Revista Bases de la Ciencia - ISSN 2588-0764

Publicación Cuatrimestral. Vol. 4, No. 3, Septiembre/Diciembre, 2019, Ecuador (p.19-40). Edición continua

SOBRE SUCESIONES DE SIDON

Adrián Infante

Departamento de Matemáticas y Estadística, Instituto de Ciencias Básicas, Universidad Técnica de Manabí.
Autor para correspondencia: ainfante@utm.edu.ec

Recibido: 15-4-2019 / Aceptado: 14-10-2019 / Publicación: 31-12-2019

Editor Académico: Dra. Carmen Judith Vanegas

RESUMEN

Estudiamos los subconjuntos de números reales con la propiedad de que todas las sumas de dos elementos son distintos, es decir que si $a_i + a_j = a_{i'} + a_{j'}$ entonces se verifica la igualdad $\{a_i, a_j\} = \{a_{i'}, a_{j'}\}$. A estos conjuntos los llamaremos conjuntos de Sidon. El problema es saber cuál es el mayor número de elementos que puede tener un conjunto de Sidon en el intervalo $[1, N]$. Presentamos ejemplos que evidencian la necesidad de conocer el tamaño del intervalo $[1, N]$ donde se va a ubicar el conjunto de Sidon para saber el tamaño $F(N)$ del conjunto de Sidon. Ruzsa I. Z. (1998) demostró la existencia de una sucesión infinita de Sidon tal que su tamaño $B(N) > N^{\sqrt{2}-1+o(1)}$. En este trabajo rehacemos detalladamente la demostración de Ruzsa, introduciendo en la prueba una modificación sustancial, al sustituir las sucesiones $\{\log p\}_{p,\, primo}$ por la sucesión de los argumentos de los enteros de Gauss $a + ib = p$ con $a < b$, a y b enteros y p primo.

Palabras clave: Conjuntos de Sidon, suma de dos elementos.

ON INFINITE SUCCESSION OF SIDON

ABSTRACT

We study the sub-sets of real number with the property that all sums of two elements is different, namely $a_i + a_j = a_{i'} + a_{j'}$ then the equation $\{a_i, a_j\} = \{a_{i'}, a_{j'}\}$ is verified. We will call these sets Sidon sets. The problem is knowing the maximum number of elements that a Sidon set can contain in the interval $[1, N]$. We present examples that show the need of knowing the size of the interval $[1, N]$ where the Sidon set will be located to know the size $F(N)$ of the Sidon set. Ruzsa I. Z. (1998) proved the existence of an infinite Sidon succession such that its size $B(N) > N^{\sqrt{2}-1+o(1)}$. In this paper, we rewrite Ruzsa proof in detail, introducing a susstantial modification in the proof, by substituting the successions $\{\log p\}_{p,\, primo}$ for the succession of the arguments of Gauss integers $a + ib = p$ with $a < b$, and integers, and prime.

Keywords: Sets of Sidon, Sums of two elements.

SOBRE SUCESSÕES INFINITAS DE SIDON

RESUMO

Estudamos os subconjuntos de números reais com a propriedade que todas as somas de dois elementos são diferentes, ou seja, se $a_i + a_j = a_{i'} + a_{j'}$, então a igualdade $\{a_i . a_j\} = \{a_{i'}, a_{j'}\}$. Nós chamamos esses conjuntos de conjuntos Sidon. O problema é saber qual é o maior número de elementos que pode ter um conjunto de Sidon no intervalo. Apresentamos exemplos que mostram a necessidade de saber o tamanho do intervalo $[1, N]$ onde o conjunto Sidon estará localizado, para saber o tamanho $F(N)$ do conjunto Sidon. Ruzsa I.Z. (1998) demonstrou a capacidade de uma sucessão infinita de Sidon de tal forma que seu tamanho $B(N) > N^{\sqrt{2}-1+o(1)}$. Neste artigo apresentamos uma explicação detalhada da demonstração de Ruzsa, introduzindo uma modificação substancial na prova, substituindo as consequência $\{\log p\}_{p,\, primo}$ pela sequência de argumentos dos inteiros Gauss $a + ib = p$ com $a < b$, a e b inteiros e p primo.
Palavras chave: Conjuntos de Sidon, somas de dois elementos são diferentes.

Citación sugerida: Adrián Infante . SOBRE SUCESIONES DE SIDON. Revista Bases de la Ciencia, 4(3), 19-40. DOI:https://doi.org/10.33936/rev_bas_de_la_ciencia.v4i3.1726

Recuperado de: https://revistas.utm.edu.ec/index.php/Basedelaciencia/article/view/1726

OrcidIDs:

Adrián Infante:http://orcid.org/0000-000-2385-77063
Carmen Judith Vanegas:http://orcid.org/0000-003-0748-5963

1. INTRODUCCIÓN

En la teoría de números ha tenido especial atención el estudio de las propiedades aditivas de los números enteros. Dentro de la amplia Teoría Aditiva destacamos aquella parte que estudia los conjuntos de números reales con la propiedad de que todas las sumas de dos elementos son distintas. Varios problemas relacionados con este tipo de conjuntos surgen en conexión con los trabajos de investigación en la teoría de Series de Fourier, como se puede ver en los trabajos de **Sidon S. (1932)**. Esta conexión se puede ilustrar de manera sencilla: sea $\mathcal{A} = \{a_k\}_k$ una sucesión de números enteros y tales que $r_{\mathcal{A}}(n) \leq g$, donde $r_{\mathcal{A}}(n)$ es el número de representaciones de n como suma de dos elementos de $\mathcal{A}$, sin repetición, es decir,

$$r_{\mathcal{A}}(n) = \#\{a_i, a_j \in \mathcal{A} : \ n = a_i + a_j, \ \ a_i \leq a_j\}.$$

Para un número real positivo p, definimos la norma p de una función $f : \mathbb{R} \to \mathbb{R}$ periódica y de período 2π por:

$$\| \ f \ \|_p = \left(\int_0^{2\pi} |f(x)| \ dx \right)^{1/p}.$$

Un simple cálculo nos permite observar que las normas 4 de funciones con frecuencia en $\mathcal{A}$, están acotadas por las normas 2. Sea

$$f(t) = \sum_{k=0}^{\infty} c_k e^{ia_k t}$$

donde $\mathcal{A} = \{a_k\}_k$ es una sucesión de números enteros y tales que $r_{\mathcal{A}}(n) \leq g$, y los C_k, $k = 0, \ 1, \ 2, \ldots$ son los coeficientes de Fourier de f. Entonces

$$\begin{aligned}
\|f\|_4^4 &= \frac{1}{2\pi} \int_0^{2\pi} |f(t)|^4 \ dt = \frac{1}{2\pi} \int_0^{2\pi} \left| f^2(t) \right|^2 \ dt \\
&= \frac{1}{2\pi} \int_0^{2\pi} \left| \left(\sum_{k,j} c_k c_j \right) e^{i(a_k + a_j)t} \right|^2 \ dt = \frac{1}{2\pi} \int_0^{2\pi} \left| \sum_{n=1}^{\infty} \sum_{\substack{k,j \\ a_k + a_j = n}} c_k c_j e^{int} \right|^2 \ dt \\
&= \sum_{n=1}^{\infty} \left| \sum_{\substack{k,j \\ a_k + a_j = n}} c_k c_j \right|^2 \leq 2g \sum_{n=1}^{\infty} \sum_{\substack{k,j \\ a_k + a_j = n}} |c_k|^2 \, |c_j|^2 \\
&\leq 2g \left(\sum_{k=1}^{\infty} |c_j|^2 \right)^2 \leq 2g \, \|f\|_2^4 .
\end{aligned}$$

En este trabajo sólo consideramos el caso en que el número de representaciones es única, es decir, si $a_i + a_j = a_{i'} + a_{j'}$ entonces se verifica la igualdad $\{a_i, a_j\} = \{a_{i'}, a_{j'}\}$. A estos conjuntos los llamaremos conjuntos de Sidon.

Sidon planteó a Erdös el siguiente problema: ¿Cúal es el máximo número de elementos que puede tener un conjunto de Sidon contenido en el intervalo $[1, N]$?

Si llamamos $F(N)$ a ese número, los siguientes ejemplos nos darán las primeras cotas inferiores.

Ejemplo 1. Las potencias de 2, cuyo crecimiento es exponencial, es el ejemplo más obvio de conjunto de Sidon. De hecho, cualquier sucesión lacunar, $B = \{b_1, b_2, b_3 \ldots\}$ con la condición $2b_{k-1} \leq b_k$, es de Sidon. De aquí obtenemos $F(N) \geq \log_2 N$.

El siguiente ejemplo nos da una mejor cota inferior.

Ejemplo 2. Vamos a construir una sucesión de Sidon, $b_1 < b_2 < \ldots$, tal que los b_n sean mucho menor que n^3, $b_n \ll n^3$. Empezado por $b_1 = 1$, $b_2 = 2$. Tomemos b_n como el menor entero positivo distinto de todos los números $b_i + b_j - b_k$, con $1 \leq i, j, k < n$. Veamos que esta construcción nos proporciona, $b_n < n^3$. Observemos que existen a lo más $(n-1)^3$ de estas tripletas i, j, k, por lo tanto los correspondientes números de enteros $b_i + b_j - b_k$ no puede superar a $(n-1)^3$. De modo que siempre podemos elegir $b_n \leq (n-1)^3 + 1 < n^3$. En este caso, tenemos $F(N) \geq N^{\frac{1}{3}}$.

Estas dos construcciones, que podemos considerar triviales, fueron superados por la siguiente construcción de Erdös.

Ejemplo 3. Sea p un primo y sea $B_p = \{b_k = 2kp + (k^2)_p : k = 1, 2, \ldots, p\}$, donde $(k^2)_p$ denota el entero positivo u, $1 \leq u \leq p$, determinado por $u \equiv k^2 \pmod{p}$. Spongamos que

$$2kp + (k^2)_p + 2pj + (j^2)_p = 2pk' + (k'^2)_p + 2pj' + (j'^2)_p$$

que podemos escribir como

$$(k^2)_p + (j^2)_p - (k'^2)_p - (j'^2)_p = 2p(k' + j' - k - j) \tag{1}$$

En particular tenemos que $k^2 + j^2 \equiv k'^2 + j'^2 \pmod p$, de donde

$$(k - k')(k + k') \equiv (j' - j)(j' + j) \qquad (\text{mod } p). \tag{2}$$

Por otra parte, como $1 \leq (k^2)_p \leq p$, se cumple que $-2p < (k^2)_p + (j^2)_p - (k'^2)_p - (j'^2)_p < 2p$, y en vista de (1) tenemos que $(k^2)_p + (j^2)_p - (k'^2)_p - (j'^2)_p = 0$, lo que implica que $k - k' = j' - j$. En el caso $j \neq j'$ en (2), como $k - k' = j' - j$, obtenemos $k + k' \equiv j + j' \pmod p$, que junto con $k + j \equiv k' + j' \pmod p$ implica $k' = j$. En el otro caso, $j = j'$ implica que $k = k'$. Es decir en cualquier caso, $\{k, j\} = \{k', j'\}$.

Hemos demostrado que B_p es un conjunto de Sidon con p elementos contenidos en el intervalo $[1,\ 2p + 1]$, esto quiere decir que $F(2p^2 + 1) \geq p$. Por otra parte, sabemos que para todo N existe un primo p tal que $N - o(N) < 2p^2 + 1 \leq N$, donde $o(N)$ denota una constante que depende de N y tal que $\lim_{N\to\infty} \frac{o(N)}{N} = 0$. Así que $F(N) \geq F(2p^2 + 1) \geq p \geq \sqrt{\frac{N}{2}} - o(\sqrt{N})$.

Con un argumento más elaborado, **Bose R.C. and Chowla S.(1962)** demostraron que

$$F(N) \geq \sqrt{N} + o(\sqrt{N}). \tag{3}$$

Reproducimos aquí una construcción más sencilla que dio I. Ruzsa.

Ejemplo 4. Para un número natural p, decimos que g es una raíz primitiva módulo p, si g genera como grupo a $\mathbb{Z}_p^*$, es decir, si para cada $b \in \mathbb{Z}_p^*$ existe $k \in \mathbb{Z}$ tal que $g^k \equiv b(\text{mod } p)$. Aquí $\mathbb{Z}_p^*$ denota los elementos invertibles módulo p.
Dado un número primo p, sea g una raíz primitiva de p. Considere el sistema de congruencias

$$\begin{cases} x \equiv k \qquad (\text{mod}(p-1)), \qquad k = 1, 2, \ldots, p-1. \\ x \equiv g^k \qquad\quad (\text{mod } p) \end{cases} \tag{4}$$

Por el teorema Chino del resto tenemos $p-1$ soluciones en $[1, p(p-1)]$. Vamos a ver que este conjunto de soluciones es un conjunto de Sidon.

Supongamos que $x_i \equiv i$, $x_j \equiv j$, $x_{i'} \equiv i'$ y $x_{j'} \equiv j' \pmod{p-1}$ tales que $x_i + x_j = x_{i'} + x_{j'}$. En

particular, $x_i + x_j \equiv x_{i'} + x_{j'} \pmod{p(p-1)}$, de donde

$$\begin{cases} x_i + x_j \equiv x_{i'} + x_{j'} \pmod{(p-1)} \\ x_i + x_j \equiv x_{i'} + x_{j'} \pmod{p} \end{cases}$$

Entonces, en vista de (4), tenemos $i + j \equiv i' + j' \pmod{(p-1)}$ y $g^i + g^j \equiv g^{i'} + g^{j'} \pmod{p}$.

Consideremos el polinomio $P(x) = (x - g^i)(x - g^j) = x^2 - x(g^i + g^j) + g^{i+j}$. Usando las congruencias anteriores tenemos que

$$P(x) \equiv x^2 - x(g^{i'} + g^{j'}) + g^{i'+j'} \equiv (x - g^{i'})(x - g^{j'}) \pmod{p}.$$

Como p es primo y P es de grado 2, no puede tener más de dos soluciones. De manera que $\{g^i, g^j\} = \{g^i, g^j\} = \{g^{i'}, g^{j'}\}$, esto implica que $\{i, j\} = \{i', j'\}$ y, por tanto $\{x_i, x_j\} = \{x_{i'}, x_{j'}\}$. Hemos demostrado que $F(p(p-1)) \geq p - 1$. Para un N cualquiera podemos tomar un primo p tal que $N - o(N) \leq (p-1)^2 \leq p(p-1) \leq N$ y, como en el ejemplo 3, concluimos que $F(N) \geq F(p(p-1)) \geq p - 1 \geq \sqrt{N} - o(\sqrt{N})$.

Cota superior para $F(N)$

Sea B un conjunto de Sidon contenido en el intervalo $[1, N]$, y consideramos el conjunto $B+B := \{b + b' : b, b' \in B\}$. Como las sumas son diferentes se cumple que $|B + B| = \binom{|B|+1}{2}$, donde $|B|$ denota el cardinal de B.

Por otra parte, $B + B \subset [2, 2N]$, y por lo tanto $|B + B| \leq 2N + 1$. De estos dos hechos se deduce que $|B|^2 + |B| \leq 4N + 2$, implica $|B|^2 \leq 4N$ y por lo tanto $|B| \leq 2\sqrt{N}$. En consecuencia $F(N) \leq 2\sqrt{N}$.

Esta estimación la podemos mejorar si consideramos el conjunto da las diferencias positivas $(B - B)_+$. Los conjntos de Sidon también verifican que las diferencias $b - b'$, con $b, b' \in B$ son todas diferentes. Por lo tanto se cumple que $|(B - B)_+| = \binom{|B|}{2}$. También se tiene $(B-B)_+ \subset [1, N-1]$ lo que implica que $|(B - B)_+| \leq N - 1$. Combinando estas dos estimaciones cocluimos que $F(N) < \sqrt{2N} + 1$.

Erdos P.,Turan P.(1941) mejoraron con un argumento combinatorio la cota superior.

$$F(N) \leq \sqrt{N} + o(\sqrt{N}). \tag{5}$$

Combinando (3) y (5) obtenemos

$$\lim_{N\to\infty} N^{-\frac{1}{2}} F(N) = 1. \tag{6}$$

2. DOS EJEMPLOS INTERESANTES

Para terminar con esta sección daremos dos ejemplos que serán útiles para ilustrar cómo se puede construir sucesiones de Sidon de enteros a partir de sucesiones de Sidon de reales.

Ejemplo 5. Dado N consideremos la sucesión $\{[4N^2 \log p]\}_p$, con p primo menor que N. Veamos que es una sucesión finita de Sidon. Sean p, q, r, s primos menores que N, tales que

$$[4N^2 \log p] + [4N^2 \log q] = [4N^2 \log r] + [4N^2 \log s]. \tag{7}$$

Si $\{p, q\} \neq \{r, s\}$, necesariamente $pq \neq rs$. Supongamos por ejemplo que $pq \geq rs + 1$. Teniendo en cuenta las propiedades del logaritmo y estimando las partes fraccionarias de (7), obtenemos la desigualdad

$$\left|4N^2 \log \frac{pq}{rs}\right| \leq 2.$$

Por otra parte, como $pq \geq rs + 1$, tenemos

$$\left|\log \frac{pq}{rs}\right| \geq \log\left(1 + \frac{1}{rs}\right).$$

Aplicando la desigualdad $\log(1 + x) > \frac{x}{2}, \;\; 0 < x < 1$, y la esimación $rs \leq N^2$ obtenemos la contradición.

$$\left|4N^2 \log \frac{pq}{rs}\right| \geq 4N^2 \log\left(1 + \frac{1}{rs}\right) > 4N^2 \frac{1}{2rs} > 2.$$

Así que la sucesión finita $\left\{[4N^2 \log p]_p\right\}$ es de Sidon. Recordemos que $\pi(N) \sim \frac{N}{\log N}$, donde $\pi(N)$ denota el número de primos menores o iguales que N, y como para cada primo p hay un término de la sucesión de Sidon en el intervalo $[1,\ 4N^2 \log N]$, en consecuencia

$$F(4N^2 \log N) \geq \pi(N) \sim \frac{N}{\log N}.$$

Tomando $M = 4N^2 \log N$, tenemos

$$N^2 = \frac{M}{4 \log N} \Rightarrow \frac{N}{\log N} = \frac{\sqrt{M}}{2\sqrt{\log N} \log N} \gtrsim \frac{M^{1/2}}{\log^{3/2} M}$$

en la útima desigualdad usamos que $M = 4N^2 \log N$ implica

$$2 \log N = \log M - \log(4 \log N) \leq \log M \Rightarrow \log N \lesssim \log M$$

concluimos

$$F(M) \gtrsim \frac{M^{1/2}}{\log^{3/2} M}.$$

Ejemplo 6. La demostración que presetaremos en este trabajo está basada en el siguiente ejemplo: sabemos que para cada p primo, $p \equiv 1 \pmod 4$, se puede representar de manera única como suma de dos cuadrados, $p = a^2 + b^2$, $0 < a < b$, ver **Zagier Don, (1990)**. De modo que a cada primo $p \equiv 1 \pmod 4$ le podemos asociar el ángulo ϕ_p del entero de Gauss $a + ib = \sqrt{p}e^{i\phi_p}$, con $0 < \phi_p < \frac{\pi}{4}$.

Dado un entero positivo N, consideremos la sucesión finita $\{[4N^2\phi_p]\}_{p\equiv 1 \pmod 4}$, con p un primo menor que N. Veamos que ésta sucesión es de Sidon.

Sea p, q, r, s primos congruentes con 1 (mod 4) menores que N y tales que

$$\left[4N^2\phi_p\right] + \left[4N^2\phi_q\right] = \left[4N^2\phi_r\right] + \left[4N^2\phi_s\right].$$

Quitando las partes enteras obtenemos la estimación

$$\left|4N^2(\phi_p + \phi_q - \phi_r - \phi_s)\right| \leq 2. \tag{8}$$

Obsérvase que $\phi_p + \phi_q - \phi_r - \phi_s$ es el ángulo de un entero de Gauss

$$A + iB = \sqrt{pqrs}e^{i(\phi_p+\phi_q-\phi_r-\phi_s)}.$$

Si $\{p, q\} \neq \{r, s\}$, entonces $|B| \geq 1$, de donde

$$\begin{aligned} 4N^2\left|\phi_p + \phi_q - \phi_r - \phi_s\right| &\geq 4N^2 \operatorname{arc\,sen} \frac{1}{\sqrt{pqrs}} \\ &\geq 4N^2 \operatorname{arc\,sen}\left(\frac{1}{N^2}\right) > 4, \end{aligned}$$

contradice (8), de manera que $\{p, q\} = \{r, s\}$ y por tanto la sucesión $\{[4N^2\phi_p]\}_{p\equiv 1 \pmod 4}$ es de Sidon. En este caso, como la sucesión $\{[4N^2\phi_p]\}_{p\equiv 1 \pmod 4}$ contiene un elemento por cada primo p menor que N, obtenemos que

$$F(4N^2\phi_N) \geq \pi(N) \sim \frac{N}{\log N}.$$

Tomando $M = 4N^2\phi_N$, como ϕ_N es acotada tenemos $M^{1/2} = 2N\sqrt{\phi_N} \sim N$, concluimos que

$$F(M) \gtrsim \frac{M^{1/2}}{\log M},$$

lo que resulta una mejora si lo comparamos con el ejemplo 5.

3. SUCESIONES DE SIDON

En el caso de sucesiones infinitas de Sidon el problema es más complicado que en el caso de sucesiones finitas. Los ejemplos 1 y 2 sí que se pueden extender a sucesiones infinitas. Sin embargo los ejemplos 3, 4 y 5, las distintas construcciones necesitan del conocimiento previo del tamaño del intervalo donde se va a ubicar el conjunto de Sidon. Por supuesto, esto nos impide extender estas construcciones finitas a sucesiones infinitas.

Cuando B es una sucesión infinita de números enteros, para estudiar su densidad definimos la

función $B(N)$, que cuenta para cada N, el número de elementos de B menores o iguales a N. Esto es,

$$B(N) = \sum_{b \leq N,\, b \in B} 1.$$

Del caso finito se deduce que si B es una sucesión infinita de Sidon que

$$\liminf_{N \to \infty} N^{-\frac{1}{2}} B(N) \leq 1$$

Erdos P.(1954) construyó una sucesión infinita de Sidon tal que

$$\limsup_{N \to \infty} N^{-\frac{1}{2}} B(N) \geq 1/2$$

y **Kruckeberg F.(1961)** construyó otra más densa que satisfacía

$$\limsup_{N \to \infty} N^{-\frac{1}{2}} B(N) \geq \frac{1}{\sqrt{2}}.$$

Comparando con el caso de conjuntos de Sidon finitos, se podría pensar que existen sucesiones infinitas de Sidon tales que $B(N) \gg \sqrt{N}$, para todo N. Erdös demostró que tales sucesiones no existen, esto fue publicado por **Stöhr A. (1955)**. Erdös demostró que si B es una sucesión infinita de Sidon se cumple que

$$\liminf_{N \to \infty} \frac{B(N)\sqrt{\log N}}{N^{\frac{1}{2}}} \ll 1,$$

donde $B(N)$ denota el número de elementos de B en $[1, N]$.

Por otro lado **Erdos P. (1956)** conjeturó:

Para todo $\epsilon > 0$, existe una sucesión $B = \{b_k\}$ de Sidon tal que $b_k \ll k^{2+\epsilon}$, esto es $B(N) \ll N^{\frac{1}{2}-\epsilon}$.

En el ejemplo 2, vimos que existe una sucesión infinita de Sidon tal que $b_r \leq r^3$, es decir $B(N) \gg (N \log N)^{\frac{1}{3}}$. **Komlos J., Ajtai and Szemeredi E. (1981)** mejoraron ligeramente este resultado, utilizando teoría de grafos, demostrando la existencia de una sucesión de Sidon tal que

$$B(N) \gg (N \log N)^{\frac{1}{3}}.$$

Un gran paso hacia la conjetura de Erdös se debe a **Ruzsa I. Z. (1998)**, quien demostró la existencia de una sucesión infinita de Sidon tal que $B(N) \gg N^{\sqrt{2}-1+o(1)}$. El propósito de este trabajo es rehacer detalladamente la demostración de Ruzsa, introduciendo en la prueba una modificación que pasamos a describir.

En su prueba, Ruzsa hace uso de las propiedades de la función logaritmo, observando que la sucesión $\{\log p\}_{p,\, primo}$ es una sucesión de Sidon de números reales. El incoveniete de esta sucesión, como veremos más adelante en la demostración, es que no está acotada. En su lugar, introducimos otra sucesión de las mismas características que $\{\log p\}_{p,\, primo}$ pero acotada. La sucesión que vamos a considerar es la sucesión $\{\phi_p\}_{p \equiv 1 \,(mod\, 4)}$ donde ϕ_p es el argumento del entero de Gauss $a + ib$, $a^2 + b^2 = p$ con $0 < a < b$.

Teorema 3.1 (I. Ruzsa)**.** *Existe un conjunto B de Sidon que satisface*

$$B(N) = N^{\gamma + o(1)}$$

donde $\gamma = \sqrt{2} - 1 = 0.41421356\ldots$

Vamos a detallar la demotración del teorema 3.1. Seguimos esencialmente la idea de **Ruzsa I. Z. (1998)**, pero añadiendo una simplificación no trivial la cual explicamos a continuación. Ruzsa

en su prueba considera la sucesión $\{\log p\}_{p,primo}$ que es una sucesión de Sidon de números reales, como se deduce del Teorema Fundamental de la Arimética. El hecho de que la sucesión $\{\log p\}_{p\ primo}$ no esté acotada implica complicaciones técnicas que nosotros evitaremos sustituyendo la sucesión $\{\log p\}_{p\ primo}$ por otra sucesión $\{\phi\}_p$ acotada y con las mismas propiedades que $\{\log p\}_{p\ primo}$.

Para definir nuestra sucesión de partida recordemos que un número primo $p \equiv 1 \pmod 4$ se puede representar de manera única como suma de dos cuadrados, $p = a^2 + b^2,\ 0 < a < b$. En lo que sigue p, q, r y s serán de esta forma. De modo que a cada primo $p \equiv 1 \pmod 4$ le podemos asociar el argumento ϕ_p del entero de Gauss $a + ib = \sqrt{p}e^{i\phi_p}$, con $0 < \phi_p < \frac{\pi}{4}$.

Lema 3.1.1. *La sucesión $\{\phi_p\}_p$ es una sucesión de Sidon de números reales.*

Demostración. Supongamos que $\phi_p+\phi_s = \phi_q+\phi_r$. Si multiplicamos los enteros de Gauss $\sqrt{p}e^{i\phi_p}$, $\sqrt{s}e^{i\phi_s}$, $\sqrt{q}e^{-i\phi_q}$ y $\sqrt{r}e^{-i\phi_r}$, obtenemos

$$A + iB = \sqrt{pqrs}e^{\phi_p+\phi_s-\phi_q-\phi_r} = \sqrt{pqrs}.$$

Esto implica que $B = 0$, y por lo tanto $A^2 = pqrs$. Como p, q, r y s son primos, entonces $A^2 = pqrs$ sólo puede ocurrir si $\{p, q\} = \{r, s\}$. En consecuencia $\{\phi_p\}$ es una sucesión de Sidon. □

Observación. Dado $\alpha > 0$, si $\{\phi_p\}_p$ es una sucesión de Sidon, de la demostración del lema se deduce que la sucesión $\{\alpha\phi_p\}_p$ también es una sucsión de Sidon.

El esquema de la demostración del teorema 3.1 será el siguiente:

Paso 1. Dado $\alpha \in [\frac{1}{2}, 1]$, consideremos la sucesión $\{\alpha\phi_p\}_p$, que es una sucesión infinita de Sidon de números reales. A cada $\alpha\phi_p$ le asociamos un número entero b_p, de tal forma que la sucesión $B_\alpha = \{b_p\}_p$ tenga un crecimiento adecuado, y que herede de alguna manera la propiedad de Sidon.

Paso 2. La sucesión B_α es de Sidon excepto por algunos términos *malos* cuyo número vamos a contar.

Paso 3. Con un argumento probabilistico podemos asegurar que para casi todos los $\alpha \in \left[\frac{1}{2}, 1\right]$ la cantidad de términos malos de la sucesión B_α, no supera la "$mitad$" de los términos de la sucesión B_α. La demostración termina observando que al quitar esos términos malos todavía nos queda una subsucesión con el crecimiento deseado.

4. CONSTRUCCIÓN DE LA SUCESIÓN B_α

Consideremos la sucesión $\{\alpha\phi_p\}_p$, con $\alpha \in \left[\frac{1}{2}, 1\right]$. Podemos expresar el desarrollo binario de $\alpha\phi_p$ como

$$\alpha\phi_p = \sum_{j=1}^{\infty} \delta_{jp} 2^{-j}$$

donde $\delta_{jp} = 0$ ó 1.

Observación. Los dígitos δ_{jp} dependen del parámetro α aunque no lo digamos explícitamente.

El desarrollo binario de $\alpha\phi_p$ lo usaremos para construir una sucesión de enteros $B_\alpha = \{b_p\}$ que crezca lo más lentamente posible, concretamente como p^β, con $\beta = \sqrt{2} + 1$. Para ello, truncamos el desarrollo binario de $\alpha\phi_p$ en un lugar K^2, donde K es definido para cada p por

$$K = K_\alpha = \text{mín}\left\{j > 2 :\ 2^{(j-1)^2} > p^\beta\right\} = 2 + \left[\sqrt{\beta \log_2(p)}\right] \tag{9}$$

Agruparemos los p cuyos desarrollos binarios han sido cortados en el mismo sitio K^2 en un conjunto que lo denominaremos P_K. Esto es

$$P_K = \{p :\ K_p = K\}. \tag{10}$$

Denotemos por λ_p la suma parcial

$$\lambda_p = \sum_{j=1}^{K^2} \delta_{jp} 2^{-j}.$$

El resto del desarrollo es menor que $p^{-\beta}$. Esto se deduce de la definición de K, haciendo el siguiente cálculo

$$|\lambda_p - \alpha\phi_p| = \sum_{j=K^2+1}^{\infty} \delta_{jp} 2^{-j} \leq 2^{-K^2} \leq 2^{-(K-1)^2} < p^{-\beta}. \tag{11}$$

Antes de definir explícitamente b_p, reordenamos el desarrollo binario de λ_p de la siguiente forma

$$\lambda_p = \sum_{l=1}^{K^2} \delta_{lp} 2^{-l} = \sum_{l=1}^{K} \left(\sum_{j=(l-1)^2+1}^{l^2} \delta_{jp} 2^{l^2-j} \right) 2^{-l^2} \tag{12}$$

$$= \sum_{l=1}^{K} \Delta_{lp} 2^{-l^2}, \tag{13}$$

donde los bloque Δ_{lp} están definidos por

$$\Delta_{lp} = \sum_{j=(l-1)^2+1}^{l^2} \delta_{jp} 2^{l^2-j}, \quad \text{para } 1 \leq l \leq K$$

y $\Delta_{lp} = 0$ para $l > K$. De esta definición se deduce que

$$\Delta_{lp} < 2^{l^2-(l-1)^2} = 2^{2l-1}.$$

4.1. CONSTRUCCIÓN DE $\{b_p\}$

El siguiente paso consiste en construir b_p a partir de λ_p. Asociamos a cada $\lambda_p = \Sigma_{l=1}^{K} \Delta_{lp} 2^{-l^2}$, el entero $\sum_{l=1}^{K} \Delta_{lp} 2^{l^2}$, y por razones técnicas, que justificamos posteriormente, separamos los bloques Δ_{lp} en el desarrollo binario introduciendo tres ceros entre cada bloque, después del último bloque el Δ_{Kp}, colocamos un 0 seguido de un 1. Este último 1, que corresponde a 2^{K^2+3K+1}, marca el tamaño de b_p. Concretamente

$$b_p = \sum_{l=1}^{K} \Delta_{lp} 2^{(l-1)^2+3l} + 2^{K^2+3K+1}.$$

Para tener una idea más clara de la forma que tiene el número b_p, vamos a desarrollar la suma anterior:

$$\begin{aligned} b_p = {} & \underbrace{\delta_1 2^3}_{2^3\Delta_1} + \underbrace{0+0+0} + \underbrace{\delta_4 2^7 + \delta_3 2^8 + \delta_2 2^9}_{2^7\Delta_2} + \underbrace{0+0+0} + \\ & + \underbrace{\delta_9 2^{13} + \delta_8 2^{14} + \cdots + \delta_5 2^{17}}_{2^{13}\Delta_3} + \cdots + \underbrace{0+0+0} + \\ & + \underbrace{\delta_{K^2} 2^{(K-1)^2+3K} + \cdots + \delta_{(K-1)^2+1} 2^{K^2+3K-1}}_{2^{(K-1)^2+3K}\Delta_{K^2}} + \\ & + \underbrace{0 + 2^{K^2+3K+1} + 0} \\ & \text{Sirve para marcar el tamaño de } b_p \end{aligned}$$

La construcción de la sucesión $\{b_p\}$ se ha hecho de modo que

1. La sucesión b_p crezca lo más lentamente posible, ($b_p \sim p^\beta$).

2. Herede, de alguna manera, las propiedades de Sidon de $\{\alpha\phi_p\}$.

Veamos que efectivamente b_p tiene el tamaño deseado. De la definición de b_p, se deduce de forma inmediata que

$$2^{K^2+3K} \leq b_p \leq 2^{K^2+3K+1}$$

o equivalentemente

$$2^{(K-1)^2+5K-1} \leq b_p \leq 2^{(K-1)^2+5K}$$

y por tanto, como $2^{(K-2)^2} < p^\beta \leq 2^{(K-1)^2}$, tenemos

$$b_p = p^{\beta+o(1)}.$$

4.2. CONTAR CUANTOS TÉRMINOS MALOS TIENE LA SUCESIÓN B_α

La sucesión B_α no es necesariamente de Sidon porque puede contener cuádruplas para las cuales se cumple

$$b_p + b_s = b_q + b_r, \quad \{b_p, b_s\} \neq \{b_q, b_r\}. \tag{14}$$

En esta sección vamos a estimar el número de las cuádruplas malas contenidas en la sucesión B_α, y veremos que son pocas en comparación con el tamaño de B_α.

En los sigientes lemas vamos a caracterizar las propiedades que tienen las cuádruplas que cumplen (14). Observemos que si b_p, b_s, b_q y b_r cumplen la condición (14) entonces se puede suponer, sin pérdida de generalidad, que b_p es el más grande de todos, por lo tanto b_s es el más pequeño de todos y así $b_q \geq b_r$, por lo que podemos escribir

$$b_p > b_q \geq b_r > b_s \tag{15}$$

El último término del desarrollo binario de b_p lo denotamos por

$$t_p = 2^{K^2+3K+1}.$$

En el siguiente lema se justifica la separación con ceros entre los bloques efectuada en la construcción de b_p.

Lema 4.0.1. *Sean x, y, u y v números positivos tales que $x+y = u+v$. Supongamos que $1 \leq m < n$ son enteros y que los m-ésimos y los n-ésimos dígitos, de los desarrollos binarios, de x, y, u y v son todos ceros. Sean x', y', u' y v' los enteros cuyos dígitos (m+1)-ésimos, (m+2)-ésimos,..., (n-1)-ésimos son idénticos a los de x, y, u y v respectivamente, y el resto de los dígitos son ceros. Entonces $x' + y' = u' + v'$.*

Demostración. Sea $x = \sum_{j=0}^{\infty} \delta_j^x 2^j$. Si denotamos por

$$\Delta_{g,h}^x = \sum_{j=g}^{h} \delta_j^x 2^j$$

entonces podemos expresar el desarrollo de x en la forma

$$\Delta_{0,m-1}^x + \delta_m^x 2^m + \Delta_{m+1,n-1}^x + \delta_n^x 2^n + \Delta_{n+1,\infty}^x.$$

Análogamente podemos hacer con y, u, v, $x+y$, $u+v$. En particular, escribimos

$$x' + y' = \Delta^x_{m+1,n-1} + \Delta^y_{m+1,n-1}, \tag{16}$$
$$u' + v' = \Delta^u_{m+1,n-1} + \Delta^v_{m+1,n-1}. \tag{17}$$

Observemos que $\Delta^x_{m+1,n-1}+\Delta^y_{m+1,n-1} = \Delta^{x+y}_{m+1,n-1}+\delta^{x+y}_n 2^n$, con $\delta^{x+y}_n = 0$, ó 1. En el caso $\delta^{x+y}_n = 0$, como $x+y = u+v$ implica que $\delta^{u+v}_n = 0$ de donde se deduce que

$$\Delta^u_{m+1,n-1} + \Delta^v_{m+1,n-1} = \Delta^{u+v}_{m+1,n-1} = \Delta^{x+y}_{m+1,n-1} = \Delta^x_{m+1,n-1} + \Delta^y_{m+1,n-1}.$$

Esto demuestra que $x' + y' = u' + v'$.

Para el otro caso procedemos de igual forma. $\delta^{x+y}_n = 1$, con $x+y = u+v$ implica que $\delta^{u+v}_n = 1$ de donde se deduce que

$$\Delta^u_{m+1,n-1} + \Delta^v_{m+1,n-1} = \Delta^{u+v}_{m+1,n-1} + 2^n = \Delta^{x+y}_{m+1,n-1} + 2^n = \Delta^x_{m+1,n-1} + \Delta^y_{m+1,n-1}.$$

Esto demuestra que $x' + y' = u' + v'$. Con lo cual está demostrado el lema.

□

Lema 4.0.2. *La ecuación $b_p+b_s = b_q+b_r$, con $\{b_p, b_s\} \neq \{b_q, b_r\}$ es cierta si y sólo si $t_p+t_s = t_q+t_r$ y $\Delta_{lp} + \Delta_{ls} = \Delta_{lq} + \Delta_{lr}$, para todo l.*

Demostración. Es una consecuencia directa de la definición de b_p, t_p, Δ_{lp} y del lema anterior.

□

Lema 4.0.3. *Si $b_p + b_s = b_q + b_r$ y $b_p > b_q \geq b_r > b_s$ entonces existen enteros $K \geq L$ tales que $p, q \in P_K$, $r, s \in P_L$, donde P_K es definido como en (10), y se cumple*

$$\lambda_p + \lambda_s = \lambda_q + \lambda_r. \tag{18}$$

Demostración. Por definición

$$\lambda_p = \sum_{l=0}^{K} \Delta_{lp} 2^{-l^2},$$

como $b_p + b_s = b_q + b_r$, se puede usar el lema 15, y así obtenemos

$$\Delta_{lp} + \Delta_{ls} = \Delta_{lq} + \Delta_{lr}, \quad 0 < l \leq K$$

y $t_p + t_s = t_q + t_r$. Los números t_p, t_s, t_q, t_r son potencias de 2, por lo tanto $t_p + t_s = t_q + t_r$, con $b_p > b_q \geq b_r > b_s$, sólo puede puede ser cierto si $t_p = t_q$ y $t_s = t_r$.

Las igualdades $t_p = t_q$ y $t_s = t_r$ implican que $p, q \in P_K$ y $r, s \in P_L$. Además, por la condición $b_p > b_q \geq b_r > b_s$ concluimos que $K \leq L$.

□

Lema 4.0.4. *Si $b_p + b_s = b_q + b_r$ y $b_p b_q \leq b_r > b_s$, entonces para los números K y L del lema anterior, $p, q \in P_K$, $r, s \in P_L$, $K > L$, se cumple las siguientes desigualdades*

$$|\phi_p + \phi_s - \phi_q - \phi_r| < 8\left(2^{-L^2}\right) \tag{19}$$

$$\sqrt{pqrs} > 2^{L^2-3} \tag{20}$$

$$(K-1)^2 > (\beta-1)(L-1)^2 + \beta(2L-4). \tag{21}$$

Demostración. La desigualdad (11) dice que $|\lambda_p| - \alpha\phi_p \leq 2^{-K^2} \leq 2^{-L^2}$, y de la desigualdad (18) tenemos $\lambda_p + \lambda_s = \lambda_s + \lambda_r$, combinando estos resultados, obtenemos

$$\begin{aligned} \alpha\left|\phi_p + \phi_s - \phi_q - \phi_r\right| &= \left|\alpha\phi_p - \lambda_p + \alpha\phi_s - \lambda_s + \lambda_q - \alpha\phi_q + \lambda_r - \alpha\phi_r\right| \\ &\leq \left|\alpha\phi_p - \lambda_p\right| + \left|\alpha\phi_s - \lambda_s\right| + \left|\lambda_q - \alpha\phi_q\right| + \left|\lambda_r - \alpha\phi_r\right| < 4\left(2^{-L^2}\right). \end{aligned}$$

esta desigualdad junto con la condición $\frac{1}{2} < \alpha$ demuestra $|\phi_p + \phi_s - \phi_q - \phi_r| < 8\left(2^{-L^2}\right)$.

La desigualdad (20) la demostraremos directamenre de las propiedades de las propiedades de ϕ_j. Sea $a_j + ib_j = \sqrt{j}e^{i\phi_j}$, $j = p, q, r, s$. Multiplicando adecuadamente, vemos que existen dos números A y B tales que $A + iB = \sqrt{pqrs}e^{i\phi}$ con $\phi = \phi_p + \phi_s - \phi_q - \phi_r$. Observemos que $\phi \neq 0$, por ser la sucesión $\{\phi_p\}$ de Sidon. Esto implica que el número entero B es distinto de cero, por lo tanto

$$1 \leq B^2 = (pqrs)\,\text{sen}^2(\phi) < pqrs\,|\phi|^2.$$

En vista de la desigualdad (19), $|\phi| < 8\left(2^{-L^2}\right)$, concluimos que

$$\sqrt{pqrs} > \frac{1}{8}2^{L^2}.$$

Para demostrar (22) combinamos las tres desigualdades siguientes, $\left(\sqrt{pq}\right)^{\beta} < 2^{(K-1)^2}$, $\left(\sqrt{rs}\right)^{\beta} < 2^{(K-1)^2}$ y $\left(\sqrt{pqrs}\right) > 2^{L^2} - 3$ para obtener que

$$2^{(K-1)^2}2^{(L-1)^2} > \left(\sqrt{pqrs}\right)^{\beta} > 2^{\beta(L^2-3)}$$

Si de esta desigualdad igualamos los exponentes entonces tenemos

$$(K-1)^2 > \beta(L^2-3) - (L-1)^2 = (\beta-1)(L-1)^2 + \beta(2L-4).$$

□

Definamos la siguiente cantidad

$$J_{KL} = \#\left\{p, q, r, s :\ p, q \in P_K;\ r, s \in P_L \ \text{ con } \ |\phi_p + \phi_s - \phi_q - \phi_r| < 8\left(2^{-L^2}\right)\right\}$$

En particular J_{KL} contiene a las cuádruplas p, q, r, s con $p, q \in P_K$ y $r, s \in P_L$ que satisfacen $b_p + b_s = b_q + b_r$ y $b_p > b_q \leq b_r > b_s$, es decir los términos malos de la sucesión B_α. De manera que para hallar una primera estimación de estos términos malos, vamos a estimar a J_{KL}, para cualquier K y L.

Lema 4.0.5.

$$J_{KL} =\ll 2^{2\gamma\left((K-1)^2+(L-1)^2\right)-L^2} \quad \left(\gamma = \frac{1}{\beta}\right).$$

Demostración. Inicialmente, consideramos q, r y s fijos. Estimaremos la medida del conjunto

$$\left\{p :\ |\phi_p + \phi_s - \phi_q - \phi_r| < 8 \cdot 2^{-L^2}\right\}$$

Recordemos que $2^{\gamma(K-2)^2} < p \leq 2^{\gamma(K-1)^2}$, como se deduce de la definición de K. Además, para cada p existen dos enteros únicos a_p, b_p tales que $a_p^2 + b_p^2 = p$. A cada entero p le asociamos el entero de Gauss $a_p + ib_p = \sqrt{p}e^{i\phi_p} = \omega_p$. De manera que estos p tienen asociados un único entero de Gauss ω_p contenido en el sector circular

$$\Gamma = \{\omega \in \mathbb{C}\} :\ 0 \leq |\omega| \leq 2^{\frac{1}{2}\gamma(K-1)^2,\ |\arg\omega + \phi_s - \phi_q - \phi_r| < 8\cdot 2^{-L^2}}.$$

Los argumentos de cada $\omega_p \in \Gamma$ son distintos, y por lo tanto los podemos ordenar:

$$\phi_{p_1} < \phi_{p_2} < \phi_{p_3} < \cdots$$

A cada punto $\omega_{p_j} \in \Gamma$ les asociamos el triágulo $\triangle_j$ con vértices ω_{p_j}, $\overline{0}$, $\omega_{p_{j+1}}$. Claramente los triágulos no tienen puntos interiores comunes y están contenidos en Γ. Así que

$$\sum_{\omega_{p_j} \in \Gamma} \text{área}(\triangle_j) \leq \text{área}(\Gamma) + 1.$$

Como el área de cualquier triágulo de vértices con coordenadas enteras, es a lo menos $1/2$. Concluimos que

$$\sum_{\omega_p \in \Gamma} 1 \leq 2 \ \text{área}(\Gamma) + 2$$

y así el área$(\Gamma) \leq 1$. Por lo tanto el número de ω_p contenido en Γ están acotado por

$$\left(2^{\frac{1}{2}\gamma(K-1)^2}\right)^2 2^{3-L^2} + 2 = O\left(2^{\gamma(K-1)^2} 2^{-L^2}\right).$$

Luego multiplicamos por el número de q que es menor que $2^{\gamma(K-1)^2}$, por el número de s que es menor que $2^{\gamma(L-1)^2}$ y por el número de r que es menor que $2^{\gamma(L-1)^2}$. Efectuando el producto termina la demostración.

□

4.3. ARGUMENTO PROBABILÍSTICO

La condición $|\phi_p + \phi_s - \phi_q - \phi_r| < 8 \cdot 2^{-L^2}$ es necesaria para hallar una solución de $b_p + b_s = b_q + b_r$, pero no es una condición suficiente. Ahora usaremos el parámetro α para obtener otras condiciones que permitirán mejores estimaciones para el número de términos malos de la sucesión B_α.

Lema 4.0.6. *Si $b_p + b_s = b_q + b_r$ con $\{b_p, b_s\} \neq \{b_q, b_r\}$, $p, q \in P_K$ y $r, s \in P_L$, con $K > L$, se cumple*

$$\left[2^{K^2}\alpha\phi_p\right] \equiv \left[2^{K^2}\alpha\phi_q\right] \quad \left(\textit{mod}\ 2^{K^2-L^2}\right) \tag{22}$$

Demostración. Recordemos que $\alpha\phi_p = \sum_{j=1}^{\infty} \delta_{jp} 2^{-j}$, con $\delta_{jp} = 1$ ó 0. Por lo tanto, como $K > L$ los términos de la derecha de la primera igualdad son todos números enteros, así tenemos

$$\left[2^{K^2\alpha\phi_p}\right] = \sum_{j=1}^{K^2} \delta_{jp} 2^{K^2-j} = \left(\sum_{j=L^2+1}^{K^2} \delta_{jp} 2^{K^2-j}\right) + 2^{K^2-L^2}\left(\sum_{j=1}^{L^2} \delta_{jp} 2^{L^2-j}\right)$$

es decir, que se cumple la siguente congruencia

$$\left[2^{K^2\alpha\phi_p}\right] \equiv \sum_{j=L^2+1}^{K^2} \delta_{jp} 2^{K^2-j} \pmod{2^{K^2-L^2}}. \tag{23}$$

Del mismo modo podemos ver que

$$\left[2^{K^2\alpha\phi_q}\right] \equiv \sum_{j=L^2+1}^{K^2} \delta_{jq} 2^{K^2-j} \pmod{2^{K^2-L^2}}. \tag{24}$$

De manera que para concluir la demostración del lema es suficiente con probar que

$$\sum_{j=L^2+1}^{K^2} \delta_{jp} 2^{K^2-j} = \sum_{j=L^2+1}^{K^2} \delta_{jq} 2^{K^2-j} \tag{25}$$

Para demostrar esta igualdad usaremos los $\triangle_{mp}$ que definimos para $p \in P_K$ por

$$\triangle_{mp} = \begin{cases} \sum_{j=(m-1)^2+1}^{m^2} \delta_{mp} 2^{m^2-j} & \text{si} \quad m \leq K \\ \\ 0 & si \quad m > K \end{cases}$$

para escribir

$$\sum_{j=(L)^2+1}^{K^2} \delta_{jp} 2^{K^2-j} = \sum_{m=L+1}^{K} \left(2^{K^2-m^2} \sum_{j=(m-1)^2+1}^{m^2} \delta_{jp} 2^{m^2-j} \right) = \sum_{j=L+1}^{K} \triangle_{mp} 2^{K^2-m^2}.$$

Del mismo modo lo hacemos usando q en lugar de p, tenemos

$$\sum_{j=L^2+1}^{K^2} \delta_{jq} 2^{K^2-j} = \sum_{j=L+1}^{K} \triangle_{qm} 2^{K^2-m^2}.$$

Así que la demosración se reduce a probar que $\triangle_{mp} = \triangle_{mq}$, para $L < m \leq K$. Ahora utilizaremos la hipótesis $b_p + b_s = b_q + b_r$ para justificar el uso del lema 4.0.2 que garantiza la igualdad

$$\triangle_{mp} + \triangle_{ms} = \triangle_{mq} + \triangle_{mr}.$$

Pero de la definición $\triangle_{mj}$, sabemos que $\triangle_{ms} = \triangle_{mr} = 0$, para $L < m$. Por lo tanto $\triangle_{mp} = \triangle_{mq}$, $L < m \leq K$. Esto termina la demostración.

□

Si $b_p + b_s = b_q + b_r$, entonces el lema anterior dice que p y q satisfacen

$$\left[2^{K^2} \alpha \phi_p\right] \equiv \left[2^{K^2} \alpha \phi_q\right] \quad (\text{ mod } 2^{K^2-L^2}) \tag{26}$$

Como la congruencia (26) depende del parámetro α, vamos a estimar la medida del conjunto que contiene a los α para los cuales se cumple (26).

Lema 4.0.7. *Sea $K > L$ y $p, q \in P_K$, $p \neq q$ dados. Supongamos que existe por lo menos un par $r, s \in P_L$ y $\alpha \in \left[\frac{1}{2}, 1\right]$ tal que se cumple la ecuación $b_p + b_s = b_q + b_r$, con $\{b_p, b_s\} \neq \{b_q, b_r\}$. Entonces tenemos*

$$\mu \left\{ \alpha : \ \left[2^{K^2 \alpha \phi_p}\right] \equiv \left[2^{K^2 \alpha \phi_q}\right] \quad (mod\ 2^{K^2-L^2}) \right\} \ll 2^{L^2-K^2} \tag{27}$$

donde μ es la medida de Lebesgue.

Demostración. Es claro que $[x] - [y] = [x - y] + 0$ ó 1, lo que nos permite escribir la congruencia (26) en la forma

$$\left[2^{K^2} \alpha (\phi_p - \phi_q)\right] \equiv 0 \quad \text{ó } -1 \quad (\text{ mod } 2^{K^2-L^2}) \tag{28}$$

Sean $M = 2^{K^2-L^2}$ y $T = \left|2^{K^2} (\phi_p - \phi_q)\right|$.

Observemos que los números reales x que satisfacen que $[x] \equiv 0$ ó -1 (mod M) ocupa un intervalo de medida 2 sobre cualquier intervalo de medida M. En particular, si tomamos $x = \alpha T$ concluimos

que los conjuntos de números α que satisfacen (28) ocupa un intervalo de medida $\frac{2}{T}$, sobre cualquier intervalo de medida $\frac{M}{T}$. El número de estos intervalos que intersecan al $\left[\frac{1}{2},\ 1\right]$ no puede ser mayor que $1+\frac{T}{2M}$. Por lo tanto

$$\mu\left\{\alpha:\ \left[2^{K^2}\alpha\phi_p\right]\equiv\left[2^{K^2}\alpha\phi_q\right]\pmod{2^{K^2-L^2}}\right\}\leq\left(\frac{2}{T}\right)\left(1+\frac{T}{2M}\right).$$

Para terminar la prueba, veamos que

$$\left(\frac{2}{T}\right)\left(1+\frac{T}{2M}\right)\ll 2^{L^2-K^2}.$$

Del lema 4.0.4, ecuación (19), sabemos que

$$|\phi_s-\phi_r|-|\phi_p-\phi_q|\leq|\phi_p+\phi_s-\phi_q-\phi_r|<8\left(2^{-L^2}\right)$$

es decir

$$|\phi_s-\phi_r|-8\left(2^{-L^2}\right)\leq|\phi_p-\phi_q|. \tag{29}$$

Por otro lado, sabemos que existen dos números enteros únicos A y B tales que $A+iB=\sqrt{rs}e^{i(\phi_r-\phi_s)}$ y además $B\neq 0$. De lo contrario $A^2=rs$ lo que es una contradición, por ser r y s primos distintos. Tenemos

$$1\leq B^2=rs\,\mathrm{sen}^2(\phi_r-\phi_s)<rs\,|\phi_r-\phi_s|^2$$

y como $r^\beta<2^{L^2}$ y $s^\beta<2^{L^2}$ implica $|\phi_r-\phi_s|>\frac{1}{\sqrt{rs}}>2^{-\frac{1}{\beta}L^2}$, si lo combinamos con (29) obtenemos la estimación

$$|\phi_p-\phi_q|\geq 2^{-\frac{1}{\beta}L^2}-8\cdot 2^{-L^2}\gg 2^{-\frac{1}{\beta}L^2}.$$

De esta manera hemos demostrado que

$$T\gg 2^{K^2-\frac{1}{\beta}L^2}>M=2^{K^2-L^2}$$

Con esta estimación podemos terminar la demostración, puesto que

$$\frac{2}{T}\left(\frac{2M+T}{2M}\right)=\left(\frac{2}{T}+\frac{1}{M}\right)\ll\frac{1}{M}=2^{L^2-K^2}.$$

□

Lema 4.0.8. *Sean $K>L$, $p,q\in P_K$, $p\neq q$ y $r,s\in P_L$ dados. Tenemos que*

$$\mu\left(\{\alpha:\ b_p+b_s=b_q+b_r\}\right)\ll 2^{L^2-K^2}$$

si $|\phi_p+\phi_s-\phi_q-\phi_r|\leq 8\cdot 2^{-L^2}$ *y* $\mu\left(\{\alpha:\ b_p+b_s=b_q+b_r\}\right)=0$ *en otro caso.*

Demostración. Si $|\phi_p+\phi_s-\phi_q-\phi_r|>8\cdot 2^{-L^2}$ el lema 4.0.4 implica que $\mu(\{\alpha:\ b_p+b_s=b_q+b_r\})=0$.

Si $|\phi_p+\phi_s-\phi_q-\phi_r|\leq 8\cdot 2^{-L^2}$ puede ocurrir que $b_p+b_s=b_q+b_r$, lo que implica, usando el lema 4.0.6, que p y q satisfacen

$$\left[2^{K^2}\alpha\phi_p\right]\equiv\left[2^{K^2}\alpha\phi_q\right]\pmod{2^{2^{K^2}-L^2}}.$$

En resumen, si $|\phi_p + \phi_s - \phi_q - \phi_r| \leq 8 \cdot 2^{-L^2}$, tenemos

$$\begin{aligned} \mu\left(\{\alpha:\ b_p + b_s = b_q + b_r\}\right) &\leq \mu\left\{\left[2^{K^2}\alpha\phi_p\right] \equiv \left[2^{K^2}\alpha\phi_q\right] \pmod{2^{K^2} - L^2}\right\} && (30) \\ &\ll 2^{L^2-K^2}. && (31) \end{aligned}$$

En la última estimación usamos la ecuación (27).

□

Sea $G_{KL}(\alpha) = \#\{p,\ q,\ r,\ s:\ p,q \in P_K,\ r,s \in P_L,\ p \neq q,\ b_p + b_s = b_q + b_r\}$. Definamos

$$G_K(\alpha) = \sum_{L<K} G_{KL}(\alpha)$$

o equivalentemente

$$G_K(\alpha) = \#\{p,\ q,\ r,\ s:\ p,q \in P_K,\ b_p + b_s = b_q + b_r y b_p > b_q \geq b_r > b_s\}.$$

Nuestro interés es ver que el número de términos malos de la sucesión B_α no son muchos. Así que vamos a comparar $G_K(\alpha)$, que representa el número de b_p, $p \in P_K$ con $b_p + b_s = b_q + b_r$, y el número de elementos de P_K. Para calcular el cardinal de P_K, usaremos el Teorema del número primo para $p \equiv 1 \pmod 4$, que dice

$$\pi'(x) \sim \frac{x}{2\log x}$$

donde $\pi'(x)$ es el número de primos congruente con 1 (mod 4) que no supera a x. Así que

$$\begin{aligned} |P_K| &= \pi'\left(2^{\gamma(K-1)^2}\right) - \pi'\left(2^{\gamma(K-2)^2}\right) && (32) \\ &= \pi'\left(2^{\gamma(K-1)^2}\right)\left(1 - \frac{\pi'\left(2^{\gamma(K-2)^2}\right)}{\pi'\left(2^{\gamma(K-1)^2}\right)}\right) \\ &\sim \frac{2^{\gamma(K-1)^2}}{(2\gamma\log 2)K^2}. && (33) \end{aligned}$$

En los siguientes dos lemas vamos a calcular una cota superior para $\int_{1/2}^{1} G_K(\alpha)\,d\alpha$. Esta estimación la usaremos para aplicar el lema de Borel-Cantelli y encontrar una cota superior para $G_K(\alpha)$. Esto lo veremos más adelante en la demostración del teorema de Ruzsa.

Lema 4.0.9. *Para cada $K > L$ tenemos*

$$\int_{\frac{1}{2}}^{1} G_{KL}(\alpha)d\alpha \ll 2^{2\gamma\left((L-1)^2+(K-1)^2\right)-K^2}.$$

Demostración. En vista de la definición de J_{KL}, para toda α se cumple que $G_{KL}(\alpha) \leq J_{KL}$, y por lo tanto, el lema 4.0.5 implica que para toda α se satisface

$$G_{KL}(\alpha) \ll 2^{2\gamma\left((K-1)^2-(L-1)^2\right)-L^2}.$$

Por otro lado, el lema 4.0.8 implica que el conjunto de los α tal que $G_{KL}(\alpha) \neq 0$ es $\ll 2^{L^2-K^2}$. Así

que

$$\int_{1/2}^{1} G_{KL}(\alpha)d\alpha \leq \mu\left(\{\alpha:\ b_p+b_s=b_q+b_r\}\right) J_{KL} \tag{34}$$

$$\ll 2^{2\gamma\left((K-1)^2+(L-1)^2\right)-L^2}\, 2^{L^2-K^2}. \tag{35}$$

□

Lema 4.0.10.

$$\int_{\frac{1}{2}}^{1} G_K(\alpha)d\alpha \ll 2^{\gamma(K-1)^2-2K}.$$

Demostración. De las definiciones de $G_K(\alpha)$ y $G_{KL}(\alpha)$, tenemos

$$G_K(\alpha)=\sum_{L\leq K} G_{KL}(\alpha).$$

Recordemos que el lema 4.0.4 dice que $b_p+b_s=b_q+b_r$ y $b_p>b_q\leq b_r>b_s$, entonces $(\beta-1)(L-1)^2<(K-1)^2$. Por lo tanto, $G_{KL}(\alpha)\neq 0$ es posible sólo si $(L-1)^2<\dfrac{(K-1)^2}{(\beta-1)}$. Usando el lema 4.0.9 y $(L-1)^2<(K-1)^2/(\beta-1)$,tenemos

$$\int_{\frac{1}{2}}^{1} G_K(\alpha)d\alpha \ll 2^{Z}$$

donde

$$Z=2\gamma\left(1+\frac{1}{(\beta-1)}\right)(K-1)^2-K^2=\left(\frac{2}{(\beta-1)}-1\right)(K-1)^2-2K+1.$$

Como $\beta=1+\sqrt{2}$, se cumple la igualdad

$$\frac{2}{\beta-1}-1=\frac{1}{\beta}$$

esto demuestra el lema.

□

4.4. DEMOSTRACIÓN DEL TEOREMA DE I. RUZSA

Usando el lema 4.0.10, tenemos

$$\mu\left(\left\{\alpha:\ \frac{G_K(\alpha)}{2\gamma(K-1)^2-K}\geq 1\right\}\right) = \int_{\frac{1}{2}}^{1}\chi_{\left\{\alpha:\ \frac{G_K(\alpha)}{2^{\gamma(K-1)^2-K}}\geq 1\right\}}d\alpha$$

$$\leq \int_{\frac{1}{2}}^{1}\frac{G_K(\alpha)}{2^{\gamma(K-1)^2-K}}d\alpha\leq 2^{-K},$$

en consecuencia, para la suma tenemos

$$\sum_{k=1}^{\infty}\mu\left(\left\{\alpha:\ \frac{G_K(\alpha)}{2^{\gamma(K-1)^2-K}}\geq 1\right\}\right)<\infty$$

aplicando el lema de Borel-Cantelli sabemos que para casi todos los α existe K_α, tal que para todo $K \geq K_\alpha$ se cumple

$$G_K(\alpha) < 2^{\gamma(K-1)^2-K} \tag{36}$$

Fijamos uno de estos α y sea K_0 tal que para todos los $K > K_0$ se cumpla (36).

Por otro lado, por (32), sabemos que

$$|P_K| \sim \frac{2^{\gamma(K-1)^2}}{(\gamma \log 2)K^2}.$$

Esta equivalencia junto con (36), demuestran que el número de $p \in P_K$ tales que $b_p + b_s = b_q + b_r$ y $b_p > b_q \geq b_r > b_s$, no pueden ser muchos, ya que

$$G_K(\alpha) < 2^{\gamma(K-1)^2-K} < \frac{2^\gamma (K-1)^2}{(\gamma \log 2)K^2} < \frac{|P_K|}{2} \tag{37}$$

Para obtener nuestro conjunto de Sidon, procedemos de la siguiente manera:

1. Denotemos por R_K el conjunto formado por $p \in P_K$, para los cuales existen p, q, r y s que satisfacen $b_p + b_s = b_q + b_r$ y $b_p > b_q \geq b_r > b_s$. La desigualdad (37) demuestra que

$$|R_K| < \frac{|P_K|}{2}.$$

2. Para cada P_K, definamos el conjunto $Q_K := \{b_p : p \in P_K,\ p \notin R_K\}$. Del paso 1, sabemos que el cardinal de Q_K satisface

$$|Q_K| > \frac{|P_K|}{2}.$$

3. La sucesión $B = B_\alpha$ la vamos a definir por

$$B = \cup_{K>K_0} Q_K.$$

Por construcción se deduce que B es una sucesión de Sidon. Veamos ahora que la sucesión B tiene crecimiento deseado. Para ello, vamos a estimar el número de elementos de B menores que N, y demostramos que

$$B(N) = N^{\gamma+o(1)}.$$

Recordemos que $b_p = \sum_{l=1}^{K} \triangle_{lp} 2^{(l-1)^2+3l} + 2^{K^2+3K+1}$. De donde se deduce que

$$b_p < 2^{K^2+3K+2} < 2^{(K+2)^2}.$$

Por lo tanto, para $K = \left[\sqrt{\log_2 N} - 2\right]$ y usando (32), tenemos que

$$\begin{aligned} B(N) &= \left| \bigcup_{L=K_0+1}^{K} Q_L \right| \\ &> \sum_{L=K_0+1}^{K} \left(\pi' \left(2^{\gamma(L-1)^2} \right) - \pi' \left(2^{\gamma(L-2)^2} \right) \right) \\ &= \frac{1}{2} \left(\pi' \left(2^{\gamma(K-1)^2} \right) - \pi' \left(2^{\gamma}(K_0 - 1)^2 \right) \right) \\ &\gg \left(\frac{1}{2} - \epsilon \right) \pi \left(2^{\gamma(K-1)^2} \right) \\ &= \left(\frac{1}{2} - \epsilon \right) \frac{2^{\gamma(K-1)^2}}{(2\gamma \log_2) K^2} \sim N^{\gamma + o(1)}. \end{aligned}$$

En otro sentido, utilizando la estimación $b_p > 2^{K^2+3K} > 2^{(K+1)^2}$, podemos demostrar que

$$B(N) \ll N^{\gamma+o(1)}.$$

Con esto terminamos la demostración del teorema de I. Ruzsa.

□

Este trabajo fue propuesto por el profesor Javier Cilleruelo con quien tuve el orgullo de conversar sobre estos temas.

5. REFERENCIAS

Bose R.C. and Chowla S. (1962). *Theorems in additive theory of number*, Commentii mathematici helvetici, **37**, 141–147.
https://www.e-periodica.ch/digbib/view?pid=com-001:1962:37#173

Erdös P.(1954). *On a problem of Sidon in additive number theory*, Acta Scientiarum Mathematicarum Universitatis. Szegediensis 15, 255–259.
http://pub.acta.hu/acta/showCustomerVolume.action?noDataSet=true

Erdös P. (1956). *Problems and resuls in additive number theory, "Colloque théorie des nombres[1955. Bruxelles]"* Liège, G. Thone; Paris, Masson, Centre Belge Recherche Mathématiques. 127–137. MR 79027, Zbl 0073.03102

Erdös P.,Turan P.(1941). *On a problem of Sidon in additive number theory, and sor related problems.* Journal of the London Mathematical Society, s1-16(4), 212–215.
DOI: https://doi.org/10.1112/jlms/s1-16.4.212

Ruzsa I. Z. (1998). *An infinite Sidon sequence.* Journal of Number Theory. **68**, 63–71.
https://www.sciencedirect.com/journal/journal-of-number-theory/vol/68/issue/1

Krückeberg F.(1961). *b_2-folgen und verwandte zahlenfolgen.* Journal für die reine und angewandte Mathematik, **206**, 53–60.
DOI: https://doi.org/10.1515/crll.1961.206.53

Komlós J., Ajtai and Szemerédi E. (1981). *A dense infinite Sidon sequence.* European Journal of Combinatorics **2**, 1–11.
DOI: https://doi.org/10.1016/S0195-6698(81)80014-5

Sidon S. (1932). *Ein satz über trigonometrische polynome und seine anwendung inder fourier-reihen.* Math. Ann. **106**, 536–539.
DOI: https://doi.org/10.1007/BF01455900

Stöhr A. (1955). *Gelöte undungelöst fragen über basen der natürlichen zahlenreihe, II.* Journal für die reine und angewandte Mathematik **194**, 111–140.
DOI: https://doi.org/10.1515/crll.1955.194.111 1975.

Zagier Don (1990). *A one-sentence proof that every prime $p \equiv 1$ mod 4 is a sum of two squares.* Amer. Math. Monthly **97**, no. 2, 144,
doi:10.2307/2323918 http://www.jstor.org/pss/2323918