^x) :\ x = 0, \ldots, p-2\}$$

es un conjunto de Sidon en $\mathbb{Z}_{p-1} \times \mathbb{Z}_p$. Demostraremos que S es también una base de orden 3. En otras palabras, que todo elemento $(a,b) \in \mathbb{Z}_{p-1} \times \mathbb{Z}_p$ se puede escribir de la forma

$$(a,b) = (x_1, g^{x_1}) + (x_2, g^{x_2}) + (x_3, g^{x_3}). \tag{3.15}$$

De hecho probaremos que el número de soluciones de (3.15) coincide exactamente con el número de puntos $(U,V),\ V \neq 0$ de la curva elíptica $U^2 = 4V^3 + (bV + g^a)^2$ en $\mathbb{F}_p$.

Vamos a contar, para cada $(a,b) \in \mathbb{Z}_{p-1} \times \mathbb{Z}_p$, el número de soluciones (x_1,x_2,x_3) del sistema

$$\begin{aligned} x_1+x_2+x_3 &\equiv a \pmod{p-1} && (3.16)\\ g^{x_1}+g^{x_2}+g^{x_3} &\equiv b \pmod{p}. && (3.17)\end{aligned}$$

Este puede reducirse al la congruencia

$$g^{x_1}+g^{x_2}+g^{a-x_1-x_2} \equiv b \pmod{p},$$

que a su vez es equivalente a la ecuación

$$X+Y+\frac{\lambda}{XY} \equiv b \pmod{p} \qquad (3.18)$$

después de hacer los cambios $g^{x_1}=X,\ g^{x_2}=Y,\ g^a=\lambda$. Haceos ahora un nuevo cambio de variables:

$$X=\frac{2V^2}{U-bV-\lambda}, \qquad Y=-\frac{\lambda}{V}.$$

Como $XY \neq 0$ tenemos que añadir las condiciones $V \neq 0,\ U \neq bV+\lambda$. Con estas restricciones el cambio de variable es biyectivo y (3.18) es equivalente a la ecuación

$$\begin{aligned} \frac{2V^2}{U-bV-\lambda}-\frac{\lambda}{V}-\frac{U-bV-\lambda}{2V} &\equiv b \pmod{p}\\ \iff \frac{2V^2}{U-bV-\lambda} &\equiv \frac{U+bV+\lambda}{2V} \pmod{p}\\ \iff 4V^3+(bV+\lambda)^2 &\equiv U^2 \pmod{p}. \end{aligned}$$

Cada punto de esta curva elíptica (excepto $(U,V)=(\pm\lambda,0)$) corresponde a una solución (X,Y) de (3.18). Por el Teorema de Hasee [37] sabemos que la curva elíptica tiene $p+O(\sqrt{p})$ puntos (U,V). □

3.4. Sucesiones con función de representación constante

Estando claro que la conjetura de Erdős-Turan es un problema muy difícil, nos podemos hacer preguntas que estén más alcance de nuestra

mano. Por ejemplo, ¿Existe alguna sucesión infinita de enteros no negativos A que $r_{A+A}(n)$ sea constante para n suficientemente grande? Un momento de reflexión nos lleva a la concluisón de que esto no puede ser cierto porque $r_{A+A}(n)$ es impar si $n = 2a$ para algún $a \in A$ y es par en otro caso. Para evitar esta contradicción trivial provocada por la simetría de la función $r_{A+A}(n)$, consideremos en su lugar la función $r_A(n) = \{(a, a') : \ a + a' = n, \ a \le a'\}$.

¿Existe una sucesión de enteros no negativos A con $r_A(n)$ constante para todo n suficientemente grande? La respuesta también es negativa pero el argumento es más sutil. Es una bonita aplicación de las funciones generatrices.

Teorema 3.4.1 (Dirac [24])**.** *No existe ninguna sucesión infinita de enteros no negativos A tal que $r_A(n)$ sea constante para todo n suficientemente grande.*

Demostración. La función generatriz de A es la función $f(x) = \sum_{a\in A} x^a$. La primera observación es que

$$f^2(x) = \sum_{a,a'\in A} x^{a+a'} = 2\sum_{a\le a'} x^{a+a'} - \sum_{a\in A} x^{2a} = 2\sum_n r_A(n)x^n - f(x^2).$$

Supongamos $r_A(n) = c$ para $n \ge n_0$. Entonces

$$f(x^2) \le f^2(x) + f(x^2) = 2\sum_{n<n_0} r_A(n)x^n + 2c\sum_{n\ge n_0} x^n = \frac{P(x)}{1-x}$$

para algún polinomio $P(x)$ de grado a lo más n_0. La contradicción aparece tomando el límite cuando $x \to -1$:

$$\lim_{x\to -1} f(x^2) = +\infty \quad \text{y} \quad \lim_{x\to -1} \frac{P(x)}{1-x} = \frac{P(-1)}{2} < \infty.$$

□

Si llamamos $L_A = \limsup_{n\to\infty} r_A(n)$ y $l_A = \liminf_{n\to\infty} r_A(n)$, otra manera de enunciar el teorema es anterior es diciendo que si $L_A - l_A \ge 1$ para toda sucesión infinita de enteros no negativos. Todavía no he visto ninguna demostración de que $L_A - l_A \ge 2$. En esta dirección C. Sandor [57] ha demostrado que $L_A - l_A \ge 2\sqrt{L_A} - 1$.

En los últimos años se han estudiado otras funciones de representación. Consideremos para $j < k$ la función $r_{j,k}(n)$ asociada a una sucesión A, que cuenta el número de representaciones de n de la forma $n = ja + ka'$, $a, a' \in A$. Cuando $j = 1$ el resultado puede parecer sorprendente.

Teorema 3.4.2 (Moser, [50])**.** *Para todo $k \geq 2$ existe una sucesión de enteros no negativos A tal que $r_{1,k}(n) = 1$ para todo $n \geq 0$.*

Demostración. La demostración es constructiva. Veamos quién tendría que ser A si existiera. Es claro que si $f(x) = \sum_{a\in A} x^a$ es la función generatriz de A entonces

$$\begin{aligned} f(x)f(x^k) &= \left(\sum_{a\in A} x^a\right)\left(\sum_{a'\in A} x^{ka'}\right) \\ &= \sum_{a,a'\in A} x^{a+ka'} = \sum_n r_{1,k}(n)x^n \\ &= \sum_{n\geq 0} x^n = \frac{1}{1-x}. \end{aligned}$$

Y sustituyendo x por x^k tenemos que

$$f(x^k)f(x^{k^2}) = \frac{1}{1-x^k}.$$

Es decir,

$$f(x) = \frac{1-x^k}{1-x} f(x^{k^2}) = \left(1 + x + x^2 + \cdots + x^{k-1}\right) f(x^{k^2}).$$

Iterando esta igualdad obtenemos que la función generatriz es

$$f(x) = \prod_{j=0} \left(1 + x^{(k^2)^j} + x^{2(k^2)^j} + \cdots + x^{(k-1)(k^2)^j}\right) f(x^{k^2}).$$

Desarrollando el producto vemos que A es la sucesión de todos los enteros no negativos con todos sus dígitos en $\{0, 1 \ldots, k-1\}$ cuando se escribe en base k^2. □

Por el contrario, en [21] se demostró que si $1 < j < k$ entonces no existe ninguna sucesión infinita A para la que $r_{j,k}(n)$ sea constante para n suficientemente grande.

Capítulo 4

El método probabilístico

4.1. El método probabilístico

El método probabilístico, muy ligado también a la figura de Paul Erdős, permite demostrar la existencia de objetos combinatorios (por ejemplo grafos o conjuntos de enteros con determinadas propiedades) que no se saben construir de manera explíta. Se ha convertido en una herramienta muy poderosa y activa en muchas áreas de las matemáticas y en particular en la combinatoria y la teoría de números. El libro [3] es una magnífica referencia del método probabilístico y en el libro [36] se hace un tratamiento exhaustivo del método probabilístico aplicado a los conjuntos de Sidon y problemas relacionados.

Comenzaremos con unos preliminares sobre probabilidad.

4.1.1. Preliminares

Recordamos que el valor esperado y la varianza de una variable aleatoria X que toma un número discreto de valores x se definen respectiamente como

$$\begin{aligned} \mu &= \mathbb{E}(X) = \sum_x x\mathbb{P}(X = x) \\ \sigma^2 &= \mathbb{E}((X-\mu)^2) = \mathbb{E}(X^2) - \mu^2. \end{aligned}$$

En el caso de que X no tome valores negativos tenemos, para todo $\lambda > 0$, la desigualdad

$$\mathbb{E}(X) \geq \sum_{x \geq \lambda} x\mathbb{P}(X = x) \geq \lambda \mathbb{P}(X \geq \lambda),$$

que se conoce como la desigualdad de Markov:

Proposición 4.1.1 (Desigualdad de Markov)**.** *Sea X una variable aleatoria no negativa. Entonces para todo $\lambda > 0$ tenemos que*

$$\mathbb{P}(X \geq \lambda) \leq \frac{\mathbb{E}(X)}{\lambda}. \tag{4.1}$$

Una consecuencia de la desigualdad de Markov es la desigualdad de Chebyshev:

Proposición 4.1.2 (Desigualdad de Chebyshev)**.** *Sea X una variable aleatoria no negativa con varianza σ^2. Entonces para todo $\lambda > 0$ tenemos que*

$$\mathbb{P}\left(|X - \mathbb{E}(X)| > \lambda\sigma\right) \leq \frac{1}{\lambda^2}. \tag{4.2}$$

Demostración. Simplemente aplicamos la desigualdad de Markov a la variable $Y = (X - \mathbb{E}(X))^2$ la cual satisface $\mathbb{E}(Y) = \sigma^2$:

$$\mathbb{P}\left(|X - \mathbb{E}(X)| > \lambda\sigma\right) = \mathbb{P}\left(Y > \lambda^2\sigma^2\right) \leq \frac{\mathbb{E}(Y)}{\lambda^2\sigma^2} = \frac{1}{\lambda^2}.$$

□

La desigualdad de Chebyshev cuantifica la concentración de una variable alrededor de su media. Pero cuando X es una variable que es suma de muchas variables independientes la concentración alrededor de la media es mucho mayor. Es de tipo exponencial.

Teorema 4.1.1 (Chernoff)**.** *Sean $X_1, \ldots, X_n$ variables aleatorias independientes tales que $|X_i - \mathbb{E}(X_i)| \leq 1$ para todo i. Sea $X = X_1 + \cdots + X_n$ y sea σ^2 la varianza de X. Entonces para todo $\lambda > 0$ se tiene que*

$$\mathbb{P}\left(|X - E(X)| \geq \lambda\sigma\right) \leq 2\,\text{máx}(e^{-\lambda^2/4}, 2^{-\lambda\sigma/2}).$$

Demostración. Por comodidad empezamos haciendo los cambios de variables

$$\begin{aligned} Y_i &= X_i - \mathbb{E}(X_i) \\ Y &= Y_1 + \cdots + Y_n. \end{aligned}$$

Es claro que las nuevas variables Y_i satisfacen $|Y_i| \leq 1$, $\mathbb{E}(Y_i) = 0$ y que además Y tiene la misma varianza σ^2 que tenía X.

Para $|t| \leq 1$ tenemos que

$$\mathbb{E}(e^{tY_i}) \leq \mathbb{E}(1 + tY_i + t^2 Y_i^2) = 1 + t^2 \mathrm{Var}(Y_i) \leq e^{t^2 \mathrm{Var}(Y_i)}. \tag{4.3}$$

La primera desigualdad es consecuencia de que $e^x \leq 1 + x + x^2$ si $|x| \leq 1$, y la segunda desigualdad se debe a que $1 + x \leq e^x$ para todo x.

Utilizando (4.3), la desigualdad de Markov y el hecho de que las variables Y_i son independientes (y por tanto las variables e^{tY_i}), tenemos, para todo λ real y para todo $|t| \leq 1$:

$$\begin{aligned} \mathbb{P}(Y \geq \lambda\sigma) &= \mathbb{P}\left(e^{tY} \geq e^{t\lambda\sigma}\right) \leq \frac{\mathbb{E}\left(e^{tY}\right)}{e^{t\lambda\sigma}} \\ &= \frac{\mathbb{E}\left(e^{tY_1} \cdots e^{tY_n}\right)}{e^{t\lambda\sigma}} = \frac{\mathbb{E}\left(e^{tY_1}\right) \cdots \mathbb{E}\left(e^{tY_n}\right)}{e^{t\lambda\sigma}} \\ &\leq \frac{e^{t^2 \mathrm{Var}(Y_1)} \cdots e^{t^2 \mathrm{Var}(Y_n)}}{e^{t\lambda\sigma}} = e^{-t\lambda\sigma} e^{t^2\sigma^2}. \end{aligned}$$

El valor de t que minimiza la parte derecha es $t = \frac{\lambda}{2\sigma}$. Así pues tomamos $t = \mín(1, \lambda/(2\sigma))$.

Si $\lambda \leq 2\sigma$ obtenemos que $\mathbb{P}(Y \geq \lambda\sigma) \leq e^{-\lambda^2/4}$.

Si $\lambda > 2\sigma$ obtenemos que $\mathbb{P}(Y \geq \lambda\sigma) \leq e^{-\lambda\sigma + \sigma^2} \leq e^{-\lambda\sigma/2}$.

Es decir, $\mathbb{P}(Y \geq \lambda\sigma) \leq \máx\left(e^{-\lambda^2/4}, 2^{-\lambda\sigma/2}\right)$. De manera análoga tenemos la misma estimación para $\mathbb{P}(Y \leq -\lambda\sigma)$, por lo que

$$\mathbb{P}(|Y| \geq \lambda\sigma) \leq 2\,\máx\left(e^{-\lambda^2/4}, 2^{-\lambda\sigma/2}\right).$$

□

El siguiente corolario cubrirá la mayoría de nuestras necesidades.

Corolario 4.1.1. *Sea $X = X_1 + \cdots + X_n$, con $X_i \in \{0,1\}$. Entonces para todo $\epsilon > 0$ se tiene que*

$$P\left(|X - \mathbb{E}(X)| \geq \epsilon \mathbb{E}(X)\right) \leq 2e^{-\min(\epsilon^2/4, \epsilon/2)\mathbb{E}(X)}.$$

Su demostración se deja como ejercicio

Ejercicio 4.1.1. Demostrar el Corolario 4.1.1.

El teorema de Borell-Cantelli es una pieza fundamental en el método probabilístico.

Teorema 4.1.2 (Borell-Cantelli)**.** *Sean $E_1, E_2, \ldots$ una sucesión de sucesos tales que $\sum_n \mathbb{P}(E_n) < \infty$. Entonces, para todo entero positivo M se tiene que*

$$\mathbb{P}(\textit{Ocurran menos de } M \textit{ sucesos } E_1, E_2, \ldots) \geq 1 - \frac{\sum_n \mathbb{P}(E_n)}{M}.$$

En particular, con probabilidad 1, ocurren a lo más un número finito de sucesos $E_1, E_2, \ldots$.

Demostración. Aplicamos la desigualdad de Markov a la variable aleatoria $Y = \sum_n \mathbf{1}(E_n)$ donde $\mathbf{1}$ es la función indicadora de un evento: $\mathbf{1}(E) = 1$ si el suceso ocurre, y $\mathbf{1}(E) = 0$ en caso contrario.

Utilizamos también el hecho de que $\mathbb{E}(Y) = \sum_n \mathbb{P}(E_n)$.

$$\begin{aligned} \mathbb{P}(Y < M) &= 1 - \mathbb{P}(Y \geq M) \\ &\geq 1 - \frac{\mathbb{E}(Y)}{M} \\ &= 1 - \frac{\sum_n \mathbb{P}(E_n)}{M}. \end{aligned}$$

□

4.2. Un problema de sumas distintas de Erdős

Según decía el propio Erdős [26], su primera conjetura seria, anterior incluso a las relativas a los conjuntos de Sidon, se refiere a un problema de sumas distintas que tiene un sabor parecido al de los conjuntos de Sidon.

Definición 4.2.1. *Decimos que un conjunto* $A = \{a_1, \ldots, a_k\}$ *es de sumas distintas si todas las sumas*

$$\epsilon_1 a_1 + \cdots + \epsilon_k a_k,\ \epsilon_i \in \{0, 1\}$$

son distintas.

El conjunto formado por las potencias de dos: $1, 2, \ldots, 2^k$ es el ejemplo más natural con esta propiedad. Erdős conjeturó que esencialmente es éste el conjunto más denso.

Conjetura 4.2.1 (Erdős)**.** *Si* $A = \{a_1, \ldots, a_k\}$ *es un conjunto de sumas distintas y* a_k *es el mayor elemento del conjunto, entonces* $a_k \gg 2^k$*.*

Conway y Guy encontraron un ejemplo con $a_k \leq 2^{k-2}$, más denso que el de las potencias de 2 pero que no contradecía la conjetura de Erdős.

Un argumento sencillo de conteo permite demostrar que

$$a_k \geq (2^k - 1)/k.$$

Hay 2^k sumas de la forma $\epsilon_1 a_1 + \cdots + \epsilon_k a_k$ con $\epsilon_i \in \{0, 1\}$ y todas ellas son distintas y no negativas. Así que la mayor de ellas ha de valer al menos $2^k - 1$. Si no fuera así alguna de esas sumas se tendrían que repetir. Por lo tanto

$$2^k - 1 \leq a_1 + \cdots + a_k \leq k a_k \implies a_k \geq (2^k - 1)/k.$$

Erdős probó que $a_k \geq \frac{2}{3\sqrt{3}} \frac{2^k}{\sqrt{k}}$ utilizando la desigualdad de Chebychev y lo dejamos como ejercicio.

Ejercicio 4.2.1. *Utilizar el Teorema de Chebychev para demostrar que si* $1 \leq a_1 < \cdots < a_k$ *tiene la propiedad de que todas las sumas de distintos elementos son distintas entonces* $a_k \geq \frac{2}{3\sqrt{3}} \frac{2^k}{\sqrt{k}}$.

Aquí damos una demostración alternativa que da una mejor constante.

Teorema 4.2.1. *Si* $A = \{1 \leq a_1 < \cdots < a_k\}$ *es un conjunto de sumas distintas entonces*

$$a_k \geq \frac{2^k}{\sqrt{3k}}.$$

Demostración. Sea X_i la variable aleatoria que toma los valores a_i y $-a_i$ con probabilidad 1/2. Es claro que $\mathbb{E}(X_i) = 0$ y que $\mathbb{E}(X_i^2) = a_i^2$.

Consideremos la variable

$$X = X_1 + \cdots + X_k.$$

Es claro que si $i \neq j$ entonces X_i, X_j son independientes y por tanto $\mathbb{E}(X_iX_j) = \mathbb{E}(X_i)\mathbb{E}(X_j) = 0$. Así que

$$\begin{aligned}\mathbb{E}(X^2) &= \sum_{i,j} \mathbb{E}(X_iX_j) = \sum_{i=1}^{k} \mathbb{E}(X_i^2) + \sum_{i\neq j} \mathbb{E}(X_iX_j)\\ &= \sum_{i=1}^{k} a_i^2 \leq k a_k^2.\end{aligned}$$

Por otra parte,

$$\mathbb{E}(X^2) = \sum_s s^2 \mathbb{P}(X = s)$$

donde s recorre todos los posibles valores que puede tomar X.

Observemos que cada uno de esos valores se toma con la misma probabilidad $P(X = s) = 2^{-k}$. Además todos ellos tienen la misma paridad que $a_1 + \cdots + a_k$ (es claro que $\epsilon_1 a_1 + \cdots + \epsilon_k a_k \equiv a_1 + \cdots + a_k \pmod 2$). Supongamos que $a_1 + \cdots + a_k$ es par (si fuera impar el razonamiento sería el mismo). En ese caso, el menor valor posible de $\mathbb{E}(X^2)$ corresponde al caso donde s recorre los 2^k pares, positivos y negativos, más cercanos a 0 (el 0 no se puede tomar porque daría lugar a dos sumas iguales). Utilizando también que $\sum_{1\leq j\epsilon n} j^2 = n(n+1)(2n+1)/6$ tenemos la desigualdad

$$\begin{aligned}\mathbb{E}(X^2) &\geq 2 \sum_{1\leq j\leq 2^{k-1}} (2j)^2 \cdot 2^{-k}\\ &= 2^{-k+3} \frac{2^{k-1}(2^{k-1}+1)(2^k+1)}{6}\\ &\geq \frac{2^{2k}}{3}\end{aligned}$$

De las cotas superior e inferior para $\mathbb{E}(X^2)$ obtenemos la desigualdad. □

Iskander Aliev [1] ha demostrado que

$$a_k > \sqrt{\frac{3}{2\pi k}} 2^k (1 + o(1)).$$

4.3. Sucesiones $B_h[g]$

Un simple conteo permite obtener una cota superior trivial para el mayor tamaño de un conjunto $B_h[g]$ en $[1, n]$. Si A es tal conjunto entonces

$$|A|^h = \sum_{n \leq hn} r_h(n) \leq h \cdot h! g n$$

de donde $|A| \leq (h \cdot h! g n)^{1/h}$.

Un argumento bastante similar al de la sección anterior permite mejorar esta cota superior (ver [14]).

Teorema 4.3.1. *Sea $A \subset [1, n]$ un conjunto $B_h[g]$. Entonces*

$$|A| \leq (\sqrt{3h} h! g)^{1/h}.$$

Demostración. Sea Y la variable aleatoria definida por

$$Y = X_1 + \cdots + X_h,$$

donde las X_j son variables aleatorias independientes distribuidas uniformemente en A. Podemos obtener una cota superior de la varianza de una manera sencilla haciendo uso del hecho de que $\mathbb{E}((X - \mu)^2)$ es mínima cuando $\mu = \mathbb{E}(X)$:

$$\begin{aligned} \mathbb{E}\left((Y - \bar{Y})^2\right) &= h\mathbb{E}\left((X - \bar{X})^2\right) \\ &\leq h\ E\left((X - (N+1)/2)^2\right) \\ &\leq h\frac{(N-1)^2}{4}. \end{aligned}$$

Para obtener una cota inferior de la varianza $E\left((Y - \bar{Y})^2\right)$ consideramos el multiconjunto $hA = \{a_1 + \cdots + a_h; a_i \in A\} = \{s_i : \quad i = 1, \ldots, k\}$, donde $k = |A|^h$.

$$|A|^h E\left((Y-\bar{Y})^2\right) = \sum_{s_i \in hA} (s_i - \bar{Y})^2.$$

El valor mínimo de la varianza ocurre cuando los elementos está tan cercanos entre sí como sea posible. Observemos que los s_i's toman valores enteros que aparecen, a lo más, $gh!$ veces (porque A es un conjunto $B_h[g]$). Entonces, la varianza no es menor que la varianza del multiconjunto

$$L = \{1, \dots 1, 2, \dots, 2, \dots, l, \dots, l\},$$

donde $l = [k/gh!]$ y cada elemento aparece exactamente $gh!$ veces en L. Así que,

$$\begin{aligned}
|A|^h \mathbb{E}\left((Y-\bar{Y})^2\right) &\geq \sum_{x\in L}(x-\bar{x})^2 = \sum_{x\in L} x^2 - |L|\bar{x}^2 \\
&= gh! \sum_{k=1}^{l} k^2 - gh! l \left(\frac{l+1}{2}\right)^2 \\
&= gh! \frac{l(l+1)(2l+1)}{6} - gh! \frac{l(l+1)^2}{4} \\
&= gh! \frac{l(l+1)(l+2)}{12} \geq \frac{k^3}{12(gh!)^2} - \frac{k}{12} \\
&\geq |A|^h \left(\frac{|A|^{2h}}{12(gh!)^2} - \frac{1}{12}\right).
\end{aligned}$$

Finalmente hemos probado que

$$\frac{1}{12}\left(\frac{|A|^{2h}}{(gh!)^2} - 1\right) \leq h\frac{(N-1)^2}{4},$$

que implica

$$|A| \leq \left((gh!)^2(3h(N-1)^2+1)\right)^{1/2h} \leq (\sqrt{3h}h!gN)^{1/h}.$$

□

4.4. El espacio probabilístico de las sucesiones infinitas

Erdős y Renyi consideraron el espacio probabilístico de todas las sucesiones A de enteros positivos donde todos los sucesos $n \in A$ son independientes entre sí y con probabilidades

$$P(n \in A) = f(n). \tag{4.4}$$

Típicamente la función $f(x)$ tiene a 0, es monótona decreciente y se elige de acuerdo con el problema a tratar. Es también la responsable del crecimiento de las sucesiones en ese espacio (de casi todas ellas para ser más preciso).

Ejercicio 4.4.1. *Demostrar que si* $f(x) = x^{-\alpha}(\log x)^{\beta}$ *con* $0 < \alpha < 1$ *entonces*

$$\sum_{2 \le i \le n} f(i) \sim \frac{1}{1-\alpha} n^{1-\alpha} (\log n)^{\beta}.$$

Proposición 4.4.1. *Sea* $f(x) = \min(cx^{-\alpha}(\log x)^{\beta}, 1)$, *con* $0 < \alpha < 1$, $c > 0$. *Con probabilidad* 1 *una sucesión aleatoria* A *en el espacio probabilístico definido en* (4.4) *satisface*

$$A(n) \sim c \frac{n^{1-\alpha}}{1-\alpha} (\log n)^{\beta}.$$

Demostración. Para cada n consideramos la variable aleatoria

$$A(n) = \sum_{i \le n} \mathbf{1}(n \in A),$$

donde $\mathbf{1}(n \in A)$ es la función indicatriz de dicho evento. El cálculo de la esperanza de $A(n)$ es un sencillo ejercicio(ver Ejercicio 4.4.1).

$$\mathbb{E}(A(n)) = c \sum_{2 \le i \le n} i^{-\alpha} (\log i)^{\beta} + O(1) \sim c \frac{n^{1-\alpha}}{1-\alpha} (\log n)^{\beta}.$$

Es claro que que $A(n)$ satisface las condiciones del Corolario 4.1.1. Por lo tanto,

$$\mathbb{P}\big(|A(n) - \mathbb{E}(A(n))| > \epsilon \mathbb{E}(A(n))\big) < e^{-\epsilon^2 \mathbb{E}(A(n))/4}$$

Tomando $\epsilon = 3\left(\frac{\log n}{\mathbb{E}(A(n))}\right)^{1/2}$ tenemos que

$$\mathbb{P}\left(|A(n) - \mathbb{E}(A(n))| > 3\sqrt{(\log n)\mathbb{E}(A(n))}\right) \quad < \quad e^{-(9/4)\log n} < n^{-2}.$$

Como la serie $\sum_n n^{-2}$ es finita se tiene que, con probabilidad 1, la sucesión aleatoria A satisface

$$|A(n) - \mathbb{E}(A(n))| < 3\sqrt{\log n \mathbb{E}(A(n))}$$

para todo n excepto quizás para un número finito de casos. Es decir, con probabilidad 1 se tiene que

$$\begin{aligned} A(n) &= \mathbb{E}(A(n)) + O\left(\sqrt{\log n \mathbb{E}(A(n))}\right) \\ &= c\frac{n^{1-\alpha}}{1-\alpha}(\log n)^{\beta}\left(1 + o(1)\right). \end{aligned}$$

□

4.4.1. Teorema de Erdős-Renyi

Una de los primeros éxitos del método probabilístico fue el siguiente teorema de Erdős y Renyi [28], donde demostraron que para todo $\epsilon > 0$ existe un $g = g(\epsilon)$ y una sucesión $B_2[g]$ tal que $A(x) \gg x^{1/2-\epsilon}$. Más concretamente,

Teorema 4.4.1. *Para todo g y para todo $\beta < \frac{1}{2} - \frac{1}{2(g+1)}$ existe una sucesión $B_2[g]$ con función contadora $A(x) \gg x^{\beta}$.*

Demostración. Consideremos la función $f(x) = x^{-\alpha}$ para un α que determinaremos más adelante. Cosideremmos también el espacio probabilístico asociado a la función $f(x)$ y sea $R_{n,g+1}$ el suceso:

El entero n tiene al menos $g+1$ representaciones de la forma

$$n = k_1 + (n - k_1) = \cdots = k_{g+1} + (n - k_{g+1})$$

con $k_1 < \cdots < k_{g+1} \leq n/2,\ k_i,\ n - k_i \in A$.

Más formalmente, podemos expresar este suceso como unión de intersecciones de sucesos de la forma siguiente,

$$R_{n,g+1} = \bigvee_{1\le k_1<\cdots<k_{g+1}\le n/2} \bigwedge_{i=1}^{g+1} (k_i, n-k_i \in A).$$

Es claro que todos los sucesos $k_i \in A, n-k_i \in A,\ i=1,\dots,g+1$ son independientes entre sí excepto los dos sucesos $k_{g+1} \in A$ y $n-k_{g+1} \in A$ cuando $k_{g+1} = n/2$ porque en ese caso los dos sucesos son el mismo. Así que distinguiremos ese caso duranto el cálculo siguiente:

$$\begin{aligned}
\mathbb{P}(R_{n,g+1}) &\le \sum_{1\le k_1<\cdots<k_{g+1}\le n/2} \mathbb{P}\big(k_1, n-k_1, \dots, k_{g+1}, n-k_{g+1} \in A\big) \\
&= \sum_{1\le k_1<\cdots<k_{g+1}<n/2} k_1^{-\alpha}(n-k_1)^{-\alpha}\cdots k_{g+1}^{-\alpha}(n-k_{g+1})^{-\alpha} \\
&+ \sum_{1\le k_1<\cdots<k_g<n/2} k_1^{-\alpha}(n-k_1)^{-\alpha}\cdots k_g^{-\alpha}(n-k_g)^{-\alpha}(n/2)^{-\alpha} \\
&= \sum_1 + \sum_2
\end{aligned}$$

Para la primera suma observemos que $(k_i-n)^{-\alpha} < (n/2)^{-\alpha}$. Por lo tanto

$$\begin{aligned}
\sum_1 &\le (n/2)^{-\alpha(g+1)} \sum_{1\le k_1<\cdots<k_{g+1}<n/2} k_1^{-\alpha}\cdots k_{g+1}^{-\alpha} \\
&\le (n/2)^{-\alpha(g+1)} \left(\sum_{1\le k<n/2} k^{-\alpha}\right)^{g+1} \\
&\ll n^{-\alpha(g+1)} n^{(1-\alpha)(g+1)} \\
&\ll n^{(g+1)(1-2\alpha)}.
\end{aligned}$$

Para la segunda procediendo de manera similar obtenemos

$$\begin{aligned}\sum_2 &\leq (n/2)^{-\alpha(g+1)}\left(\sum_{1\leq k<n/2} k^{-\alpha}\right)^g\\ &\ll n^{-\alpha(g+1)}n^{(1-\alpha)g}\\ &\ll n^{(g+1)(1-2\alpha)-(1-\alpha)}.\end{aligned}$$

Así que,

$$\mathbb{P}\big(R_{n,g+1}\big)\big) \ll n^{(g+1)(1-2\alpha)}.$$

Tomando $\alpha = \frac{1}{2} + \frac{1}{2(g+1)} + \epsilon$ tenemos que

$$\mathbb{P}\big(R_{n,g+1}\big) \ll n^{-1-2\epsilon(g+1)}.$$

Por lo tanto la suma $\sum_n \mathbb{P}(R_{n,g+1})$ es finita y podemos aplicar el teorema de Borel-Cantelli para deducir que con probabilidad 1, a lo más un número de sucesos $R_{n,g+1}$ ocurren.

Tomemos cualquiera de estas sucesiones A y sea n_0 el mayor n tal que $R_{n,g+1}$ ocurre. Eliminemos de A todos los elementos hasta n_0. La sucesión resultante es entonces una sucesión $B_2[g]$ y por la Proposición 4.4.1, su función contadora satisface

$$A(x) \sim cx^{\frac{1}{2}-\frac{1}{2(g+1)}-\epsilon}$$

para cierta constante c. □

4.4.2. Bases con pocas representaciones

Teorema 4.4.2. *Existe una sucesión A con*

$$r_A(n) \asymp \log n.$$

Demostración. Sea $f(x) = \min(10\sqrt{\log x/x}, 1)$ y consideremos el espacio probabilístico de todas las sucesiones donde todos los sucesos $x \in A$ son independientes y $P(x \in A) = f(x)$. Nuestro objetivo será demostrar que con probabilidad 1 tenemos que $r_A(n) \asymp \log n$.

El número de representaciones de n como suma de dos elementos de A es la variable aleatoria definida

$$r_A(n) = \sum_{\substack{x \le y \\ x+y=n}} I_A(x,y),$$

donde $I_A(x_1,\dots,x_k) = 1$ si todos los $x_i \in A$ y vale 0 en otro caso. La primera observación es que todos los sucesos $(x, y \in A)$ con $x + y = n$ son independientes.

El valor esperado de esta variable aleatoria puede ser calculado fácilmente:

$$\begin{aligned} \mathbb{E}(r_A(n)) &= \sum_{\substack{x \le y \\ x+y=n}} \mathbb{E}(I_A(x,y)) \\ &= \sum_{x<n/2} f(x)f(n-x) + f(n/2), \end{aligned}$$

donde $f(n/2)$ es simplemente 0 si n es impar.

Se deja como ejercicio justificar los detalles de los siguientes pasos:

$$\begin{aligned} \mu_n = \mathbb{E}(r_A(n)) &\sim \int_1^{n/2} f(t)f(n-t)dt \qquad (4.5) \\ &\sim n\int_{1/n}^{1/2} f(sn)f(n(1-s))ds \\ &\sim 100\int_{1/n}^{1/2} \frac{\sqrt{\log sn \log(n(1-s))}}{\sqrt{s(1-s)}}ds \\ &\sim 100\pi \log n. \end{aligned}$$

Estamos en condiciones de aplicar el Corolario 4.1.1 con $\epsilon = 1/2$.

$$\begin{aligned} P\left(\frac{1}{2}\mu_n < r_A(n) < \frac{3}{2}\mu_n\right) &< 2e^{-\frac{\mu_n}{16}} \\ &< 2n^{-100\pi/16(1+o(1))} \\ &\ll \frac{1}{n^2}. \end{aligned}$$

Como la serie $\sum_n n^{-2}$ es convergente podemos aplicar el Teorema de Borel-Cantelli para concluir que con probabilidad 1 se tiene que

$$\frac{1}{2}\mu_n < r_A(n) \frac{3}{2}\mu_n$$

para todo n excepto para un finito número de enetros n. La demostración finaliza observando que $\mu_n \sim 100\pi \log n$. □

Ejercicio 4.4.2. *Demostrar que para todo $\epsilon > 0$ existe una constante C y una sucesión de enteros positiva A tal que*

$$C \log n \leq r_A(n) \leq C(1+\epsilon) \log n.$$

Capítulo 5

Aplicaciones a problemas aritméticos y combinatorios

En este capítulo se verán aplicaciones de los conjuntos de Sidon a problemas aritméticos y combinatorios en cuerpos finitos. Muchos de ellos se puden describir utilizando conjuntos de Sidon en grupos finitos. Algunos de ejemplos que veremos en este capítulo son los siguientes:

- Último Teorema de Fermat en $\mathbb{F}_q$: ¿Tiene la congruencia

$$x^n + y^n \equiv z^n \pmod{p}$$

  soluciones no triviales?

- Estimaciones suma producto en $\mathbb{F}_p$: ¿Existe algún conjunto $A \subset \mathbb{F}_p$ con tamaños de los conjuntos $A + A$ y AA simultaneamente pequeños?

- Ecuaciones en $\mathbb{F}_q$: ¿Cuántas soluciones tiene la ecuación

$$x_1 x_2 = x_3 + x_4$$

  en $\mathbb{F}_q$ con $x_i \in A_i$?

Las respuestas clásicas a estos problemas se han servido de la maquinaria de las sumas de caracteres, pero utilizandoconjuntos de Sidon es

posible dar deostraciones de naturaleza eleental. Los resultados que sirven de caja negra para estos y otros problemas se explican en la siguiente sección.

5.1. Equidistribución de conjuntos de Sidon densos en conjuntos suma

Teorema 5.1.1. *Sea A un conjunto de Sidon en un grupo conmutativo finito G con $|A| = \sqrt{|G|} - \delta$. Entonces, para todo par $B, B' \subset G$ tenemos que*

$$|\{(b,b') \in B \times B',\ b+b' \in A\}| = \frac{|A|}{|G|}|B||B'| + \theta(|B||B'|)^{1/2}|G|^{1/4},$$

con $|\theta| < 1 + \frac{|B|}{|G|}\,\text{máx}(0,\delta)$.

Demostración. Como A es un conjunto de Sidon,

$$\begin{aligned}\sum_{x\in G} r_{B-B}(x)r_{A-A}(x) &= |A||B| + \sum_{x\neq 0} r_{B-B}(x)r_{A-A}(x)\\ &\leq |A||B| + \sum_{x\neq 0} r_{B-B}(x) = |A||B| + |B|^2 - |B|.\end{aligned}$$

Usando esta desigualdad y las identidades (1.4) y (5.5) tenemos

$$\begin{aligned}\sum_{x\in G}\left(r_{A-B}(x) - \frac{|A||B|}{|G|}\right)^2 &= \sum_{x\in G} r_{B-B}(x)r_{A-A}(x) - \frac{|A|^2|B|^2}{|G|} \qquad (5.1)\\ &\leq |B|(|A|-1) + |B|^2\frac{|G|-|A|^2}{|G|}.\end{aligned}$$

Observemos que

$$|\{(b,b') \in B\times B',\ b+b' \in A\}| - \frac{|B||B'||A|}{|G|} = \sum_{b'\in B'}\left(r_{A-B}(b') - \frac{|A||B|}{|G|}\right).$$

Aplicando la desigualdad de Cauchy-Schwarz y tomando en cuenta (5.1) y $|A| = |G|^{1/2} - \delta$, se tiene

$$\begin{aligned}\left|\sum_{b' \in B'} \left(r_{A-B}(b') - \frac{|A||B|}{|G|}\right)\right|^2 &\leq |B'| \left(|B|(|A|-1) + |B|^2 \frac{|G| - |A|^2}{|G|}\right) \\ &= |B'||B| \left(|G|^{1/2} - \delta - 1 + |B| \frac{\delta(2|G|^{1/2} - \delta)}{|G|}\right) \\ &< |B||B'||G|^{1/2} \left(1 + 2\,\text{máx}(0,\delta) \frac{|B|}{|G|}\right).\end{aligned}$$

□

Los conjuntos que consideraremos en las aplicaciones satisfacen $\delta \leq 1$ y $|B| = o(|G|)$. En estos casos tendremos $|\theta| \leq 1 + o(1)$.

Cuando $B = B'$ es un subgrupo de G obtenemos un sencillo corolario

Corolario 5.1.1. *Sea A un conjunto de Sidon en un grupo conmutativo finito G con $|A| = \sqrt{|G|} - \delta$ y sea B un subgrupo de G. Entonces*

$$|B \cap A| = \frac{|B||A|}{|G|} + \theta |G|^{1/4}$$

con $|\theta| < 1 + \frac{|B|}{|G|}\,\text{máx}(0, \delta)$.

Demostración. Cada elemento $z \in B$ tiene $|B|$ representaciones de la forma $z = b + b',\ b, b \in B$. Por lo tanto

$$|B \cap A| = \frac{|\{(b, b') \in B \times B,\ b + b' \in A\}|}{|B|}.$$

El corolario sigue del Teorema 5.1.1. □

El siguiente corolario también será de utilidad en las estiaciones suma-producto.

Corolario 5.1.2. *Sea A un conjunto de Sidon en G con $|A| = |G|^{1/2} - \delta$. Para todo par de conjuntos $B, B' \subset G$ tenemos*

$$|A \cap B| \leq \frac{|B + B'||A|}{|G|} + \theta \left(\frac{|B + B'|}{|B'|}\right)^{1/2} |G|^{1/4},$$

para algún θ *con* $|\theta| \le 1 + \max(0,\delta)\frac{|B'|}{|G|}$.

Demostración. Por el Teorema 5.1.1 tenemos

$$\begin{aligned}|B'||A\cap B| &= |\{(-b', b+b') :\ b\in B,\quad b'\in B',\ -b'+(b+b')\in A\}|\\ &\le |\{(b', b'') :\ b'\in (-B')\times (B+B'),\ b'+b''\in A\}|\\ &\le \frac{|A||B'||B+B'|}{|G|} + \theta\sqrt{|B'||B+B'|}|G|^{1/4}\end{aligned}$$

para algún θ con $|\theta| \le 1 + \max(0,\delta)\frac{|B'|}{|G|}$ y se sigue el Lema. □

5.2. El último Teorema de Fermat en $\mathbb{F}_p$

El Último Teorema de Fermat afirma que para cualquier entero $n \ge 3$, la ecuación

$$x^n + y^n = z^n \tag{5.2}$$

no tiene soluciones enteras x, y, z con $xyz \neq 0$. Descubierto en el margen de un libro de Fermat no se convirtió en un auténtico teorema hata que Andrew Willes lo demostró completamente en 1998.

Si en lugar de considerar la ecuación (5.2) en los enteros, la consideramos en $\mathbb{F}_p$, el problema es bien distinto. De hecho sí que va a tener soluciones no triviales, al menos si p es suficientemente grande. Las demostraciones clásicas del Teorema 5.2.1 utilizan análisis de Fourier en grupos finitos. La deostración que ofrecemos aquí es de naturaleza elemental y es una consecuencia directa del Corolario 5.1.1.

Teorema 5.2.1. *Para todo* $n \ge 1$ *y para todo primo* $p \gg n^4$*, la congruencia*

$$x^n + y^n \equiv z^n \pmod p \tag{5.3}$$

tiene soluciones $x, y, z,\ xyz \neq 0$.

Dividiendo la ecuación (5.3) entre z^n, el problema es equivalente a estudiar la ecuación $x + y \equiv 1 \pmod p$ cuando x, y pertenecen al grupo multiplicactivo generado por las potencias de exponente n.

Teorema 5.2.2. *Sea Q un subgrupo multiplicativo de $\mathbb{F}_p$ y sea $S(Q)$ el número de soluciones de*

$$x + y \equiv 1 \pmod{p}, \quad x, y \in Q. \tag{5.4}$$

Entonces

$$S(Q) = \frac{|Q|^2}{p} + O(\sqrt{q}).$$

Demostración. Sea g un generador de $\mathbb{F}_p^*$. Si $|Q| = m$ entonces m es un divisor de $p-1$ y el grupo multiplicativo Q será de la forma

$$Q = \{g^{nx} : \ 0 \leq x \leq m-1\}$$

donde $n = \frac{p-1}{m}$. Consideremos el subgrupo

$$B = \{(nu, nv) : \ 0 \leq u, v \leq m-1\}$$

y el conjunto de Sidon

$$A = \{(x, y) : \ g^x + g^y = 1\} \subset G = \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}.$$

Cada solución $(x, y) = (g^{nu}, g^{nv})$ de (5.4) la podemos identificar con un elemento $(nu, nv) \in B \cap A$. Aplicando el Corolario 5.1.1 tenemos que

$$S(Q) = |B \cap A| = \frac{|Q|^2}{p} + O(\sqrt{p}).$$

□

5.3. Sumas contra productos

Es bien conocido que el tamaño de $A + A = \{a + a', \ a, a' \in A\}$ se minimiza cuando A es es una progresión aritmética y que el tamaño de $AA = \{aa', \ a, a' \in A\}$ lo hace cuando A es una progresión geométrica. Ya que parece difícil que un conjunto A se parezca simultaneamente a una progresión aritmética y a una progresión geométrica, tiene sentido conjeturar que o bien $A + A$ o bien AA son grandes.

Conjetura 5.3.1 (Erdős-Szemeredi)**.** $|A + A| + |AA| \gg |A|^{2-\epsilon}$

Resultados del tipo $|A+A|+|AA| \gg |A|^{1+\delta}$ se han ido consiguiendo en los últimos tiempos. La última mejora,

$$|A+A|+|AA| \gg \frac{|A|^{4/3}}{(\log|A|)^{1/3}},$$

ha sido obtenida por J. Solymosi [61] y es consecuencia inmediata del siguiente teorema:

Teorema 5.3.1 (Solymosi)**.** *Para todo conjunto A de números reales,*

$$|AA||A+A|^2 \geq \frac{|A|^4}{4\log_2|A|}$$

Demostración. La energía multiplicativa de A se define como

$$E(A) = \sum_\lambda |\{(a,a');\ aa' = \lambda\}|^2 = \sum_\lambda |\{(a,a');\ a/a' = \lambda\}|^2$$

La igualdad se debe que $E(A)$ cuenta el número de cuadruplas (a_1,a_2,a_3,a_4) tales que $a_1a_2 = a_3a_4$, que es igual al número de cuadruplas tales que $a_1/a_3 = a_4/a_2$. Mediante la desigualdad de Cauchy-Schwarz,

$$|A|^2 = \sum_{\lambda\in AA} |\{(a,a');\ aa' = \lambda\}| \leq |AA|^{1/2}E(A)^{1/2},$$

obtenemos que

$$E(A) \geq \frac{|A|^4}{|AA|}. \tag{5.5}$$

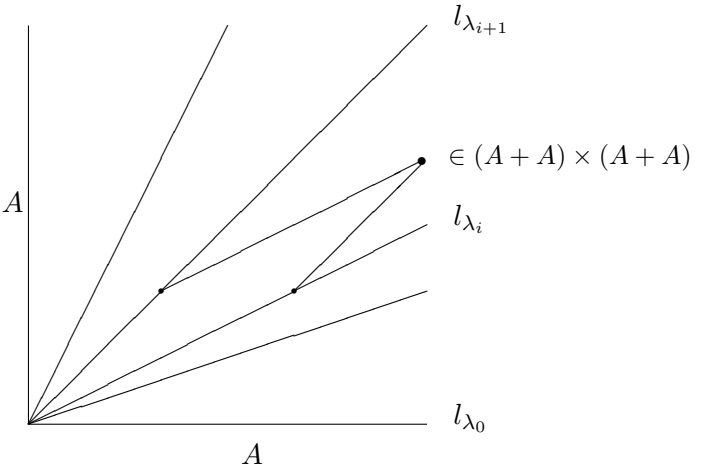
Si definimos las rectas $l_\lambda :\ y = \lambda x$ podemos escribir

$$\begin{aligned} E(A) &= \sum_\lambda |l_\lambda \cap (A\times A)|^2 \\ &\leq \sum_{0\leq j\leq \log_2|A|} 2^{2j}\#\{l_\lambda :\ 2^{j-1} < |l_\lambda\cap(A\times A)| \leq 2^j\} \end{aligned}$$

Existe entonces un j y un m tales que

$$m = \#\{l_\lambda :\ 2^{j-1} < |l_\lambda\cap(A\times A)| \leq 2^j\} \tag{5.6}$$

$$\geq 2^{-2j}\frac{E(A)}{\log_2|A|}. \tag{5.7}$$



Sean $0 = \lambda_0 < \lambda_1 < \cdots < \lambda_m$ las pendientes de las rectas correspondientes, donde hemos añadido la recta $y = 0$. La observación clave es que para cada dos rectas consecutivas $l_{\lambda_i}, l_{\lambda_{i+1}}$, todas las sumas $(x,y)+(x',y')$, $(x,y) \in l_{\lambda_i}$, $(x',y') \in l_{\lambda_{i+1}}$ son distintas (ver dibujo) y además todas ellas son distintas de las que se obtienen con otras dos rectas consecutivas. Además todas las sumas están en $(A+A)\times(A+A)$

Entonces

$$|A+A|^2 \geq \left| \bigcup_{i=0}^{m-1} (l_{\lambda_i} \cap (A\times A)) + \big(l_{\lambda_{i+1}} \cap (A\times A)\big) \right| \tag{5.8}$$

$$= \sum_{i=0}^{m-1} |l_{\lambda_i} \cap (A\times A)||l_{\lambda_{i+1}} \cap (A\times A)| \geq m2^{2j-2}. \tag{5.9}$$

De (5.6) y (5.8) obtenemos

$$E(A) \leq 4|A+A|^2 \log_2 |A|$$

que junto con (5.5) nos da el teorema. □

Si en lugar de considerar el problema suma-producto en los enteros o en los reales lo consideramos en $\mathbb{F}_p$ el problema es bien distinto. Si

$A \subset \mathbb{F}_p$ y $|A| < p^{1/2}$ se sabe que

$$|A+A| + |AA| \gg |A|^{13/12}.$$

la demostración de este estimación supera los objetivos de este curso. Cuando $|A| \geq p^{1/2}$ Garaev [30] demostró la siguiente desigualdad que es óptima en el rango $|A| \geq p^{2/3}$.

Teorema 5.3.2. *Si $A \subset \mathbb{F}_p$ entonces*

$$\max(|A+A|, |AA|) \gg \min(\sqrt{|A|p}, |A|^2/\sqrt{p}).$$

La demostración original de Garaev utiliza sumas trigonométricas y existe otra demostración de Solymosi utilizando teoría espectral de grafos. La demostración que ofrecemos aquí será consecuencia del Corolario 5.1.2.

Demostración del Teorema 5.3.2. Consideramos el conjunto de Sidon

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

y observemos que $\delta = \sqrt{|G|} - |A| = \sqrt{p(p-1)} - (p-1) \ll 1$. Consideremos también los conjuntos

$$B = B' = (\log A) \times A.$$

Como todos los elementos de la forma $(\log a, a)$, $a \in A$ están en S tenemos que $|S \cap B| = |A|$. Por otra parte observemos que $|B+B| = |AA||A+A|$. El Corolario 5.1.2 implica la desigualdad

$$|A| \leq \frac{|AA||A+A|}{p} + \theta\sqrt{p\frac{|AA||A+A|}{|A||A|}},$$

para algún θ con $|\theta| \ll 1$.

Si $\frac{|AA||A+A|}{p} > |A|/2$ entonces $\max(|AA|, |A+A|) \gg \sqrt{|A|p}$.

Si $\frac{|AA||A+A|}{p} \leq |A|/2$ entonces $|AA||A+A| \gg |A|^4/p$ y por tanto $\max(|AA|, |A+A|) \gg |A|^2/\sqrt{p}$. □

Ejercicio 5.3.1. *Demostrar que para todo $A_1, A_2, A_3 \subset \mathbb{F}_p$ se tiene que*

$$\max(|A_1 + A_2|, |A_1 A_3|) \gg \min\left(\sqrt{|A_1|q}, \sqrt{|A_1|^2|A_2||A_3|/q}\right).$$

Se puede imitar las demostración anterior para conseguir las siguiente estimación suma-producto.

Teorema 5.3.3 (Garaev-Shen [31])**.** *Sean $A_1, A_2, A_3 \subset \mathbb{F}_q^*$. Se tiene que*

$$\max(|(A_1 + 1)A_2|, |A_1 A_3|) \gg \min\left(\sqrt{|A_1|q}, \sqrt{|A_1|^2|A_2||A_3|/q}\right).$$

Demostración. Se considera ahora el conjunto de Sidon $S = \{(x, y) : g^x - g^y = 1\}$, los conjuntos $B = \log(A_1+1) \times \log A_1$ y $B' = \log A_2 \times \log A_3$ y se procede como en la deostración del Teorema 5.3.2. □

Ejercicio 5.3.2 (Solymosi [61], Hart-Li-Shen [37])**.** *Sean $p(x), q(x) \in \mathbb{F}_q[X]$ polinomios independientes de grado a lo más 2. Demostrar que para todo $A_1, A_2, A_3 \subset \mathbb{F}_q$ se tiene que*

$$\max(|p(A_1) + A_2|, |q(A_1) + A_3|) \gg \min\left(\sqrt{|A_1|q}, \sqrt{|A_1|^2|A_2||A_3|/q}\right).$$

Ejercicio 5.3.3. *Completar los detalles de la demostración del Teorema 5.3.3.*

5.4. Incidencias de rectas y puntos en $\mathbb{F}_q$

Sea $I(P, L)$ el número de incidencias entre un conjunto P de puntos y un conjunto L de rectas en $\mathbb{F}_q \times \mathbb{F}_q$; es decir,

$$I(P, L) = |\{(p, l) \in P \times L : \ p \in l\}|.$$

Utilizando sumas de caracteres Vinh [64] demostró $I(P, L) \leq \frac{|P||L|}{q} + q^{1/2}\sqrt{|P||L|}$. Daremos una estimación asintótica para $I(P, L)$ como una consecuencia del Teorema 5.1.1.

Teorema 5.4.1. *Sea L un conjunto de lineas y sea P un conjunto de putos en $\mathbb{F}_q \times \mathbb{F}_q$. En ese caso tenemos*

$$I(P, L) = \frac{|P||L|}{q} + O(q^{1/2}\sqrt{|P||L|}). \tag{5.10}$$

Demostración. Sean los conjuntos

$$\begin{aligned} L &= \{y = \lambda_i x + \mu_i : \ 1 \le i \le |L|\} \\ P &= \{(p_j, q_j) : \ 1 \le j \le |P|\}. \end{aligned}$$

Consideremos el conjunto de Sidon

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

descrito en el ejemplo (2) y los conjuntos

$$\begin{aligned} B &= \{(\log \lambda_i, -\mu_i) : \ 1 \le i \le |L|\} \\ B' &= \{(\log p_j, q_j) : \ 1 \le j \le |P|\}. \end{aligned}$$

Observemos que cada incidencia corresponde a una solución de

$$\lambda_i p_j = q_j - \mu_i$$

y el número de soluciones de esta ecuación es

$$|\{(b, b') \in B \times B' : \ b + b' \in S\}|.$$

El resultado sigue del Teorema 5.1.1. □

Capítulo 6

Conjuntos de Sidon en otros escenarios

Aunque los conjuntos de Sidon más estudiados son los conjuntos de Sidon en los enteros, aparecen problemas muy interesantes cuando nos preguntamos por conjuntos de Sidon en otros escenarios. ¿Es la sucesión $A = \{n^5 : \ n \geq 1\}$ un conjunto de Sidon? ¿Es cierto que todo conjunto de n enteros contiene un subconjunto de Sidon A de tamaño $|A| \sim \sqrt{n}$? ¿Cuántos elementos tiene el conjunto de Sidon de mayor cardinal en el conjunto de los n primeros cuadrados? Estos problemas, interesantes todos ellos, todavía buscan respuesta.

6.1. Conjuntos de Sidon en d dimensiones

Los conjuntos de Sidon de puntos de coordenadas enteras en el plano tienen una bonita interpretación geométrica. Se pueden visualizar como aquellos que tienen la propiedad de que no existe un paralelogramo con vértices en los elementos del conjunto. En el primer capítulo ya vimos conjuntos de Sidon en grupos finitos de estructura bidimensional $(\mathbb{Z}_p \times \mathbb{Z}_p, \ \mathbb{Z}_p \times \mathbb{Z}_{p-1}, \ \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1})$ y que en particular son conjuntos de Sidon de puntos de coordenadas enteras en los cuadrados o rectángulos correspondientes.

6.1.1. Conjuntos de Sidon finitos en d dimensiones. Cotas superiores

¿Cuál es el mayor número de puntos de coordenadas enteras que podemos dibujar en el cuadrado $[1,n]\times[1,n]$ de tal manera que nunca cuatro de ellos formen un paralelogramo?

Definamos en general,

$$F_{2,d}(n) = \max |A| : \ A \text{ es de Sidon en } [1,n]^d.$$

Lindström [45] obtuvo la siguiente cota superior para $F_{2,d}(n)$.

Teorema 6.1.1.

$$F_{2,d}(n) \le n^{d/2} + O\left(n^{\frac{d^2}{2d+2}}\right). \tag{6.1}$$

Demostración. La primera observación es que si $A \subset [1,n]^d$ es un conjunto de Sidon, todas las posibles diferencias $a-a'$, $a \neq a' \in A$ son distintas y están en $[-n+1, n-1]^d$, lo que implica que

$$\binom{|A|}{2} \le (2n-1)^d \implies |A| \ll n^{d/2}.$$

A continuación vamos a utilizar el Lemma 1.2.1 con $B=[1,s]^d$ para un s que elegiremos después. Es claro que $A+B \subset [1, n+s]^d$ y por lo tanto

$$|A+B| = (n+s)^d = n^d + O(n^{d-1}s).$$

El Lemma 1.2.1 implica que

$$|A|^2 \le |A+B|\left(1+\frac{|A|-1}{|B|}\right) = n^d\left(1+O(n^{-1}s)\right)\left(1+O(n^{d/2}s^{-d})\right).$$

Eligiendo $s = \left\lfloor n^{\frac{d+2}{2d+2}} \right\rfloor$ para minimizar el error obtenemos

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

Por lo tanto, $|A| \le n^{d/2}\left(1+O(n^{-\frac{d}{2d+2}})\right) \le n^{d/2} + O\left(n^{\frac{d^2}{2d+2}}\right)$. □

Erdős and Turan conjeturaron $F_{2,1}(n) < n^{1/2}+O(1)$, que corresponde a los conjuntos de Sidon en intervalos. Esta conjetura fue generalizada por Lindström [45] en 1969 para todo d:

$$F_{2,d}(n) < n^{d/2} + O(1). \tag{6.2}$$

Como ya comentamos en el primer capítulo se cree que la conjetura es falsa en el caso $d = 1$.

Mientras que todavía no se sabe cómo refutar la conjetura 6.2 para $d = 1$, Cilleruelo[9] y Ruzsa han demostrado, independientemente, que la conjetura no es cierta para $d = 2$.

Teorema 6.1.2. *Existe una constante $c > 0$ e infinitos enteros m tales que*

$$F_{2,2}(m) > m + c \log m \log\log\log m.$$

Demostración. Sea n_p el menor residuo no cuadrático (mód p), donde p es un primo impar. Se sabe [35] que existe una constante $c_0 > 0$ tal que la desigualdad $n_p > c_0 \log p \log\log\log p$ es cierta para infinitos primos p. Sea p cualquiera de estos primos y consideremos el conjunto

$$A_p = \{((n_p k^2)_p\ , (n_p(k+1)^2)_p),\ k = 1, \dots p\},$$

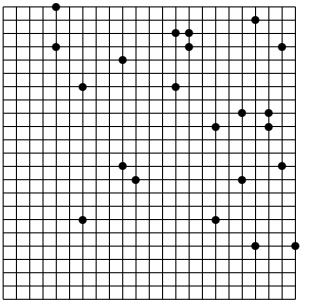
donde $(x)_p$ es el mínimo entero positivo congruente con x (mód p). En el Ejercico 1.3.3 se demuestra que este conjunto es de Sidon en $\mathbb{Z}_p \times \mathbb{Z}_p$ y en particular lo será en $[1, p] \times [1, p]$.

Como $n_p k^2$ y $n_p(k+1)^2$ son residuos no cuadráticos (mód p), tenemos que $A_p \subset [n_p, p]^2$. Entonces, el conjunto $A_p - (n_p - 1, n_p - 1)$ es un conjunto de Sidon con p elementos incluido en $[1, p - n_p + 1]^2$. Por lo tanto,

$$F_2(p - n_p + 1) \geq p = p - n_p + 1 + n_p - 1,$$

y el teorema se sigue tomando $m = p - n_p + 1$. □

La siguiente figura ilustra la construcción utilizada en el Teorema 6.1.2 para $p = 23$ con $n_p = 5$.



Se cree que la conjetura correcta es la siguiente.

Conjetura 6.1.1. *$F_2(n) < n + O(n^{\varepsilon})$ para todo $\varepsilon > 0$.*

Para poner en valor la dificultad de esta conjetura, al menos en el caso $d = 2$, vamos a ver cómo ésta implicaría la siguiente conjetura clásica de Vinogradov:

Conjetura 6.1.2 (Conjetura de Vinogradov)**.** *: El menor residuo no cuadrático* mód p *satisface $n_p = O(n^{\epsilon})$ para todo $\epsilon > 0$.*

Usando la misma construcción que en el teorema 6.1.2 y asumiendo (6.1.1) tenemos que

$$p \leq F_{2,2}(p - n_p) < p - n_p + O((p - n_p)^{\varepsilon}) \implies n_p < n^{\varepsilon}.$$

6.1.2. Construcciones de conjuntos de Sidon finitos en d dimensiones

Existe una manera natural de transformar conjuntos de Sidon en dimensión 1 a conjuntos de Sidon en dimensión d. Para ello utilizaremos el hecho de que dada una sucesión de enteros positivos $n_1, n_2, \ldots$, todo entero positivo a puede representarse de manera única de la forma

$$a = \delta_1 + \delta_2 n_1 + \delta_3 n_1 n_2 + \cdots + \delta_i n_1 \cdots n_{i-1} + \cdots \tag{6.3}$$

con $0 \leq \delta_i < n_i$. Los $n_i's$ son las bases y los $\delta_i's$ los dígitos. Por brevedad escribimos $N_1 = 1$ y $N_i = n_1 \cdots n_{i-1}$. Con esta notación,

$$a = \sum_{i \geq 0} \delta_i N_i \tag{6.4}$$

Teorema 6.1.3. *Sean $n_1, \dots, n_d$ enteros positivos. Si $F_2(n_1, \dots, n_d)$ Es el tamaño del conjunto de Sidon más grande contenido en $[1, n_1] \times \cdots \times [1, n_d]$, entonces*

$$F_2(n_1, \dots, n_d) \geq F_2(n_1 \cdots n_d).$$

En particular,

$$F_{2,d}(n) \geq F_{2,1}(n^d). \tag{6.5}$$

Demostración. Sea φ_d la función definida por $\varphi_d(a) = (\delta_1, \dots, \delta_d)$, donde $\delta_1, \dots, \delta_d$ son los dígitos de a en la base $n_1, \dots, n_d$. Vamos a ver que esta función transforma conjuntos de Sidon en $\mathbb{N}$ en conjuntos de Sidon en $\mathbb{N}^d$. Sea $\varphi_d(A) = \{\varphi_d(a) : \ a \in A\}$ la imagen de un conjunto de Sidon A en $\mathbb{N}$ y supongamos que para $a, a', a'', a''' \in A$ tenemos que

$$\varphi_d(a) + \varphi_d(a') = \varphi_d(a'') + \varphi_d(a''').$$

Entonces,

$$\delta_i + \delta_i' = \delta_i'' + \delta_i''', \qquad \text{for } i = 1, \dots, d.$$

Sumando en todos los i tenemos que

$$\sum_{i=1}^{d} \delta_i N_i + \sum_{i=1}^{d} \delta_i' N_i = \sum_{i=1}^{d} \delta_i'' N_i + \sum_{i=1}^{d} \delta_i''' N_i,$$

y por lo tanto, $a + a' = a'' + a'''$. Como A es un conjunto de Sidon, tenemos que $\{a, a'\} = \{a'', a'''\}$, y por lo tanto $\{\varphi_d(a), \varphi_d(a')\} = \{\varphi_d(a''), \varphi_d(a''')\}$. Así que hemos demostrado que el conjunto $\varphi_d(A)$ es un conjunto de Sidon en $\mathbb{N}^d$.

Sea $A \subset [1, n_1 \cdots n_d]$ be a un conjunto de Sidon. Entonces $A - 1$ es un conjunto de Sidon en $[0, n_1 \cdots n_d - 1]$ y $\varphi_d(A - 1)$ es un conjunto de Sidon en $[0, n_1 - 1] \times \cdots \times [0, n_d - 1]$.

Por lo tanto el conjunto $\varphi_d(A-1)+(1, \dots, 1)$ es un conjunto de Sidon en $[1, n_1] \times \cdots \times [1, n_d]$. □

Corolario 6.1.1. *Para todo d, tenemos que*

$$F_{2,d}(n) \sim n^{d/2} \quad as \quad n \to \infty$$

Demostración. Es consecuencia de (6.1) y (6.5). □

6.1.3. Conjuntos de Sidon infinitos en d dimensiones

Las sucesiones infinitas de Sidon son mucho más difíciles que las finitas. Ya lo vimos en dimesión 1 y sigue siendo cierto en dimensiones mayores.

Sea $A \subset \mathbb{N}^d$ un conjunto infinito de Sidon y sea

$$A(n) = \#\{a = (a_1, \dots, a_d) \in A,\ a_i \le n,\ \text{for all } i = 1, \dots, d\}$$

la función contadora de A cuando contamos por cuadrados. Pero engenral, dados números reales $t_1, \dots, t_d$, sean

$$A(n^{t_1}, \dots, n^{t_d}) = \#\{a = (a_1, \dots, a_d) \in A,\ a_i \le n^{t_i},\ \text{for all } i = 1, \dots, d\}.$$

Obviamente, para todo cnjunto A infinito en $\mathbb{N}^d$, tenemos que

$$A(n) \le F_{2,d}(n) \ll n^{d/2}. \tag{6.6}$$

Es natural preguntarse si existe una sucesión infinita de Sidon $A \subset \mathbb{N}^d$ tal que $A(n) \gg n^{d/2}$ para todo n. Ya vimos en el Teorema 2.1.1 que la respuesta es negativa para $d = 1$. Trujillo [63] estudió el caso $d = 2$ y dio una respuesta parcial a esta pregunta demostrando que

$$\lim_{N\to\infty} \inf_{n,m>N} \frac{A(n,m)}{\sqrt{nm/\log(nm)}} \ll 1,$$

Pero esto no es suficientemente para concluir que $\liminf_{n\to\infty} \frac{A(n)}{n} = 0$ para toda sucesión infinita Sidon $A \subset \mathbb{N}^2$. En [9] se da respuesta a este problema para todo $d \ge 1$.

Teorema 6.1.4. *Para todo $d \ge 1$ y para toda sucesión infinita de Sidon $A \subset \mathbb{N}^d$, se tiene que*

$$\liminf_{n\to\infty} \frac{A(n)}{\sqrt{n^d/\log n}} \ll 1.$$

Demostración. Sea

$$\tau(N) = \inf_{n>N} \frac{A(n)(\log n)^{1/2}}{n^{d/2}}$$

y consideremos el conjunto $(0, N^2]^d$. Para todo $\vec{\imath} = (i_1, \ldots, i_d)$, $0 \leq i_j < N$, escribimos $C_{\vec{\imath}}$ para designar el número de elementos de A en el hipercubo $N \cdot \vec{\imath} + (0, N]^d$. Para cada $l = 0, 1, \ldots$, sea $D_l = \sum_{|\vec{\imath}|=l} C_{\vec{\imath}}$, donde $|\vec{\imath}\,| = \max_{1 \leq j \leq d} i_j$. Entonces

$$D_l^2 \leq d(l+1)^{d-1} \sum_{|\vec{\imath}|=l} C_{\vec{\imath}}^2,$$

así que,

$$\frac{1}{d} \sum_{0 \leq l < N} \frac{D_l^2}{(l+1)^{d-1}} \leq \sum_{0 \leq |\vec{\imath}| < N} C_{\vec{\imath}} + \sum_{0 \leq |\vec{\imath}| < N} C_{\vec{\imath}}(C_{\vec{\imath}} - 1).$$

Por (6.6), tenemos que

$$\sum_{0 \leq |\vec{\imath}| < N} C_{\vec{\imath}} = A(N^2) \ll_d N^d.$$

Observemos que todas las diferencias $As - As'$ con $As \neq As'$, ambos en el mismo hipercubo, están en $(-N, N)^d$. Esto, junto con la propiedad de Sidon, implica que

$$\sum_{\vec{\imath}} C_{\vec{\imath}}(C_{\vec{\imath}} - 1) \leq (2N)^d.$$

Por lo tanto,

$$\sum_{0 \leq l < N} \frac{D_l^2}{(l+1)^{d-1}} \ll_d N^d.$$

Por otro lado podemos escribir

$$\left(\sum_{0 \leq l < N} \frac{D_l}{(l+1)^{d/2}} \right)^2 \leq \left(\sum_{0 \leq l < N} \frac{D_l^2}{(l+1)^{d-1}} \right) \left(\sum_{0 \leq l < N} \frac{1}{(l+1)} \right) \ll_d N^d \log N. \tag{6.7}$$

Ahora sumamos por partes para obtener

$$\begin{aligned} \sum_{0 \leq l < N} \frac{D_l}{(l+1)^{d/2}} &= \sum_{1 \leq l \leq N} \frac{D_{l-1}}{l^{d/2}} \gg_d \int_1^N \frac{\sum_{l \leq t} D_{l-1}}{t^{d/2+1}} dt \\ &\gg_d \int_1^N \frac{A(tN)}{t^{d/2+1}} dt \gg_d \int_1^N \frac{\tau(N)(tN)^{d/2}}{(\log(tN))^{1/2}} \frac{1}{t^{d/2+1}} dt \\ &\gg_d \tau(N) N^{d/2} (\log N)^{1/2}. \end{aligned} \tag{6.8}$$

De (6.7) y (6.8) obtenemos que $\lim_{N\to\infty} \tau(N) \ll_d 1$. □

Para medir la densidad de sucesiones infinitas de Sidon en $\mathbb{N}^d$, definimos, para cualesquiera $t_1, \dots, t_d$ reales positivos, la cantidad

$$\alpha(t_1, \dots, t_d) = \sup_{A \text{ Sidon set in } \mathbb{N}^d} \liminf_{n\to\infty} \frac{\log A(n^{t_1}, \dots, n^{t_d})}{\log n}.$$

Observar que $\alpha(1, \dots, 1) = \alpha_d$ y que es conocido que $\sigma_1 = \sqrt{2} - 1$. El siguiente resultado muestra que el problema de encontrar sucesiones de Sidon infinitas es equivalente en todas las dimensiones.

Teorema 6.1.5. *Para cualesquiera $t_1, \dots, t_d$, reales positivos se tiene que*

$$\alpha(t_1, \dots, t_d) = (t_1 + \cdots + t_d)\alpha_1. \tag{6.9}$$

In particular, $\alpha_d = d\alpha_1$.

Demostración. Para probar que $\alpha(t_1, \dots, t_d) \le (t_1 + \cdots + t_d)\alpha_1$ es suficiente con construir una función inyectiva ϕ de $\mathbb{N}^d$ en $\mathbb{N}$ con las siguientes propiedades:

i) φ transforma conjuntos de Sidon en $\mathbb{N}^d$ en conjuntos de Sidon en $\mathbb{N}$.

ii) $\varphi(([1, n^{t_1}] \times \cdots \times [1, n^{t_d}]) \cap \mathbb{N}^d) \subset [1, n^{t_1+\cdots+t_d+\epsilon(n)}]$, con $\epsilon(n) \to 0$ cuando $n \to \infty$.

Dadas d bases $n_{j1}, \dots, n_{ji}, \dots \quad j = 1, \dots, d$, definimos por $\delta_{ji}(a)$ el dígito de a que ocupa el lugar i en la base j,

$$a = \sum_i \delta_{ji}(a) N_{ji}$$

where $N_{j1} = 1$ and $N_{ji} = \prod_{s\le i-1} n_{js}$ for $i \ge 2$.

Ahora construimos una nueva base $m_1, m_2, \dots m_s$ definida por $m_s = 2n_{ji},\ s = j + (i-1)d,\ 1 \le j \le d$ y definimos la función

$$\varphi(a_1, \dots, a_d) = \sum_s \delta_s(a_1, \dots, a_d) M_s \tag{6.10}$$

donde

$$\delta_s(a_1,\dots,a_d)=\delta_{ji}(a_j),$$

para $s=j+(i-1)d,\ 1\le j\le d$, $M_1=1$ and $M_s=\prod_{l\le s-1}m_l$.

Observemos que si $s=j+(i-1)d$ entonces

$$0\le\delta_s(a_1,\dots,a_j)<n_{ji}=m_s/2. \tag{6.11}$$

Para probar i), demostraremos que si $A\in\mathbb{N}^d$ es un conjunto de Sidon, entonces $\phi(A)$ también lo es. Supongamos que

$$\varphi(a_1,\dots,a_d)+\varphi(a_1',\dots,a_d')=\varphi(a_1'',\dots,a_d'')+\varphi(a_1''',\dots,a_d'''),$$

donde $(a_1,\dots,a_d),(a_1',\dots,a_d'),(a_1'',\dots,a_d''),(a_1''',\dots,a_d''')\in A$. Thus,

$$\begin{aligned}&\sum_s\left(\delta_s(a_1,\dots,a_d)+\delta_s(a_1',\dots,a_d')\right)M_s\\ =&\sum_s\left(\delta_s(a_1'',\dots,a_d'')+\delta_s(a_1''',\dots,a_d''')\right)M_s.\end{aligned}$$

Usando (6.11) vemos que

$$0\le\delta_s(a_1,\dots a_d)+\delta_s(a_1',\dots,a_d'),\delta_s(a_1'',\dots,a_d'')+\delta_s(a_1''',\dots,a_d''')<m_s.$$

Pero entonces ambas sumas son dos representaciones del mismo número en una base y tenemos que

$$\delta_s(a_1,\dots,a_d)+\delta_s(a_1',\dots a_d')=\delta_s(a_1'',\dots,a_d'')+\delta_s(a_1''',\dots,a_d''')$$

para todo s. En particular, si$s=j+(i-1)d$ tenemos que

$$\delta_{ji}(a_j)+\delta_{ji}(a_j')=\delta_{ji}(a_j'')+\delta_{ji}(a_j''')$$

y

$$\begin{aligned}a_j+a_j'&=\sum_{i\ge1}\left(\delta_{ji}(a_j)+\delta_{ji}(a_j')\right)N_{ji}\\ &=\sum_{i\ge1}\left(\delta_{ji}(a_j'')+\delta_{ji}(a_j''')\right)N_{ji}=a_j''+a_j'''.\end{aligned}$$

Así que,

$$(a_1,\dots,a_d)+(a_1',\dots,a_d')=(a_1'',\dots,a_d'')+(a_1''',\dots,a_d''').$$

Como A es un conjunto de Sidon, tenemos que

$$\{(a_1,\dots,a_d),(a_1',\dots,a_d')\} = \{(a_1'',\dots,a_d''),(a_1''',\dots,a_d''')\},$$

así que

$$\{\phi(a_1,\dots,a_d),\phi(a_1',\dots,a_d')\} = \{\phi(a_1'',\dots,a_d''),\phi(a_1''',\dots,a_d''')\},$$

y por lo tanto $\phi(A)$ es un conjunto de Sidon.

Para probar ii), consideremos las bases anteriores con $n_{ji} = 2^{\lceil it_j\rceil}$. Sea i_0 el mayor entero i tal que $\delta_{ji}(a_j)\neq 0$ para algún j. Tenemos que

$$a_j = \sum_{l\le i_0}\delta_{jl}N_{jl} \ge N_{ji_0} \ge 2^{\lceil t_j\rceil+\cdots+\lceil(i_0-1)t_j\rceil} = 2^{i_0^2t_j/2+O(i_0)}.$$

Si $a_j \le n^{t_j}$ entonces $i_0 \le \sqrt{2\log_2 n}+O(1)$.

En el otro sentido, observemos que $\phi(a_1,\dots,a_d)\le M_{s+1}$ donde $s = i_0d$. Finalmente tenemos que

$$\begin{aligned} M_{s+1} = \prod_{l\le s-1} m_s = \prod_{l\le i_0-1}\prod_{j=1}^{d}(2n_{lj}) &\le \prod_{l\le i_0-1}\prod_{j=1}^{d}2^{lt_j+2} \\ &\le 2^{(t_1+\cdots+t_d)i_0(i_0-1)/2+2d(i_0-1)} \le n^{t_1+\cdots t_d+\epsilon(n)} \end{aligned}$$

donde $\epsilon(n) = O(1/\sqrt{\log n})$.

La desigualdad $\alpha(t_1,\dots,t_d)\ge(t_1+\cdots+t_d)\alpha_1$ se demuestra de forma parecida construyendo una función φ con las propiedades:

i) φ transforma conjuntos de Sidon en $\mathbb{N}$ a conjuntos de Sidon en $\mathbb{N}^d$.

ii) $\varphi([1,n^{t_1+\cdots+t_d}]\cap\mathbb{N}) \subset [1,n^{t_1+\epsilon_1(n)}]\times\cdots\times[1,n^{t_d+\epsilon_d(n)}]$, with $\epsilon_i(n)\to 0$ cuando $n\to\infty$ para $i=1,\dots,d$.

Sea la sucesión $n_1,\dots,n_i,\dots$ with $n_{j+id} = 2^{\lceil it_j\rceil}$ y, dado $a\in\mathbb{N}$, escribimos a en la base $N_1,\dots$:

$$a = \sum_i \delta_s N_s$$

donde $N_1 = 1$ and $N_s = \prod_{i \le s-1} n_i$ for $i \ge 2$. Definimos la función $\varphi(a) = (\varphi_1(a), \ldots, \varphi_d(a))$ by

$$\varphi_j(a) = \sum_i \delta_{j+id} M_{ji}$$

donde $M_{j0} = 1$ and $M_{ji} = \prod_{s \le i-1}(2n_{j+sd})$.

Comprobar que φ satisface las propiedades requeridas es un problema rutinario, similar al que se hizo anteriormente para demostrar la otra desigualdad. □

Ejercicio 6.1.1. *Demostrar que el conjunto* $A = \{(n, n^2) : \ n \in \mathbb{N}\}$ *es un conjunto de Sidon en* $\mathbb{N} \times \mathbb{N}$.

Este ejercicio demuestra que $\alpha(1,2) \ge 1$, y por el teorema anterior, que $\alpha_1 \ge 1/3$. Es cierto que podemos obtener esta cota interior con la sucesión generada por el algoritmo avaricioso, pero la construcción que nos da el teorema anterior es *explícita* (no necesitamos conocer los elementos anteriores para calcular a_n).

Ejercicio 6.1.2. *A partir del conjunto de Sidon* $\{(n, n^2) : \ n \in \mathbb{N}\}$ *construir la sucesión infinita de Sidon explícita generada por* (6.10).

En cualquier caso la sucesión infinita de Sidon que hemos construido en el capítulo 2 también es explícita y muestra que $\alpha_1 \ge \sqrt{2}-1$, una cota inferior mayor que $1/3$. La demostración consiste simplemente en hacer explícita la construcción del teorema anterior para este caso particular.

6.2. Conjuntos de Sidon en sucesiones polinómicas

La sucesión de los cuadrados no es una sucesión de Sidon, ni siquiera es una sucesión $B_2[g]$ para ningún g porque el número de representaciones de n como suma de dos cuadrados no está acotado uniformemente en n. Se conjetura que la sucesión $A = \{n^5 : \ n \ge 1\}$ es una sucesión de Sidon pero ni siquiera se sabe si existe un polinomio $P(x)$ tal que la sucesión $A = \{P(n) : \ n \ge 1\}$ sea de Sidon. Observar que se trata de encontrar un polinomio tal que la ecuación $P(x) + P(y) = P(z) + P(w)$

no tenga soluciones triviales en los enteros. Por ejemplo si $P(x) = x^5$, el problema es, obviamente, más difícil que el último teorema de Fermat para el exponente 5. La mejor aproximación a una sucesión polinómica que sea de Sidon es un resultado de Ruzsa en el que demuestra que existe un α tal que la sucesión $A = \{n^4 + \lfloor \alpha n \rfloor\}$ es una sucesión de Sidon.

Volviendo a los cuadrados, uno de los problemas más esquivos es el que consiste en dar estimaciones del mayor tamaño de un conjunto de Sidon en $\{1^2, \dots, n^2\}$. Como el número de enteros Q_n representables como suma de dos cuadrados y menores que n es $\sim \frac{n}{\sqrt{\log n}}$ se tiene que si $A \subset \{1, \dots, n^2\}$ es de Sidon entonces

$$\begin{aligned} |A|^2 &= \sum_{j \in \{x^2+y^2,\ x,y \le n\}} |\{(a,a') :\ j = a + a',\ a, a' \in A\} \le 2|Q_{2n}| \\ &\ll \frac{n}{\sqrt{\log n}} \end{aligned}$$

lo que implica que $|A| \ll n^{1/2}(\log n)^{-1/4}$. Sin embargo no se ha sabido construir un conjunto A que se acerque a esta cota. Utilizando el método probabilístico es posible demostrar de manera sencilla que existe un conjunto A con $|A| \gg n^{1/3-\epsilon}$ para todo $\epsilon > 0$. Incluso, con argumento más complicado es posible demostrar (ver [42]) la existencia de un conjunto con $|A| \gg n^{1/3}$. Es decir, si A es el conjunto de Sidon de mayor cardinal en $\{1^2, \dots, n^2\}$ lo único que se sabe es que

$$n^{1/3} \ll |A| \ll n^{1/2}(\log n)^{-1/4}. \tag{6.12}$$

En [11], utilizando el método probabilístico se demuestra un resultado análogo al de Erdős-Renyi:

Teorema 6.2.1. *Para todo $g \ge 1$ existe una sucesión $B_2[g]$ de cuadrados A, tal que*

$$A(x) \gg x^{\frac{1}{2} - \frac{1}{4g+2}} (\log x)^{-C_g}$$

donde $C_g = \frac{g2^{g+3}}{2g+1}$.

En principio podría haber una subsucesión de los cuadrados con función contadora $A(x) \gg x^{1/2-\epsilon}$, pero es sin duda un problema muy difícil.

La sucesión de los cuadrados es la sucesión convexa por excelencia (la sucesión formada por las diferencias de los elementos consecutivos es

estrictamente creciente). Ello sugiere considerar sucesiones de Sidon que además sean convexas.

¿Qué se puede decir del mayor tamaño posible de un conjunto de Sidon en $\{1, \dots, n\}$ que además es convexo? Probablemente $|A| = o(\sqrt{n})$ pero todavía no hay una demostración de este hecho.

6.3. Conjuntos de Sidon en los enteros

Vimos en el capítulo 3 que no había ninguna sucesión de enteros no negativos con la propiedad de que la función

$$r_A(n) = |\{(a, a') : \ n = a + a', \ a \leq a', \ a, a' \in A\}|$$

fuese constante a partir de un cierto n. La posibilidad de incluir a los enteros negativos ofrece más flexibilidad.

Es fácil construir una sucesión de enteros A con la propiedad de que la función $r_A(n)$ tome el valor 1 para todo entero 1.

Sean $B_1 = \{0, 1\}$ y $C_1 = \{-4, 3\}$ y $A_1 = B_1 \cup C_1$. En general construimos $B_k = \{k - n_k, n_k\}$ donde n_k es el menor entero positivo tal que al añadir B_k a

$$\bigcup_{j=1}^{k-1} \left(B_j \bigcup C_j \right)$$

no aparece ningún entero con más de una represntación. De la misma manera construimos $C_k = \{-k - m_k, m_k\}$ donde m_k es el menor entero positivo tal que al añadir C_k a $B_k \cup \left(\cup_{j=1}^{k-1} (B_j \cup C_j) \right)$ no aparece ningún entero con más de una representación. Es claro que el conjunto

$$A = \bigcup_{j=1}^{\infty} (B_j \cup C_j)$$

satisface las condiciones.

Ejercicio 6.3.1. *Demostrar que existe una sucesión A de enteros positivos tal que todo $n \geq 1$ tiene una represntación única de la forma $n = a - a', \ a, a' \in A$ y tal que $A(x) \gg x^{1/3}$.*

Es natural preguntarse por sucesiones de enteros que satisfagan la condición de que $r(n) = 1$ para todo entero n y que sean tan densas como sean posible. En [15] se demuestra el siguiente resultado.

Teorema 6.3.1. *Sea B una sucesión infinita de Sidon. Entonces existe una sucesión de enteros A tal que $r_A(n) = 1$ para todo $n \in \mathbb{Z}$ y tal que $A(x) = |A \cap [1, x]|$ satisface la desigualdad $A(x) \gg B(x/3)$.*

En particular el teorema muestra que existe una sucesión infinita de enteros A con $|A \cap [-x, x]| > x^{\sqrt{2}-1+o(1)}$ y tal que $r_A(n) = 1$ para todo $n \in \mathbb{Z}$.

6.4. Conjuntos de Sidon de números reales

Consideremos una sucesión finita $a_1, \dots, a_n$ de números reales módulo 1. Pedir que A sea una sucesión de Sidon no tiene mucho sentido porque casi todas las sucesiones de números reales lo van a ser. La manera de considerar el problema análogo consiste en estudiar cómo distan entre sí las sumas $a_i + a_j$. Definimos

$$\delta_n = \min_{\substack{j,k,u,v \le n \\ \{j,k\} \neq \{u,v\}}} \|(a_j + a_k) - (a_u + a_v)\|,$$

donde $\|x\|$ es la distancia de x a los enteros. Como hay $n(n-1)$ diferencias $a - a'$, además del 0, dos de estas diferencias estarán a distancia menor que $\frac{1}{n(n-1)+1}$ y por lo tanto

$$\delta_n \le \frac{1}{n(n-1)+1}.$$

De hecho hay ejemplos para los que se alcanza la cota superior. Para p primo consideramos el conjunto de Sidon de $p+1$ elementos en $\mathbb{Z}_{p^2+p+1}$, digamos $x_1, \dots, x_{p+1}$. La sucesión $a_i = x_i/(p^2+p+1)$ es una sucesión de números reales tales que $\|(a_j + a_k) - (a_u + a_v)\| \ge 1$ para $\{j,k\} \neq \{u,v\}$. Tomando $n = p + 1$ tenemos que

$$\delta_n = \delta_{p+1} \ge \frac{1}{p^2+p+1} = \frac{1}{n(n-1)+1}.$$

Es decir, en lo que se refiere a sucesiones finitas de números reales módulo 1, el problema es equivalente a estudiar los conjuntos de Sidon en grupos cíclicos y el problema no nos ofrece ninguna sorpresa. Muy distinto es lo que ocurre para sucesiones infinitas.

¿Existe una sucesión infinita (a_n) de números reales módulo 1 tal que $\delta_n \gg \frac{1}{n^2}$. Este problema se puede considerar como el problema análogo de encontrar una sucesión infinita de Sidon en los enteros con $A(x) \gg x^{1/2}$. Mientras que Erdős deostró que en este caso sabemos que la respuesta es negativa, para las sucesiones de números reales no sabemos cuál es la respuesta.

Por el contrario, podemos construir una sucesión infinita de numeros reales (a_n) para la que el orden de magnitud de δ_n es sólo un poco menor.

Teorema 6.4.1. *Existe una sucesión infinita de números reales con la propiedad de que*

$$\delta_n \gg \frac{1}{(n \log n)^2}.$$

Demostración. Sean $q_1 = 5 < q_2 < \cdots$ al sucesión de los primos $p \equiv 5$ y escribimos de la forma $p_j = \rho_j \overline{\rho}_j$ para el correspondiente primo Gaussiano ρ_j. Consideremos ahora los números $\alpha_j = \overline{\rho}_j/\rho_j$. Para $\{j,k\} \neq \{u,v\}$ con $j,k,u,v \leq n$ estimamos la diferencia de los productos

$$\alpha_j\alpha_k - \alpha_u\alpha_v = \frac{\overline{\rho}_j\overline{\rho}_k\rho_u\rho_v - \rho_j\rho_k\overline{\rho}_u\overline{\rho}_v}{\rho_j\rho_k\rho_u\rho_v}.$$

El numerados es un entero de Gauss distinto de cero por la factorización única de los enteros de Gauss. Por lo tanto su módulo es al menos 1 y tenemos que

$$|\alpha_j\alpha_k - \alpha_u\alpha_v| \geq \frac{1}{|\rho_j\rho_k\rho_u\rho_v|} = \frac{1}{\sqrt{p_jp_kp_up_v}} \geq \frac{c}{(n\log n)^2}$$

para alguna constante $c > 0$, debido a que $p_j, p_k, p_u, p_v \leq p_n \sim n \log n$.

Finalmente definimos a_j de la forma $\alpha_j = e^{2\pi i a_j}$ y se tiene la desigualdad

$$\begin{aligned} |\alpha_j\alpha_k - \alpha_u\alpha_v| &= |1 - \alpha_u\alpha_v/(\alpha_j\alpha_k)| \\ &= |1 - e^{2\pi i(a_u+a_v-a_j-a_k)}| \\ &\leq 2\pi|a_j + a_k - a_u - a_v|. \end{aligned}$$

Sustituyendo esto en la desigualdad anterior obtenemos el teorema. □

Capítulo 7

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 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 puede sevir de fuente de inspiración para jóvenes investigadores.

7.0.1. Conjuntos de Sidon en intervalos

Erdős y Turan [29] demostraron que si $A \subset [1, n]$ es un conjunto de Sidon entonces $|A| < n^{1/2} + O(n^{1/4})$. Lindstrom [43] y Ruzsa [54] 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 [9] (que ya estaba implícita en [54]) y que supone la cota $|A| < n^{1/2} + n^{1/4} + 1/2$. Mejorar esta cota superior (incluso eliminar el $1/2$ a partir de un cierto n) 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 [26], 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 7.0.1 (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 7.0.2. *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 [9].

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 7.0.3. *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.*

7.0.2. Conjuntos de Sidon en dimensiones superiores

Conjetura 7.0.4. *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 7.0.5. *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.

7.0.3. 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 $n = p(p-1)$, $n = q^2 + q + 1$ y $n = q^2 - 1$ entonces $\mathbb{Z}_n$ que contienen un conjunto de Sidón 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 $\liminf_{n\to\infty} \frac{F_2(\mathbb{Z}_n)}{\sqrt{n}} \geq 1/\sqrt{2}$.

Conjetura 7.0.6.

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

Probablemente este límite es en realidad $1/\sqrt{2}$.

Los conjuntos de la forma

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

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 7.0.7. *Todos los conjuntos de Sidon en $\mathbb{Z}_p \times \mathbb{Z}_p$ con p elementos son de esta forma.*

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.

7.0.4. 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 7.0.8. *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 [55] ha demostrado que $M(n) \ll (n \log n)^{1/3}$.

Problema 7.0.1. *¿Es cierto que $M(n)/n^{1/3} \to \infty$?*

Una respuesta afirmativa a este problema implicaría inmediatamente la conjetura 7.0.8.

La siguiente conjetura aparece insistentemente en varios artículos de Erdős.

Conjetura 7.0.9 (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 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 [41] lo demostró para $c = 1/\sqrt{2}$.

Conjetura 7.0.10 (Erdős)**.** *Existe una sucesión infinita de Sidon con*

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

Erdős también observó que la conjetura 7.0.10 seguiría de la siguiente.

Conjetura 7.0.11 (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 7.0.2. *Sea A una sucesión infinita con $|A_x + A_x| \sim |A_x|^2/2$. ¿Es cierto que $\liminf_{x\to\infty} \frac{A(x)}{\sqrt{x}} = 0$?*

7.0.5. 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 7.0.3. *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, $F_h(n) \sim n^{1/h}$.

Merece la pena mencionar el siguiente resultado de Timmons.

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 7.0.12. *Si A es una sucesión B_h infinita entonces*

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

Los conjuntos $B_2[g]$ con $g \geq 2$ son más difíciles de estudiar que los conjuntos de Sidon.

Problema 7.0.4. *Demostrar que para todo $g \geq 2$ existe el límite*

$$\sigma_g = \lim_{N\to\infty} \frac{F_2(g,N)}{\sqrt{gN}}.$$

Solo se conoce la existencia de este límite cuando $g = 1$. En ese caso, como ya hemos visto, $\sigma_1 = 1$. Si definimos

$$\underline{\sigma}_g = \liminf_{N\to\infty} \frac{F_2(g,N)}{\sqrt{gN}} \leq \limsup_{N\to\infty} \frac{F_2(g,N)}{\sqrt{gN}} = \overline{\sigma}_g,$$

se sabe que

$$\lim_{g\to\infty} \underline{\sigma}_g = \lim_{g\to\infty} \overline{\sigma}_g = \sigma$$

donde σ es una constante explícita, aunque difícil de calcular.

7.0.6. 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 7.0.5. *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 [27] y la cota superior a Pikhurko[52].

Conjetura 7.0.13. *Demostrar que si $A \subset \{1,\ldots,n\}$ 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 7.0.6. *Construir un conjunto, lo más grande posible, $A \subset \{1,\ldots,n\}$ 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 7.0.7. *¿ 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 [58]. 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 [40] 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 7.0.14 (Erdős)**.** *Todo conjunto de enteros de n elementos contiene un conjunto de sidon con $\sim \sqrt{n}$ elementos.*

Mi opnión personal es que esta conjetura es falsa.

7.0.7. 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 7.0.15. *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 7.0.16. *Si $A(x) \gg x^{1/2}$ entonces su función de representación no estáacotada. Es decir, A no es una sucesión $B_2[g]$ para ningún g.*

En general se conjetura que si $A(x) \gg x^{1/h}$ entonces A no puede ser una sucesión $B_h[g]$ para ningún g.

En la otra dirección una Erdős conjeturó lo siguiente.

Conjetura 7.0.17 (Erdős)**.** *Existe alguna sucesión de Sidon que es base asintótica de orden 3.*

Esta conjetura parece difícil pero recientemente se ha demostrado [8] 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, *The greedy Sidon sequence*, en preparación.

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

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

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

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

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

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

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

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

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

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

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

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

[20] 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)

[21] 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)

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

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

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

[25] 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.

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

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

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

[29] 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.

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

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

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

[33] 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.

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

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

[36] Halberstam and Roth, *Sequences*

[37] 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[64] 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.

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

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

La Asociación Matemática Venezolana fue fundada en 1990 como una organización civil sin fines de lucro cuya finalidad es trabajar por el desarrollo de las matemáticas en Venezuela.

Asociación Matemática Venezolana
Apartado 47.898, Caracas 1041-A, Venezuela
`http://www.ciens.ucv.ve/ciens/amv/`

Gobierno **Bolivariano** de Venezuela

Ministerio del Poder Popular para **Ciencia, Tecnología e Innovación**

juventud BICENTENARIA