Capítulo 1

Teoría Aditiva y Combinatoria de Números

En este capítulo trataremos algunos problemas aditivos en la teoría de números con cierto sabor combinatorio.

¿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 en cada una de las siguientes ecuaciones representa un problema central en la teoría combinatoria de números.

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

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.

Muchos problemas de la teoría de números se pueden plantear en términos de los conjuntos suma.

Por ejemplo la conjetura de Goldbach afirma que $P + P = \{6, 8, 10, ..., 2n, ...\}$ donde P es el conjunto de los primos impares. El teorema de Lagrange que vimos en una sección anterior afirma que $S + S + S + S = \{0, 1, 2, 3, ..n, ..\}$ donde $S = \{k^2 : \ k \geq 0\}$.

El estudio de todos estos problemas nos permiten ilustrar los diferentes métodos, combinatorios, analíticos y probabilísticos que aparecen con frecuencia en la teoría aditiva combinatoria de números.

Empezaremos con los métodos de criba que han permitido resolver muchos problemas.

1.1. Métodos de criba

Supongamos que queremos construir una tabla formada por todos los números primos menores que un cierto entero positive x.

Empezaremos escribiendo todos los enteros menores que x. Como un entero compuesto debe ser divisible por por un primo menor o igual que su raíz cuadrada, el procedimiento a seguir consistirá en ir tachando todos aquellos que sean divisibles por algún primo menor que $\sqrt{x}$. Los números que sobrevivan a esta criba, los no tachados, serán aquellos primos comprendidos entre $\sqrt{x}$ y x.

Este simple ejercicio es conocido como la criba de Eratóstenes.

Desde un punto de vista más general, el método de la criba trata de contar el número de términos de una sucesión no divisibles por ningún primo perteneciente a un conjunto determinado de ellos.

Dada una sucesión A de enteros positivos, y una sucesión B de primos; por $S(A; B, z)$ designaremos al número de elementos de la sucesión A no divisibles por ningún primo $p \in B, \ p \leq z$.

Si definimos

$$P(z) = \prod_{p<z, \ p\in B} p,$$

tenemos que

$$S(A; B, z) = \#\{a : \ a \in A, \ (a, P(z)) = 1\}.$$

Recordemos la función μ de Möbius y una de sus propiedades

$$\mu(n) = \begin{cases} 1 \text{ si } n = 1 \\ (-1)^k, \ n = p_1 \cdots p_k \\ 0 \text{ si } p^2 \mid n \text{ para algún } n \end{cases}$$

Ahora podemos escribir

$$S(A;B,z)=\sum_{\substack{a\in A\\(a,P(z))=1}}1=\sum_{a\in A}\sum_{d|(a,P(z))}\mu(d)=\sum_{d|P(z)}\mu(d)\sum_{a\in A,\ d|a}1.$$

Si definimos $A_d=\{a\in A:\ a\equiv 0 \pmod d\}$ entonces

$$S(A;B,z)=\sum_{d|P(z)}\mu(d)|A_d|.$$

Veamos algunos ejemplos:

Ejemplo 1. Si $A=\{n\le x\}$, $B=\{p:\ p \text{ primo}\}$ y $z=\sqrt{x}$ nos encontramos ante el ejemplo más sencillo de la criba de Eratóstenes

$$S(A;B,\sqrt{x})=\pi(x)-\pi(\sqrt{x})+1.$$

Hemos de añadir el 1, que no es divisible por ningún primo menor que $\sqrt{x}$ pero que tampoco es primo.

Observando que, en este caso, $|A_d|=\left[\frac{x}{d}\right]$ obtenemos la denominada fórmula de Legendre.

$$\pi(x)-\pi(\sqrt{x})+1=\sum_{d|P(\sqrt{x})}\mu(d)\Big[\frac{x}{d}\Big].$$

Ejemplo 2. Consideremos ahora la sucesión $A=\{(2n-1)(2n+1):\ n<x/2\}$, $B=\{p:\ p>2\}$ y $z=\sqrt{x}$. Si $(2n-1)(2n+1)$ no es divisible por ningún primo menor que $\sqrt{x}$, entonces $2n-1$ y $2n+1$ son primos simultáneamente y nos encontramos ante una pareja de primos gemelos.

$$S(A;B,\sqrt{x})=\#\{p:\ \sqrt{x}<p<x,\ p+2 \text{ primo}\}.$$

Es decir, $S(A;B,\sqrt{x})=\pi_2(x)+O(x^{1/2})$, donde $\pi_2(x)$ cuenta el número de primos gemelos menores que x.

La conjetura sobre la existencia d infinitos primos gemelos es una de las más famosas en la Teoría de los Números. En esta sección demostraremos un teorema debido a Viggo Burn: *La suma de los inversos de los primos gemelos es convergente.*

Ejemplo 3. Dado un número positivo par N, consideremos la sucesión $A=\{n(N-n):\ n<N\}$, $B=\{p>2\}$ y $z=\sqrt{N}$. Por las mismas razones que en

el ejemplo anterior, si $n(N-n)$ no es divisible por ningún primo menor que $\sqrt{N}$, entonces n y $N-n$ son primos y su suma es N. Es decir,

$$S(A,B,\sqrt{N}) = \#\{N = p+q : \ p,q > \sqrt{N}, \ p,q, \ \text{primos}\} = r(N) + O(N^{1/2}),$$

donde $r(N)$ es el número de representaciones de N como suma de dos primos.

Después de estas primeras dosis de optimismo que pueden dar la impresión de que el método de la criba lo soluciona casi todo, nos enfrentaremos a los numerosos inconveninetes que tiene el ponerlos en práctica.

Recordemos la fórmula

$$S(A;B,z) = \sum_{d|P(z)} \mu(d)|A_d|.$$

Si el cardinal de A es A, intentaremos aproximar $|A_d|$ por $\frac{\omega(d)}{d}|X|$ de tal manera que ω sea una función multiplicativa y que $r_d = |A_d| - \frac{\omega(d)}{d}X$ sea lo más pequeño posible.

Si ahora sustituimos en la fórmula anterior obtenemos

$$\begin{aligned} S(A,B,z) &= X \sum_{d|P(z)} \frac{\mu(d)\omega(d)}{d} + \sum_{d|P(z)} \mu(d) r_d \\ &= X \prod_{\substack{p<z,\\ p\in B}} \Big(1 - \frac{\omega(p)}{p}\Big) + \sum_{d|P(z)} \mu(d) r_d. \end{aligned}$$

El término principal es relativamente fácil de estimar utilizando las fórmulas de Mertens. Sin embargo, el término de error tiene demasiados sumandos y la cancelación que pudiera haber es casi imposible de aprovechar.

Interesa, entre otras cosas, que z sea lo más pequeña posible. Observemos que si $z_2 \le z_1$ entonces $S(A;B,z_1) \le S(A;B.z_2)$. Por ello es mucho más fácil conseguir cotas superiores que inferiores.

Necesitaremos el lema siguiente, una consecuencia inmediata de las fórmulas de Mertens.

Lema 1.1.1. *Para todo entero $k \neq 0$ tenemos la estimación*

$$\prod_{k<p<x} \Big(1 - \frac{k}{p}\Big) \ll \frac{1}{(\log x)^k}. \tag{1.1}$$

Demostración. Tomando logaritmos tenemos

$$\log\Big(\prod_{k<p<x} \Big(1-\frac{k}{p}\Big)\Big) = -\sum_{k<p<x} \frac{k}{p} + O\Big(\sum_{k<p<x} \frac{k^2}{p^2}\Big) = -k\log\log x + O(k) \tag{1.2}$$

por la fórmula de Mertens. □

Este primer teorema nos familiarizará con la notación y nos dará una cota superior no trivial de los primos menores que x.

Teorema 1.1.2.

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

Demostración. Si $A = \{n : \ n \leq x\}$ y $B = \{p\}$ entonces $S(A; B, \sqrt{x}) = \pi(x) + O(\sqrt{x})$, como vimos anteriormente.

También, si $z \leq \sqrt{x}$ tenemos que $S(A; B, z) \leq S(A; B, \sqrt{x}$. Aproximamos A_d por $|A_d| = \left[\frac{x}{d}\right] = \frac{x}{d} - \frac{x}{d}$. Entonces $\omega(d) = 1$ para todo d y $r_d = -\{x/d\}$. Luego,

$$S(A; B, z) \leq x \prod_{p<z}\Big(1 - \frac{1}{p}\Big) + \sum_{d|P(z)} 1.$$

Haciendo $k = 1$ en el lemma 1.1.1 tenemos que

$$\prod_{p<z}\Big(1 - \frac{1}{p}\Big) \ll \frac{1}{\log z}.$$

Por otra parte el número de divisores de $P(z)$ es $2^{\pi(z)} \ll 2^z$. Luego,

$$\pi(x) \ll \frac{x}{\log z} + 2^z + x^{1/2}.$$

Eligiendo $z = \log x$ obtenemos $\pi(x) \ll \frac{x}{\log\log x}$. □

Este teorema es mucho menos preciso que el teorema del número primo e incluso que el teorema de Chebychev. Esto es debido a que el z elegido es mucho más pequeño que $\sqrt{x}$.

Los diferentes métodos de criba consisten en acotar $\sum_{d|P(z)}$ por otro tipo de funciones que hagan más pequeño el término del error y permitan elegir z más grande.

1.1.1. Criba de Viggo Brun

Lema 1.1.3.

$$\sum_{\substack{d|n \\ \nu(d)\leq 2k+1}} \leq \sum_{d|n} \mu(d) \leq \sum_{\substack{d|n \\ \nu(d)\leq 2k}} \mu(d). \tag{1.3}$$

Demostración. Si $n = 1$, las tres sumas son iguales. Sea $\nu(n) = v$. Entonces

$$\sum_{\substack{d|n \\ \nu(d)=m}} \mu(d) = (-1)^m \binom{v}{m}.$$

Si definimos

$$\sigma_k(n) = \sum_{\substack{d|n \\ \nu(d)\leq k-1}} \mu(d) = \sum_{m=0}^{k-1} (-1)^m \binom{v}{m},$$

demostraremos que $\sigma_k(n) = (-1)^{k-1}\binom{v-1}{k-1}$ y por lo tanto el lema.

Lo haremos por inducción sobre k. Para $k = 1$ es obvio. Aplicando la hipótesis de inducción tenemos

$$\begin{aligned}\sigma_{k+1}(n) &= (-1)^k \binom{v}{k} + \sigma_k(n) = (-1)^k \binom{v}{k} + (-1)^{k-1} \binom{v-1}{k-1} \\ &= (-1)^k \left\{ \binom{v}{k} - \binom{v-1}{k-1} \right\} = (-1)^k \binom{v-1}{m}\end{aligned}$$

□

En el siguiente teorema veremos cómo se utiliza la criba de Brun en el problema de los primos gemelos.

Teorema 1.1.4. *La suma de los inversos de los primos gemelos es convergente.*

Demostración. Lo que demostraremos es que

$$\pi_2(x) \ll \frac{x}{\log^2 x} (\log\log x)^2.$$

Después de esto la suma la podemos estimar de la manera siguiente:

$$\begin{aligned}\sum_{p,\ p+2 \text{ primos}} \frac{1}{p} &\ll \sum_{k=0}^{\infty} \sum_{\substack{2^k < p \leq 2^{k+1} \\ p, p+2 \text{ primos}}} \frac{1}{p} \ll \sum_{k=0}^{\infty} \frac{1}{2^k} \pi_2(2^{k+1}) \\ &\ll \sum_{k=0}^{\infty} \frac{1}{2^k} \frac{2^{k+1} \log^2(k+1)}{(k+1)^2} \ll \sum_{k=1}^{\infty} \frac{\log^2 k}{k^2} < +\infty.\end{aligned}$$

Sea $A = \{(2n-1)(2n+1) : \ n \leq x/2\}$, $B = \{p : \ p > 2\}$. Según hemos visto antes, $S(A; B, \sqrt{x}) = \pi_2(x) + O(\sqrt{x})$. Luego si $z \leq \sqrt{x}$, tenemos $\pi_2(x) \ll S(A; B, z) + O(\sqrt{x})$.

Por otra parte, utilizando el teorema anterior, podemos escribir

$$S(A;B,z) = \sum_{\substack{a\in A\\(a,P(z))=1}} 1 = \sum_{a\in A}\sum_{d|(a,P(z))}\mu(d) \le \sum_{a\in A}\sum_{\substack{d|(a,P(z)\\ \nu(d)\le 2k}}\mu(d)$$
$$= \sum_{\substack{d|P(z)\\ \nu(d)\le 2k}}\mu(d)\sum_{\substack{a\in A\\ d|a}} 1 = \sum_{\substack{d|P(z)\\ \nu(d)\le 2k}}\mu(d)|A_d|,$$

para un k que elegiremos más adelante.

La cantidad $|A_d|$ es el número de enteros $n \le x/2$ que satisfacen la congruencia $(2n-1)(2n+1) \equiv 0 \pmod d$. Como $\mu(d) \neq 0$ y d es impar tenemos que

$$|A_d| = \sum_{d_1d_2=n} \#\{n:\ n\le x/2,\ 2n-1\equiv 0 \pmod{d_1},\ 2n+1\equiv 0 \pmod{d_2}\}$$
$$= \sum_{d_1d_2=d}\Big\{\frac{x}{2d}+O(1)\Big\} = \frac{\tau(d)}{2d}+O(\tau(d)),$$

donde $\tau(d)$ = número de divisores de d.

Sustituyendo arriba tenemos

$$S(A;B,z) \le \frac{x}{2}\sum_{\substack{d|P(z)\\ \nu(d)\le 2k}}\frac{\mu(d)\tau(d)}{d} + O\Big(\sum_{\substack{d|P(z)\\ \nu(d)\le 2k}}\tau(d)\Big).$$

El término de error se puede calcular de la siguiente manera. Si $\nu(d) = r$ entonces $\tau(d) = 2^r$ y

$$\sum_{\substack{d|P(z)\\ \nu(d)\le 2k}}\tau(d) = \sum_{r=0}^{2k} 2^r\binom{\pi(z)}{r} \le \sum_{r=0}^{2k}2^r\frac{\pi^r(z)}{r!} \le \pi^{2k}(z)2^2.$$

Por otra parte, la suma del término principal la podemos escribir

$$\sum_{\substack{d|P(z)\\ \nu(d)\le 2k}}\frac{\mu(d)\tau(d)}{d} = \sum_{d|P(z)}\frac{\mu(d)\tau(d)}{d} - \sum_{\substack{d|P(z)\\ \nu(d)\ge 2k+1}}\frac{\mu(d)\tau(d)}{d}$$
$$= \prod_{2<p<z}\Big(1-\frac{2}{p}\Big) - \sum_{\substack{d|P(z)\\ \nu(d)\ge 2k+1}}\frac{\mu(d)\tau(d)}{d}.$$

Para estimar la última suma utilizaremos la siguiente desigualdad:

$$\Big|\sum_{\substack{d|P(z)\\ \nu(d)=r}} \frac{\mu(d)\tau(d)}{d}\Big| \le 2^r \sum_{\substack{d|P(z)\\ \nu(d)=r}} \frac{1}{d} \le 2^r \frac{\Big(\sum_{2<p<z} \frac{1}{p}\Big)^r}{r!}.$$

Por las fórmulas de Mertens sabemos que $\sum_{2<p<z} \frac{1}{p} \le \log\log x + C$ para una constante universal C. Entonces

$$\Big|\sum_{\substack{d|P(z)\\ \nu(d)\ge 2k+1}} \frac{\mu(d)\tau(d)}{d}\Big| \le \sum_{r=2k+1}^{\infty} \frac{(2\log\log z + 2C)^r}{r!}$$

$$\le \sum_{r=2k+1}^{\infty} \Big(\frac{2e\log\log z + 2eC}{r}\Big)^r.$$

Hemos utilizado la desigualdad $r! > (r/e)^r$, que se puede probar por inducción observando que $(1+1/n)^n < e$ para todo n.

Si elegimos $k = [4e\log\log z + 4eC] + 1$, la suma se puede mayorizar por

$$2^{-2k} \le \frac{1}{(\log z)^{8e\log 2}} \le \frac{1}{(\log z)^8}.$$

Sustituyendo obtenemos

$$\pi_2(x) \le \frac{x}{2} \prod_{2<p<z} \Big(1 - \frac{2}{p}\Big) + \frac{x}{\log^8 z} + \pi^{2k}(z) + O(x^{1/2}).$$

Si ahora tomamos $z = x^{1/(4k)}$ y utilizamos las estimaciones

$$\pi(x) \ll \frac{x}{\log x} \text{ y } \prod_{2<p<z} \Big(1 - \frac{2}{p}\Big) \ll \frac{1}{\log^2 z}$$

obtenemos

$$\pi_2(x) \ll \frac{x}{\log^2 x}(\log\log x)^2.$$

□

1.2. Conjuntos de Sidon

1.2.1. 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

$$x = a + a', \quad a, a' \in A \tag{1.4}$$

$$x = a - a', \quad a, a' \in A \tag{1.5}$$

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 $x = a + b,\ a \in A,\ b \in B$. Observemos que

$$\sum_x r_{A+B}(x) = |A||B| \tag{1.6}$$

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

$$\sum_x r^2_{A+B}(x) = \sum_x r_{A-A}(x) r_{B-B}(x). \tag{1.7}$$

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 (1.6) y (1.7) 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

$$\sum_x r_A(x) = \sum_x d_A(x) = |A|^2 \tag{1.8}$$

$$\sum_x r^2_A(x) = \sum_x d^2_A(x). \tag{1.9}$$

1.2.2. Cotas superiores

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

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

de donde

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

Teorema 1.2.1. *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 (1.6), (1.7) 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 una sección posterior veremos que el término $N^{1/2}$ en esta cota superior es óptimo.

1.2.3. 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 ingeniosa 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. Con esta observación comprobaremos que el conjunto

$$\mathcal{A} = \left\{ a_p = \left\lfloor \frac{2n}{\log n} \log p \right\rfloor,\ p \leq \sqrt{\frac{n}{2\log n}},\ p \text{ primo} \right\}$$

es un conjunto de Sidon $\mathcal{A} \subset \{1, \ldots, n\}$, que tendrá tantos elementos como primos haya menores que $\sqrt{\frac{n}{2\log n}}$.

Supongamos que $a_p + a_q = a_r + a_s,\ \{p, q\} \neq \{r, s\}$. Entonces podemos escribir

$$\frac{2n\left(\log p + \log q - \log r - \log s\right)}{\log n}$$
$$= \left\{\tfrac{2n\log r}{\log n}\right\} + \left\{\tfrac{2n\log s}{\log n}\right\} - \left\{\tfrac{2n\log p}{\log n}\right\} - \left\{\tfrac{2n\log q}{\log n}\right\},$$

donde $\{x\}$ indica la parte fraccionaria de x. Como $|\{x\} + \{y\} - \{z\} - \{v\}| \leq 2$ para cualesquiera números reales x, y, z, v tenemos que

$$\left|\log\left(\frac{pq}{rs}\right)\right| \leq \frac{\log n}{n}.$$

Pero por otro lado tenemos (supongamos que $pq > rs$)

$$\log\left(\frac{pq}{rs}\right) = \log\left(1 + \frac{pq - rs}{rs}\right) \geq \log\left(1 + \frac{1}{rs}\right) \geq \frac{1}{2rs} > \frac{\log n}{n},$$

obteniendo así una contradicción.

El teorema del número primo, $|\{p \leq x,\ p \text{ primo }\}| \sim x/\log x$, nos permite ver que $\mathcal{A}$ es un conjunto de Sidon con $\sim n^{1/2}/(\sqrt{2}\log^{3/2} n)$ elementos.[1]

[1] Ruzsa explotó esta idea para construir la sucesión infinita de Sidon más densa que se conoce hoy en día.

1.2.4. Conjuntos de Sidon en grupos

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

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

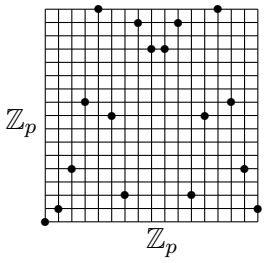
Ejemplo 1.2.3. *A Golomb se debe el conjunto de Sidon de $p-2$ elementos*

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

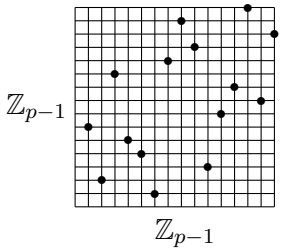
Ejemplo 1.2.4. *Welch descubrió el conjunto de Sidon de $p-1$ elementos*

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

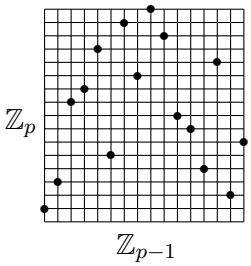
Dejamos como ejercicio comprobar que los tres conjuntos de los ejemplos anteriores son de Sidon.



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

$$\mathcal{A} = \{(p-1)(x - g^x)_p + x,\ 1 \le x \le p-1\} \subset \mathbb{Z}_{p(p-1)}, \tag{1.10}$$

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.

1.3. Aplicaciones de los conjuntos de Sidon

Los conjuntos de Sidon más interesantes son aquellos que $|\mathcal{A}| = \sqrt{|G|} - \delta$ con δ pequeño. El siguiente teorema va a tener muchas aplicaciones.

Teorema 1.3.1. *Sea $\mathcal{A}$ un conjunto de Sidon en un grupo G con $|\mathcal{A}| = \sqrt{|G|} - \delta$. Entonces, para todo $B, B' \subset G$ tenemos*

$$\#\{(b,b') \in B \times B',\ b+b' \in \mathcal{A}\} = \frac{|\mathcal{A}|}{|G|}|B||B'| + \theta(|B||B'|)^{1/2}|G|^{1/4}, \tag{1.11}$$

con $|\theta| \leq \left(1 + 2\frac{\max\{0,\delta\}|B|}{|G|}\right)^{1/2}$.

Demostración. Empezaremos demostrando la siguiente desigualdad:

$$\sum_{x\in G}\left(r_{\mathcal{A}-B}(e) - \frac{|\mathcal{A}||B|}{|G|}\right)^2 \leq |B|(|\mathcal{A}|-1) + |B|^2\frac{|G|-|\mathcal{A}|^2}{|G|}. \tag{1.12}$$

Para hacerlo utilizamos las igualdades (1.6) y (1.7)) y obtenemos

$$\sum_{x\in G}\left(r_{\mathcal{A}-B}(e) - \frac{|\mathcal{A}||B|}{|G|}\right)^2 = \sum_{x\in G} r_{B-B}(e)r_{\mathcal{A}-\mathcal{A}}(e) - \frac{|\mathcal{A}|^2|B|^2}{|G|}. \tag{1.13}$$

Como $\mathcal{A}$ es un conjunto de Sidon entonces

$$\begin{aligned}\sum_{x\in G} r_{B-B}(x)r_{\mathcal{A}-\mathcal{A}}(x) &= |\mathcal{A}||B| + \sum_{x\neq 0} r_{B-B}(x)r_{\mathcal{A}-\mathcal{A}}(x) \\ &\leq |\mathcal{A}||B| + \sum_{x\neq 0} r_{B-B}(x) = |\mathcal{A}||B| + |B|^2 - |B|.\end{aligned} \tag{1.14}$$

La desigualdad (1.12) se sigue de (1.13) y (1.14).

Asumimos que $|B| \leq |B'|$ y observemos que

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

Ahora aplicamos la desigualdad de Cauchy, la desigualdad 1.12 y la hipótesis $|\mathcal{A}| = |G|^{1/2} - \delta$.

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

□

En los tres ejemplos de conjuntos de Sidon en grupos finitos que hemos visto, todos ellos satisfacen $\delta \leq 1$.

Corolario 1.3.2. *Si $\mathcal{A} \subset G$ es un conjunto de Sidon con $|\mathcal{A}| = \sqrt{|G|} - \delta$ y $B \subset G$ es un subgrupo, entonces*

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

donde $|\theta| \leq \left(1 + 2\frac{\text{máx}(0,\delta)|B|}{|G|}\right)^{1/2}$.

Demostración. Observemos que cada elemento de $\mathcal{A} \cap B$ se puede escribir como $b + b',\ b, b' \in B$ de exactamente $|B|$ maneras. Así que

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

y después aplicamos el teorema 1.3.1. □

Como veremos, la estrategia consiste en elegir el conjunto de Sidon $\mathcal{A}$ y los conjuntos B y B' según el problema.

1.3.1. Ecuaciones en $\mathbf{F}_q$

Empezamos con un ejemplo sencillo.

Teorema 1.3.3. *Sean $A_1, A_2, A_3, A_4 \subset \mathbf{F}_q$ y sea $T = |A_1||A_2||A_3||A_4|$. Entonces, el número de soluciones de la ecuación $x_1 + x_2 = (x_3 + x_4)^2$ en $\mathbf{F}_q$ es*

$$S = \frac{T}{q} + \theta\sqrt{qT}, \qquad |\theta| \leq 1. \tag{1.15}$$

Demostración. Consideramos el conjunto de Sidon $\mathcal{A} = \{(x, x^2) :\ x \in \mathbf{F}_q\}$ y los conjuntos $B = A_2 \times A_4$ y $B' = A_1 \times A_3$. Observemos que $S = |\{(b, b') \in B \times B' : b + b' \in \mathcal{A}\}$ y aplicamos el teorema 1.3.1. □

Teorema 1.3.4. *Sean $X_1, X_2, X_3, X_4 \subset \mathbf{F}_q^*$ y sea $T = |X_1||X_2||X_3||X_4|$. Para todo $\lambda \neq 0$ escribimos S_λ para el número de soluciones de $x_1x_2 - x_3x_4 = \lambda$. Entonces tenemos que*

$$S_\lambda = \frac{T}{q} + \theta\sqrt{Tq}, \quad |\theta| \leq 1 + o(1).$$

Demostración. Consideramos el conjunto de Sidon $\mathcal{A} = \{(\log x, \log(x-\lambda) : \ x \neq 0, \lambda\}$ y $B = \log X_1 \times \log X_3$, $B' = \log X_2 \times \log X_4$. Es claro que $S_\lambda = \{(b, b') \in B \times B' : \ b + b' \in \mathcal{A}\}$. Y ahora aplicamos el teorema 1.3.1. □

En particular, si $|X_1||X_2||X_3||X_4| \gg p^3$ ambas congruencias tiene solución.

Teorema 1.3.5. *Sean $X_1, X_2 \subset \mathbf{F}_q^*$ y $X_3, X_4 \subset \mathbf{F}_q$ y pongamos $T = |X_1||X_2||X_3||X_4|$. Para todo λ escribimos S_λ para el número de soluciones de $x_1x_2 + x_3 + x_4 = \lambda$. Entonces tenemos,*

$$S_\lambda = \frac{T}{q} + \theta\sqrt{Tq}, \ |\theta| \leq 1 + o(1).$$

Demostración. Consideramos el conjunto de sidon $\mathcal{A} = \{(x, g^x - \lambda)\}$ y los conjuntos $B = X_1 \times \log X_3$ y $B' = X_2 \times \log X_4$. □

1.3.2. Estimaciones suma-producto en $\mathbf{F}_q$

Garaev demostró el siguiente resultado utilizando sumas trigonométricas. Aquí lo haremos de una manera más sencilla como corolario del teorema (1.3.1).

Teorema 1.3.6. *Sean $A_1, A_2 \subset \mathbf{F}_q^*$ y $A_3 \subset \mathbf{F}_q$. Entonces*

$$|A_1A_2||A_1 + A_3| \gg \text{mín}\left(|A_1|q, \frac{|A_1|^2|A_2||A_3|}{q}\right)$$

Demostración. Consideremos el conjunto de Sidon $\mathcal{A} = \{(x, \log x) : \ x \neq 0\}$ y los conjuntos $B = \ (A_1 + A_2, \log A_1 + \log A_3)$ and $B' = (-A_2, -\log A_3)$.

Hay $|A_1||A_2||A_3|$ pares $(b, b') \in B \times B'$ de la forma

$$(b, b') = ((a_1 + a_2, \log a_1 + \log a_3), (-a_2, -\log a_3)), \ a_i \in A_i.$$

Todos ellos son distintos y $b + b' = (a_1, \log a_1) \in \mathcal{A}$. Entonces

$$\#\{(b, b') \in B \times B', \ b + b' \in \mathcal{A}\} \geq |A_1||A_2||A_3|.$$

ahora aplicamos el teorema 1.3.1 y obtenemos

$$|A_1||A_2||A_3| \leq \frac{|A_1 + A_2||A_1A_3||A_2||A_3|}{q} + O\left(\sqrt{|A_1 + A_2||A_1A_3||A_2||A_3|q}\right),$$

que implica la desigualdad del teorema. □

1.3.3. 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 1.3.7 (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

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

El término $o(1)$ refleja una cantidad que tiende a cero cuando n tiende a infinito.

1.4. 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 1.4.1 (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 1.8.7 y 1.8.9.

1.5. 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 1.5.1. *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 1.5.2 (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

$$E(A) \geq \frac{|A|^4}{|AA|}. \tag{1.16}$$

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

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

Existe entonces un j y un m tales que

$$m = \#\{l_\lambda :\ 2^{j-1} < |l_\lambda\cap(A\times A)| \leq 2^j\} \geq 2^{-2j}\frac{E(A)}{\log_2|A|}. \tag{1.17}$$

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

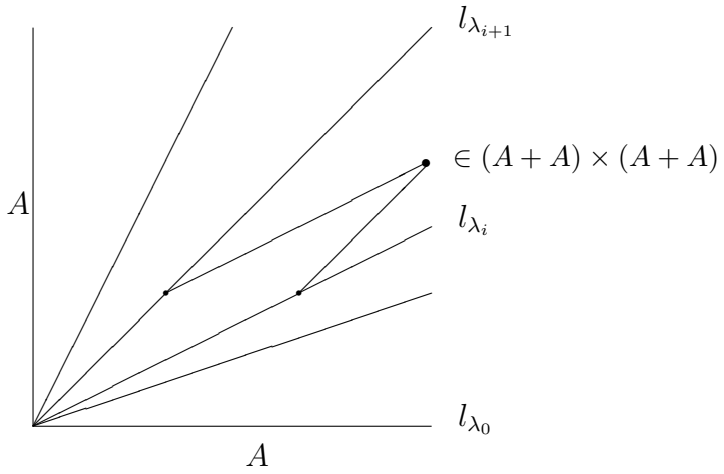
$$|A+A|^2 \geq \left|\bigcup_{i=0}^{m-1} (l_{\lambda_i}\cap(A\times A)) + \big(l_{\lambda_{i+1}}\cap(A\times A)\big)\right| \tag{1.18}$$

$$= \sum_{i=0}^{m-1} |l_{\lambda_i}\cap(A\times A)||l_{\lambda_{i+1}}\cap(A\times A)| \geq m2^{2j-2}. \tag{1.19}$$

De (1.17) y (1.18) obtenemos

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

que junto con (1.16) 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 $|AA| < \frac{|A|^{4/3}}{(\log |A|)^{1/3}}$. □

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

Teorema 1.5.3. *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 **??** 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. □

1.6. 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 1.6.1. *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. □

1.7. 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 1.7.1. *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. □

1.8. Ejercicios de este capítulo

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

1.8.2. *Demostrar que si A es un conjunto g-Sidon en un grupo abeliano de orden N entonces*

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

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

1.8.4. *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* $A = \{[p\phi_p],\ p \equiv 1 \pmod 4,\ p \leq N\}$ *es un comjunto de Sidon en* $\{1, \dots, N\}$ *con* $\gg N^{1/2}/\log N$ *elementos.*

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

1.8.6. *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'.

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

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

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

$$r'_A(n) = \#\{(a, a') :\ a + 2a' = n,\ a, a' \in A\}$$

hallando una sucesión A *de números no negativos tal que* $r'_A(n) = 1$ *para todo* $n \geq 0$.

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

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

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

1.8.13. *Sean* $A_1, A_2 \subset \mathbf{F}_q^*$ *y* $A_3 \subset \mathbf{F}_q$. *Demostrar que*

$$|A_1 A_2||(A_1 + 1)A_3| \gg \text{mín}(|A_1|q, \frac{|A_1|^2|A_2||A_3|}{q}).$$

1.8.14. *Demostrar que si* $p > 2n^4$ *entonces la ecuación de Fermat en* $\mathbf{F}_q$, $x^n + y^n = z^n$ *tiene soluciones no triviales.*

1.8.15. *Sea* g *una raíz primitiva. Demostrar que para todo* $x \in \mathbb{Z}_p$ *se tiene que* $x \equiv g^y - g^z \pmod p$ *para algunos* $0 \leq y, z \leq 2p^{3/4}$.