Capítulo 7

Teoría Combinatoria de Números

La Teoría combinatoria de números se ocupa de aquellos problemas de la teoría de números con mayor sabor combinatorio. El matemático más representativo de este área ha sido sin duda el matemático húngaro Paul Erdős. No sólo planteo infinidad de problemas, algunos de ellos imprescindibles para entender las matemáticas del Siglo XX, sino que desarrollo teorías, novedosas en su día, que hoy son parte habitual de las herramientas usadas en esta disciplina. El método probabilístico es un buen ejemplo de ello.

¿Qué podemos decir acerca del tamaño de un conjunto $A \subset [1, N]$ de enteros con la propiedad de que sus elementos no satisfacen una ecuación determinada?

La respuesta a esta pregunta para cada una de las siguientes ecuaciones representa un problema central en la teoría combinatoria de números.

1. $x + y = 2z$ (Conjuntos sin progresiones aritméticas)
2. $x + y = z + w$ (Conjuntos de Sidon)
3. $x + y = z$ (Conjuntos libres de sumas)

Uno de los resultados más representativos de la teoría combinatoria de números es el siguiente.

Definicion 7.0.1. *Decimmos que una sucesión infinita de enteros A tiene densidad (asintótica inferior) positiva si* $\liminf_{x\to\infty} \frac{A(x)}{x} > 0$.

Por ejemplos la sucesión de los primos es un ejemplo de sucesión de densidad cero. La sucesión de los enteros positivos libres de cuadrados es un ejemplo de sucesi'on de densidad positiva, concretamente de densidad $6/\pi^2$.

El siguiente teorema, que no demostraremos aquí afirma lo siguiente respecto a la ecuación 1) de arriba.

Teorema 7.0.2 (Roth, 1970)**.** *Si A es una sucesión con densidad positiva entonces contiene 3 términos en progresión aritmtíca.*

Erdős conjeturó que lo mismo debería ser cierto para progresiones aritméticas de longitud k, fuera quien fuera k. Esto fue confirmado finalmente por E. Szemeredi.

Teorema 7.0.3 (Szemeredi, 1976)**.** *Para todo $k \geq 3$, si A es una sucesión con densidad positiva entonces contiene k términos en progresión aritmética.*

De otra manera, una sucesión con densidad positiva contiene progresiones aritméticas arbitrariamente largas.

Aunque el Teorema de Szemeredi no se aplicar a la sucesión de los números primos (por tener densidad cero), B. Green y T. Tao demostraron este resultado para la sucesión de los primos.

Teorema 7.0.4 (Green-Tao, 1998)**.** *La sucesión de los primos contiene progresiones aritméticas arbitrariamente largas.*

Los resultados comentados anteriormente son demasiado difíciles como para incluir en este curso sus demostraciones.

7.1. Conjuntos de Sidon

7.1.1. Preliminares

Dado un grupo G decimos que $A \subset G$ es un conjunto de Sidon si todas las diferencias $a - a' : \ a, a' \in A$ son distintas. Representaremos por $r_A(x)$ y $d_A(x)$ al número de representaciones de n de la forma

$$x = a + a', \quad a, a' \in A \tag{7.1}$$

$$x = a - a', \quad a, a' \in A \tag{7.2}$$

respectivamente.

Un conjunto de Sidon es por tanto aquel tal que $d_A(x) \leq 1$ para todo $x \in G, \ x \neq 0$ o de otra manera, aquel tal que $r_A(x) \leq 2$ para todo $x \in G$.

De manera más general, dados dos conjuntos A, B, definimos $r_{A+B}(x)$ como el número de representaciones de x de la forma $x = a + b, \ a \in A, \ b \in B$.

Se define el conjunto suma de dos conjuntos A y B como

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

De manera más general se define

$$A_1+\cdots+A_k=\{a_1+\cdots+a_k:\ a_i\in A_i\}.$$

Los conjuntos productos se definen de manera análoga.

Observemos que

$$\sum_x r_{A+B}(x)=|A||B| \tag{7.3}$$

ya que

$$\begin{aligned}\sum_x r_{A+B}(x) &= \sum_x \#\{(a,b),\ a+b=x,\ a\in A,\ b\in B\}\\ &= \#\{(a,b),\ a\in A,\ b\in B\}=|A||B|\end{aligned}$$

Recientemente se ha acuñado el término energía aditiva de A y B para la suma

$$\sum_x r^2_{A+B}(x)=\sum_x r_{A-A}(x)r_{B-B}(x). \tag{7.4}$$

La igualdad es debido a que la suma $\sum_x r^2_{A+B}(x)$ cuenta el número de cuadruplas (a,b,a',b') tales que $a+b=a'+b'$, que coincide con el número de cuadruplas tales que $a-a'=b'-b$, que es precisamente el valor de la suma $\sum_x r_{A-A}(x)r_{B-B}(x)$.

En el caso $A=B$, las identidades (7.3) y (7.4) se traducen simplemente en $\sum_x r_{A+A}(x)=\sum_x r_{A-A}(x)=|A|^2$ y $\sum_x r^2_{A+A}(x)=\sum_x r^2_{A-A}(x)$. Recuperando la notación anterior, $r_A=r_{A+A}$ y $d_A=r_{A-A}$, tenemos

$$\sum_x r_A(x) = \sum_x d_A(x)=|A|^2 \tag{7.5}$$

$$\sum_x r^2_A(x) = \sum_x d^2_A(x). \tag{7.6}$$

7.1.2. Cotas superiores

La cota superior más ingenua para el tamaño de un conjunto de Sidon $A\subset[1,N]$ es consecuencia de la observación

$$|A|^2=d_A(0)+\sum_{1\le|n|\le N-1} d_A(n)\le |A|+2N-2,$$

de donde

$$|A|\le\sqrt{2N}+1/2.$$

Teorema 7.1.1. *Si $A \subset [1, N]$ es un conjunto de Sidon entonces*

$$|A| \leq N^{1/2} + N^{1/4} + 1/2.$$

Demostración. Sea $B = [0, l]$ con $l = \lfloor \sqrt{n(|A|-1)} \rfloor$. Utilizando (7.3), (7.4) y la desigualdad de Cauchy obtenemos

$$(|A||B|)^2 = \left(\sum_{n \in A+B} r_{A+B}(n) \right)^2 \leq |A+B| \sum_n r_{A+B}^2(n) = |A+B| \sum_n r_{A-A}(n) r_{B-B}(n).$$

La última suma está acotada por

$$r_{A-A}(0) r_{B-B}(0) + \sum_{n \neq 0} r_{B-B}(n) \leq |A||B| + |B|^2 - |B|.$$

De donde

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

Por lo tanto $|A| - \sqrt{N} \leq \sqrt{|A|-1}$. Escribiendo $|A| = \sqrt{N} + cN^{1/4} + 1/2$ y elevando al cuadrado tenemos $c^2\sqrt{N} + cN^{1/4} + 1/4 < \sqrt{N} + cN^{1/4} - 1/2$, que no se satisface si $c \geq 1$. □

En la siguiente sección veremos que el término $N^{1/2}$ en esta cota superior es óptimo.

7.1.3. Conjuntos de Sidon. Construcciones.

La construcción más ingenua de un conjunto de Sidon consiste en empezar con $a_1 = 1,\ a_2 = 2$, y una vez construidos $a_1, \ldots, a_{n-1}$, añadir el menor entero positivo a_n tal que $a_n \neq a_i - a_j + a_k,\ 1 \leq i, j, k \leq n-1$. Los primeros términos de esta sucesión, conocida como sucesión de Mian-Chowla, son los siguientes:

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

Se desconoce cómo crece realmente esta sucesión aunque como a lo más hay $(n-1)^3$ enteros prohibidos para a_n siempre es cierto que $a_n \leq (n-1)^3+1$, lo que nos permite seleccionar un conjuno de Sidon en $\{1,\ldots,n\}$ con $n^{1/3}$ elementos por lo menos.

Una construcción más densa se basa en el hecho de que el conjunto de los primos es un conjunto de Sidon multiplicativo; es decir, todos los productos pq son distintos.

Teorema 7.1.2. *Dado un primo q y una raiz primitiva g (mód q), el conjunto*

$$A = \{x : \ g^x \equiv p \pmod{q}, \quad \textit{para algún primo } p \leq \sqrt{q}\}$$

es un conjunto de Sidon en $\mathbb{Z}_{q-1}$ de tamaño $|A| = \pi(\sqrt{q}) \sim \frac{\sqrt{q}}{2\log q}$.

Demostración. Supongamos que $x_1+x_2 \equiv x_3+x_4 \pmod{q-1}$ para $x_1,x_2,x_3,x_4 \in A$. Entonces existirán primos $p_i \leq \sqrt{q}$ tales que $g^{x_i} \equiv p_i \pmod{q}$, $i=1,2,3,4$. Eso implica que $g^{x_1+x_2} \equiv g^{x_3+x_4} \pmod{q}$ y ppor tanto $p_1p_2 \equiv p_3p_4 \mod q$. Pero como $1 \leq p_1p_2,\ p_3p_4 \leq q$, lo que tenemos es una igualdad entre enteros: $p_1p_2 = p_3p_4$, así que $\{p_1,p_2\} = \{p_3,p_4\}$ por ser los p_i primos. □

La rica estructura de algunos grupos nos va a permitir construir los conjuntos finitos de Sidon más densos que se conocen.

En las tres construcciones que presentamos a continuación p es siempre un primo impar y g es una raíz primitiva en $\mathbf{F}_p$. Los tres ejemplos se pueden representar gráficamente (ver figuras más adelante) y el lector puede recrear su vista observando que no existen cuatro puntos formando un paralelogramo.

La construcción del ejemplo 3, en particular, nos permitirá construir, después de unas observaciones sencillas, un conjunto de Sidon en $\{1,\ldots,n\}$ con $\sim n^{1/2}$ elementos.

Ejemplo 7.1.3. *El conjunto de Sidon más sencillo que se conoce es el conjunto de p elementos*

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

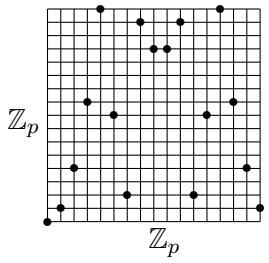
Ejemplo 7.1.4. *A Golomb se debe el conjunto de Sidon de $p-2$ elementos*

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

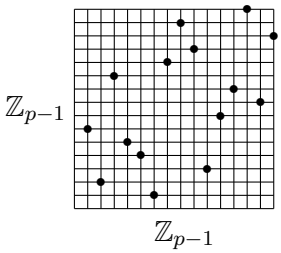
Ejemplo 7.1.5. *Welch descubrió el conjunto de Sidon de $p-1$ elementos*

$$\mathcal{A} = \{(x,g^x), 0 \leq x < p-1\} \subset \mathbb{Z}_{p-1} \times \mathbb{Z}_p.$$

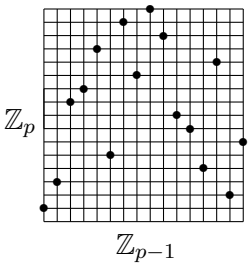
Dejamos como ejercicio comprobar que los tres conjuntos de los ejemplos anteriores son de Sidon.



Ejemplo 1



Ejemplo 2



Ejemplo 3

Los isomorfismos entre grupos transforman conjuntos de Sidon en conjuntos de Sidon. Es decir, si $\phi : G \to G'$ es un isomorfismo entre los grupos G y G', y $\mathcal{A}$ es un conjunto de Sidon en G entonces el conjunto $\phi(\mathcal{A}) = \{\phi(a),\ a \in \mathcal{A}\}$ es un conjunto de Sidon en G'. Basta observar que

$$\phi(a) + \phi(b) = \phi(c) + \phi(d) \implies \phi(a + b - c - d) = 0$$

y por lo tanto $a + b = c + d$. Pero como a, b, c, d pertenecen a un conjunto de Sidon entonces $\{a, b\} = \{c, d\}$, por lo que $\{\phi(a), \phi(b)\} = \{\phi(c), \phi(d)\}$.

En particular, el isomorfismo natural $\phi : \mathbb{Z}_{p-1} \times \mathbb{Z}_p \to \mathbb{Z}_{(p-1)p}$ definido por $\phi(a, b) = x$ donde x es el elemento de $\mathbb{Z}_{(p-1)p}$ tal que $x \equiv a \pmod{p-1}$ y $x \equiv b \pmod{p}$, transforma, mediante el teorema chino del resto, el conjunto de Sidon del ejemplo 3 en el conjunto de Sidon

$$\mathcal{A} = \{(p-1)(x - g^x)_p + x,\ 1 \le x \le p-1\} \subset \mathbb{Z}_{p(p-1)}, \tag{7.7}$$

donde $(y)_p$ es el menor resto positivo congruente con $y \pmod{p}$.

Aunque hay otras dos construcciones clásicas de conjuntos de Sidon en grupos de la forma $\mathbb{Z}_m$, ésta, debida a Ruzsa, es la más sencilla de describir.

Veamos cómo podemos utilizar este conjunto para construir conjuntos de Sidon en nuestro conjunto original $\{1, \ldots, n\}$.

Los enteros en $\{1, \ldots, m\}$ que representan los elementos de un conjunto de Sidon en $\mathbb{Z}_m$ forman en particular un conjunto de Sidon en $\{1, \ldots, m\}$. Como sabemos de la existencia de conjuntos de Sidon en $\mathbb{Z}_m$ con $\sim m^{1/2}$ para valores particulares de m, por ejemplo para los de la forma $m = p(p-1)$ con p primo, buscaremos el primo p_i tal que $p_i(p_i - 1) \le n < p_{i+1}(p_{i+1} - 1)$. Si llamamos $F(n) = \text{máx}\{|A|,\ A \subset [1, n],\ A \text{ Sidon}\}$, claramente,

$$\frac{F(n)}{\sqrt{n}} \ge \frac{F(p_i(p_i-1))}{\sqrt{p_{i+1}(p_{i+1}-1)}} \ge \frac{p_i}{p_{i+1}} \to 1$$

por el teorema del número primo.

El siguiente lema es interesante para muchas aplicaciones

Lema 7.1.6. *Sea A un conjunto de Sidon en un grupo abeliano G. Entonces, para cualquier conjunto $B \subset G$ tenemos*

$$\sum_{x\in G}\left(|A\cap(B+x)-\frac{|A||B|}{|G|}\right)^2 \leq (|A|-1)|B|+|B|^2\frac{|G|-|A|^2}{|G|}.$$

Demostración. Utilizaremos el hecho de que $|A\cap(B+x)| = r_{A-B}(x)$ y que $\sum_x r_{A-B}(x) = |A||B|$ para obtener

$$\sum_{x\in G}\left(|A\cap(B+x)|-\frac{|A||B|}{|G|}\right)^2 = \sum_{x\in G} r^2_{A-B}(x) - \frac{|A|^2|B|^2}{|G|}. \tag{7.8}$$

La identidad (7.4) nos permite escribir

$$\sum_{x\in G}\left(|A\cap(B+x)|-\frac{|A||B|}{|G|}\right)^2 = \sum_{x\in G} r_{A-A}(x)r_{B-B}(x) - \frac{|A|^2|B|^2}{|G|}. \tag{7.9}$$

Como A es un conjunto de Sidon entonces $r_{A-A}(x) \leq 1$ para todo $x \neq 0$ y entonces

$$\begin{aligned}\sum_{x\in G} r_{A-A}(x)r_{B-B}(x) &= |A||B| + \sum_{e\neq 0} r_{A-A}(x)r_{B-B}(x) \\ &\leq |A||B| + \sum_{x\neq 0} r_{B-B}(x) = |A||B| + |B|^2 - |B|.\end{aligned} \tag{7.10}$$

y concluimos la demostración. □

7.1.4. Sucesiones de Sidon infinitas

Nuestro conocimiento sobre las sucesiones infinitas de Sidon es mucho más escaso. No se sabe, ni siquiera de una manera aproximada, cuál es el crecimiento más lento que puede llegar a tener una sucesión de Sidon. Utilizaremos el término "sucesión de Sidon"para referirnos a conjuntos de Sidon infinitos.

La sucesión de las potencias de dos es una sucesión de Sidon porque claramente $2^j + 2^k = 2^{j'} + 2^{k'} \implies \{j,k\} = \{j',k'\}$. Es natural preguntarse por sucesiones de Sidon con un crecimiento más lento, por ejemplo de tipo polinómico.

¿Para que valores de k la sucesión $\mathcal{A} = \{n^k,\ n \geq 1\}$ es una sucesión de Sidon?

Seguramente el lector ya haya observado que el problema es equivalente a decidir si la ecuación

$$x^k + y^k = u^k + v^k$$

tiene soluciones no triviales y que entonces es por lo menos tan difícil como el último teorema de Fermat. Se sabe que para $k = 2, 3, 4$ la ecuación anterior sí tiene soluciones y se conjetura que no las tiene para $k \geq 5$. Sin embargo no se conoce ningún polinomio $p(x)$ para el cual la sucesión $\mathcal{A} = \{p(n),\ n \geq 1\}$ sea de Sidon.

La manera de medir el tamaño de sucesiones infinitas es por medio de la función contadora de la sucesión, $\mathcal{A}(n) = |\{a \leq n,\ a \in \mathcal{A}\}|$. A la vista de lo que ya hemos visto para conjuntos finitos, tenemos que, si $\mathcal{A}$ es una sucesión de Sidon, entonces

$$\mathcal{A}(n) \leq n^{1/2} + n^{1/4} + 1,$$

por lo que parece natural preguntarse si existe alguna sucesión de Sidon $\mathcal{A}$ tal que $\mathcal{A}(n) \gg n^{1/2}$. Es decir, si existe una sucesión que tenga un crecimiento parecido al de la sucesión de los cuadrados.

Erdős demostró que no existe tal sucesión. Más concretamente, demostró que si $\mathcal{A}$ es una sucesión de Sidon infinita entonces

$$\liminf_{n\to\infty} \frac{\mathcal{A}(n)}{\sqrt{n/\log n}} < \infty.$$

¿Para que valores de α existe una sucesión de Sidon $\mathcal{A}$ con $\mathcal{A}(n) \gg n^\alpha$?

Conjetura 7.1.7 (Erdős)**.** *Para todo $\epsilon > 0$, existe una sucesión de Sidon $\mathcal{A}$ con $\mathcal{A}(n) \gg n^{\frac{1}{2}-\epsilon}$.*

La sucesion de Mian-Chowla definida al principio de la sección 2 satisface $\mathcal{A}(n) \geq n^{1/3}$. Ruzsa en 1998 demostró la existencia de una sucesión de Sidon infinita con

$$\mathcal{A}(n) > n^{\sqrt{2}-1-o(1)}.$$

Recientemente, el autor de estas notas ha construido de manera explícita una sucesión de Sidon infinita del mismo crecimiento que la de Ruzsa. El término $o(1)$ refleja una cantidad que tiende a cero cuando n tiende a infinito.

7.2. La conjetura de Erdős-Turan

¿Existe alguna sucesión infinita de enteros no negativos $\mathcal{A}$ tal que $r_{\mathcal{A}}(n)$ es constante para todo n suficientemente grande, pongamos $n \geq n_0$?

La respuesta es que no. Los analistas apreciarán sin duda el siguiente argumento de Dirac. Sea la función $f(z) = \sum_{a\in\mathcal{A}} z^a,\ |z| < 1$. Entonces

$$f^2(z) = \sum_{a,a'\in\mathcal{A}} z^{a+a'} = \sum_{n\geq 0} \tilde{r}_{\mathcal{A}}(n) z^n.$$

Observando que $\tilde{r}_{\mathcal{A}}(n) = 2r_{\mathcal{A}}(n) - 1$ si $n = 2a$ para algún $a \in \mathcal{A}$ y $\tilde{r}_{\mathcal{A}}(n) = 2r_{\mathcal{A}}(n)$ en otro caso, podemos escribir

$$f^2(z) = 2\sum_{n\geq 0} r_{\mathcal{A}}(n) z^n - \sum_{a\in\mathcal{A}} z^{2a}.$$

Si asumimos que $r_{\mathcal{A}}(n) = C$ para todo $n \geq n_0$, obtenemos la igualdad

$$f^2(z) + f(z^2) = 2\sum_{0\leq n<n_0} r_{\mathcal{A}}(n) z^n + 2\sum_{n\geq n_0} r_{\mathcal{A}}(n) z^n = P(z) + 2C\frac{z^{n_0}}{1-z},$$

donde $P(z)$ es un polinomio de grado $n_0 - 1$.

Cuando $z \to -1$ la parte de la derecha tiende a $P(-1) + C(-1)^{n_0} < \infty$ y la parte de la izquierda diverge ya que $f^2(z) > 0$ y $f(z^2) \to f(1) = \infty$, obteniendo una contradicción.

Imponer la condición de que $r_{\mathcal{A}}(n)$ sea constante para n suficientemente grande puede parecer muy exigente y el resultado de Dirac era previsible.

¿Y si sólo pedimos, por ejemplo, que $1 \leq r_{\mathcal{A}}(n) \leq 1000$?

Aquí es donde hace su aparición una de los problemas más importantes en la teoría aditiva de números.

Conjetura 7.2.1 (Erdős-Turán)**.** *Si $r_{\mathcal{A}}(n) \geq 1$ para todo $n \geq 1$, la función $r_{\mathcal{A}}(n)$ no está acotada uniformemente en n.*

Si algún lector decide intentar demostrar esta conjetura, debería hacer primero los ejercicios 7.7.8 y 7.7.10.

7.3. Bases

Definicion 7.3.1. *Se dice que una sucesin de enteros no negativos A es una base (asinttica) de orden h si todo entero no negativo (suficientemente grande) se puede escribir como suma de h elementos de A.*

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

Otro ejemplo notable es la sucesind de los primos, que despus 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 sucesin de los primos es una base de orden 2 para los pares mayores que 2.

Es claro que cuanto ms densa sea una sucesin ms fcil es que sea una base. Por el contrario, si la sucesin es muy densa, ms difcil es que sea una sucesind e Sidon o una sucesin B_h. Otra manera de enunciar la conjetura de Erdős Turan es diciendo que no puede existir una sucesin $B_2[g]$ que sea una base asinttica 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 nmero 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 fcil construir bases de orden h con funcin contadora $A(n) \ll n^{1/h}$. Considerse por ejemplo la sucesin

$$A = \bigcup_{k=0}^{h-1} A_k \tag{7.11}$$

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 estimacin del orden de magnitud de $A(x)$.

No es difcil demostrar que una sucesin de Sidon no puede ser una base asinttica de orden 2. Una conjetura famosa de Erdős afirma que la exitencia de una sucesin de Sidon que es base asinttica de orden 3.

Conjetura 7.3.2 (Erdős)**.** *Existen sucesiones de Sidon que son bases asintticas de orden* 3*.*

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

Definicion 7.3.3. *Decimos que A es una base asinttica de orden $h+\epsilon$ si todo entero n suficientemente grande se puede escribir de la forma*

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

El que escribe estas notas ha demostrado el siguiente teorema.

Teorema 7.3.4. *Para todo $\epsilon > 0$ existe una sucesinde Sidon que es una base asinttica de orden $3 + \epsilon$.*

La demostracin es demasiado complicada para ser incluida en este curso.

7.4. Conjuntos suma y producto

Es fácil ver que si A es una progresión aritmética de números enteros entonces $|A + A| = 2|A| - 1$. Un poco más difícil es ver que las progresiones aritméticas son los únicos conjuntos donde se da la igualdad.

Teorema 7.4.1. *Si A y B son conjuntos de enteros entonces $|A+B| \geq |A|+|B|-1$. Además, la igualdad se da si alguno de los dos conjuntos tiene un sólo elemento o si los dos conjuntos son progresiones aritméticas con la misma diferencia.*

Demostración. Sean $a_1 < \cdots < a_j$ y $b_1 < \cdots < b_k$ los elementos de A y B respectivamente. Es claro que

$$b_1 + a_1 < b_1 + a_2 < \cdots < b_1 + a_j < b_2 + a_j < \cdots < b_k + a_j.$$

Entonces tenemos por lo menos $j + k - 1 = |A| + |B| - 1$ elementos diferentes en esta colección de elementos de $A + B$.

Para ver el resultado inverso, pongamos las dos sucesiones ordenadas de elementos de $A + B$

$$b_1 + a_1 < b_1 + a_2 < b_1 + a_3 < \cdots < b_1 + a_j < b_2 + a_j < \cdots < b_{k-1} + a_j < b_k + a_j$$
$$b_2 + a_1 < b_2 + a_2 < \cdots < b_2 + a_{j-1} < b_3 + a_{j-1} < \cdots < b_k + a_{j-1}$$

En la primer sucesión ya hay $j + k - 1$ elementos. Si $A + B$ no tiene más elementos que estos, los elementos de la segunda sucesión tienen que estar en la primera. Pero como $b_1 + a_1$ y $b_k + a_j$ no pueden estar en la segunda, luego necesariamente $b_1+a_2 = b_2+a_1, \ldots b_1+a_3 = b_2+a_2, ..., b_1+a_j = b_2+a_{j-1}$. Es decir, $a_{i+1}-a_i = b_2-b_1$ para todo $i = 1, \ldots, j-1$. Luego A es una progresión aritmética de diferencia b_2-b_1. De la misma manera demostramos que B tiene que ser una progresión aritmética de diferencia a_2-a_1. Pero como $a_2-a_1 = b_2-b_1$ concluimos que A y B son progresiones aritméticas de la misma diferencia. □

Por otra parte el tamaño de $A+A$ es máximo cuando todas las sumas $a+a'$ son distinta; es decir, cuando A es un conjunto de Sidon. En ese case $|A+A| = \frac{|A|(|A|-1)}{2}$.

De la misma manera que hemos hecho para los conjuntos suma se puede ver (ver ejercicios) que $2|A| - 1 \leq |AA| \leq \frac{|A|(|A|-1)}{2}$ y que la cota superior se alcanza cuando A es una progresión geométrica.

Erdős y Szemeredi conjeturaron que el conjunto suma y el conjunto producto no pueden ser simultaneamente pequeños. Más concretamente conjeturaron que para todo $\epsilon > 0$ se tiene que $|A+A|+|AA| \gg |A|^{2-\epsilon}$. Este problema está aún sin resolver. El mejor resultado se debe a Solymosi. Es consecuencia inmediata del siguiente teorema:

Teorema 7.4.2 (J. Solymosi, 6 de Junio de 2008)**.** *Para todo conjunto A de números reales,*

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

En particular,

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

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

$$E(A) \geq \frac{|A|^4}{|AA|}. \tag{7.12}$$

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

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

Existe entonces un j y un m tales que

$$m = \#\{l_\lambda :\ 2^{j-1} \leq |l_\lambda \cap (A\times A)| < 2^j\} \geq 2^{-2j}\frac{E(A)}{\log_2|A|}. \tag{7.13}$$

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

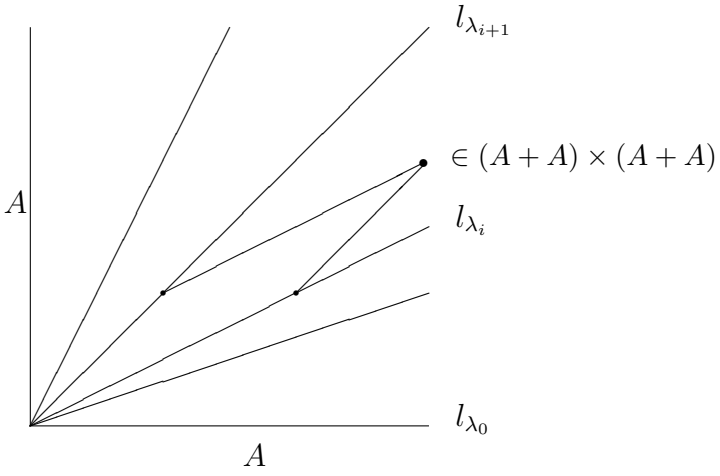
$$|A+A|^2 \geq \left|\bigcup_{i=0}^{m-1} (l_{\lambda_i}\cap(A\times A)) + \big(l_{\lambda_{i+1}}\cap(A\times A)\big)\right| \tag{7.14}$$

$$= \sum_{i=0}^{m-1} |l_{\lambda_i}\cap(A\times A)||l_{\lambda_{i+1}}\cap(A\times A)| \geq m2^{2j-2}. \tag{7.15}$$

De (7.13) y (7.14) obtenemos

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

que junto con (7.12) nos da la primera afirmación del teorema.



Para demostrar la segunda, simplemente observar que si $|A+A| < \frac{|A|^{4/3}}{(\log|A|)^{1/3}}$ entonces la primera parte del teorema nos da $|AA| > \frac{|A|^{4/3}}{4(\log|A|)^{1/3}}$. □

7.4.1. Estimaciones suma-producto en $\mathbf{F}_p$

Teorema 7.4.3. *Sea A un subconjunto de $\mathbf{F}_p$. Entonces*

$$|AA||A+A| \geq \frac{1}{3} \min\left(|A|p, \frac{|A|^4}{p}\right)$$

Demostración. Escribamos $\log A = \{y : \ g^y \in A_i\}$. Es claro que $|\log A| = |A|$.

Consideramos el conjunto de Sidon $\mathcal{A} = \{(x, g^x) : \ x \in \mathbb{Z}_{p-1}\} \subset \mathbb{Z}_{p-1} \times \mathbf{F}_p$ y el conjunto $B = (\log A + \log A, A + A)$.

Es claro que $\{(\log a, a) : \ a \in A_1\} \subset B + e$ para todo $e \in (-\log A) \times (-A)$ y que $\{(\log a, a) : \ a \in A\} \subset \mathcal{A}$. Entonces $|\mathcal{A} \cap (B+e)| \geq |A|$ para todo $e \in (-\log A) \times (-A)$.

Supongamos que $|AA||A+A| < \frac{1}{3}|A|p$. Como $|\mathcal{A}| = p-1$, $|G| = p(p-1)$ y $|B| = |A_1A_2||A_1+A_3|$ tenemos que

$$|\mathcal{A} \cap (B+e)| - \frac{|\mathcal{A}||B|}{|G|} \geq |A| - \frac{|AA||A+A|}{p} \geq \frac{2|A|}{3}$$

para todo $e \in (-\log A) \times (-A)$. Así que

$$\sum_{e\in G}\left(|\mathcal{A}\cap(B+e)| - \frac{|\mathcal{A}||B|}{|G|}\right)^2 \geq \sum_{e\in(-\log A)\times(-A)}\left(\frac{2|A|}{3}\right)^2 = \frac{4}{9}|A|^4$$

El Lemma 7.1.6 implica que

$$\frac{4}{9}|A|^4 \leq (p-2)|B| + \frac{|B|^2}{p} < (p-2)|B| + \frac{|B||A|}{3} < \frac{4}{3}p|B|$$

y obtenemos el resultado. □

7.5. Conjuntos libres de sumas

Se dice que un conjunto está libre se sumas si ningún elemento del conjunto puede escribirse como suma de dos elementos del mismo conjunto. Por ejemplo el conjunto de los números impares es un conjunto libre de sumas. El objeto de esta sección es demostrar el siguiente teorema

Teorema 7.5.1. *Todo conjunto de enteros A contiene un subconjunto $S \subset A$ libre de sumas con al menos $|A|/3$ elementos.*

Demostración. Metamos A en un $\mathbb{Z}_p$ con $p \equiv 1 \pmod 3$. Para cada $x \in \mathbf{F}_p^*$, consideremos el conjunto $xA = \{xa,\ a \in A\}$ como subconjunto de $\mathbb{Z}_p$. Para todo conjunto I que no contiene al 0, tenemos que

$$\mathbb{E}(|xA\cap I|) = \frac{1}{p-1}\sum_{x\in\mathbf{F}_p^*}\sum_{a\in A} I(ax) = \frac{1}{p-1}\sum_{a\in A}\sum_{x\in F_p^*} I(ax) = \frac{1}{p-1}|A||I|.$$

Por lo tanto existe un x tal que $|xA\cap I| \geq \frac{1}{p-1}|A||I|$.

Vamos a ver que si $I = [\frac{p-1}{3}, \frac{2(p-1)}{3})$ entonces el conjunto $S = \{a \in A,\ xa \in I\}$ es libre de sumas. Es claro que I es libre de sumas en $\mathbb{Z}_p$, por lo que $xA \cap I$ también lo es.

Si S no fuera libre de sumas, existirían $a, a', a'' \in S$ tal que $a = a + a'$. En particular, $xa \equiv xa' + xa'' \pmod p$, contradiciendo lo dicho anteriormente. □

7.6. Un problema de Erdős

Decimos que un conjunto $A = \{1 \leq a_1 < \cdots < a_k\}$ es de Erdős si todas las sumas de elmentos distintos de A son distintas. El conjunto de las potencias de dos es un ejemplo.

Erdős se preguntó por una cota inferior para a_k (en función de k). La sucesión $a_i = 2^{i-1},\ i = 1, \ldots, k$ muestra que la cota no puede ser mayor que $\frac{1}{2}2^k$. De hecho se conocen construcciones ligeramente mejores con $a_k = c2^k$ para algún $c < 1/2$. Erdős ha conjeturado que $a_k \gg 2^k$. La cota inferior que vamos a demostrar aquí es prácticamente lo mejor que se sabe salvo por la constante 3.

Teorema 7.6.1. *Si $A = \{1 \leq a_1 < \cdots < a_k\}$ es un conjunto de Erdős entonces $a_k \geq \frac{2^k}{\sqrt{3k}}$.*

Demostración. Sea X_i la variable aleatoria que toma los valores a_i and $-a_i$ con probailidad $1/2$. Es claro que $\mathbb{E}(X_i) = 0$ y $\mathbb{E}(X_i^2) = a_i^2$. Consideremos la varaible $X = X_1 + \cdots + X_k$.

$$\mathbb{E}(X^2) = \sum_{i,j} \mathbb{E}(X_i X_j) = \sum_{i=1}^{k} \mathbb{E}(X_i^2) + \sum_{i \neq j} \mathbb{E}(X_i X_j) = \sum_{i=1}^{k} a_i^2$$

Por una parte es claro que $\sum_{i=1}^{k} a_i^2 \leq k a_k^2$. Por otra,

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

donde s recorre todos los posibles valores que puede tomar X. Observar que cada uno de esos valores se toma con la misma probabilidad 2^{-k} (por ser un conjunto de Erdős) y que todos ellos tienen la misma paridad, pongamos que son todos impares. Entonces

$$\mathbb{E}(X^2) \geq 2^{-k} \cdot 2 \sum_{1 \leq j \leq 2^{k-1}} (2j-1)^2 \geq 2^{2k}/3.$$

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

7.7. Ejercicios de este capítulo

7.7.1. *Demostrar que para todo α, β con $0 \leq \alpha \leq \beta \leq 1$ existe una sucesión de enteros positivos A tal que $\liminf_{n\to\infty} A(n)/n = \alpha$ y $\limsup_{n\to\infty} A(n)/n = \beta$.*

7.7.2. *Demostrar que si $A \subset [1, N]$ y $d_A(n) \leq s$ para todo $n \neq 0$ entonces $|A| \leq (sN)^{1/2} + (sN)^{1/4} + 1/2$.*

7.7.3. *Demostrar que si $r_A(x) \leq g$ para todo $x \in G$, grupo abeliano de orden N, entonces*

$$|A| \leq \sqrt{(2g-1)(N-1)} + 1.$$

7.7.4. *Encontrar un conjunto de Sidon de 8 elementos en* $\{1,\dots,35\}$ *y demostrar que no existe ninguno con 9 elementos.*

7.7.5. *Para cada primo* $p \equiv 1 \pmod 4$ *definimos* $0 < \phi_p < \pi/4$ *como el argumento del entero gaussiano* $a+bi$ *tal que* $a^2+b^2 = p$. *Demostrar que el conjuno* $A = \{[10N\phi_p],\ p \equiv 1 \pmod 4,\ p \le \sqrt{N}\}$ *es un comjunto de Sidon en* $\{1,\dots,N\}$ *con* $\gg N^{1/2}/\log N$ *elementos.*

7.7.6. *Demostrar que los tres conjuntos descritos en los ejemplos 1,2,3 son de Sidon.*

7.7.7. *Demostrar que si* $\phi : G \to G'$ *es un isomorfismo entre grupos y* A *es un conjunto de Sidon en* G, *entonces* $\phi(A)$ *es un conjunto de Sidon en* G'.

7.7.8. *Demostrar que la conjetura de Erdős-Turan no es cierta en* $\mathbb{Z}$ *(en lugar de* $\mathbb{N}$*).*

7.7.9. *Demostrar que existe un conjunto infinito de enteros* A *tal que* $d_A(n) = 1$ *para todo entero* n *distinto de* 0.

7.7.10. *Demostrar que la conjetura de Erdős-Turan no es cierta si en lugar de* $r_A(n)$ *consideramos*

$$r_A^*(n) = \#\{(a,a') :\ a+2a' = n,\ a,a' \in A\}.$$

Más concretamente, utilizar las funciones generatrices para hallar una sucesión A *de números no negativos tal que* $r_A^*(n) = 1$ *para todo* $n \ge 0$.

7.7.11. *Demostrar que la función contadora de la sucesión* A *descrita en* (7.11) *satisface* $A(x) \gg x^{1/h}$.

7.7.12. *Demostrar que si* $A \subset \mathbb{Z}_p$ *es un conjunto libre de sumas, entonces* $|A| \le (p-1)/3$.

7.7.13. *Sean* A *y* B *conjuntos de enteros con más de un elemento cada uno. Demostrar que* $|AB| \ge |A|+|B|-1$ *y que la igualdad es cierta sólo cuando* A *y* B *son progresiones geométricas de la misma razón.*

7.7.14. *Sea* $\lambda \cdot A = \{\lambda a :\ a \in A\}$. *Demostrar que* $|A+2\cdot A| \ge 3|A|-2$ *y que la igualdad es cierta sólo cuando* A *es una progresión aritmética.*

7.7.15. *Utilizar el lema 7.1.6 y un conjunto de Sidon apropiado para demostrar que si* X_1, X_2, X_3, X_4 *son subconjuntos de* $\mathbb{Z}_p$ *tales que* $|X_1||X_2||X_3||X_4| \ge 10p^3$ *entonces* $X_1X_2 - X_3X_4 = \mathbf{F}_p$.