Revista Colombiana de Matemáticas
Volumen 45(2011)2, páginas 113-127

Una nota sobre conjuntos de Sidon infinitos

A Remark on Infinite Sidon Sets

Juan Pablo Maldonado López

Université Pierre et Marie Curie, Paris, Francia

Resumen. Un conjunto de Sidon es un subconjunto de los enteros con la propiedad que la suma de cada dos elementos es distinta. En 1998, I. Ruzsa dio una construcción probabilística de un conjunto de Sidon infinito cuya función de conteo es $x^{\sqrt{2}-1+o(1)}$. En este trabajo mostramos una simplificación de dicha construcción.

Palabras y frases clave. Conjuntos de Sidon, teoría combinatoria de números, primos gaussianos.

2000 Mathematics Subject Classification. 11P21, 11B75.

Abstract. A Sidon set is a subset of the integers with the property that the sums of every two elements are distinct. In 1998, I. Ruzsa gave a probabilistic construction of an infinite Sidon set whose counting function is given by $x^{\sqrt{2}-1+o(1)}$. In this work we simplify such a construction.

Key words and phrases. Sidon sets, Additive number theory, Gaussian primes.

1. Introducción

Un conjunto de enteros positivos $\mathcal{S}$ se llama *conjunto de Sidon* si las sumas de cualesquiera dos elementos de $\mathcal{S}$ son distintas. Por ejemplo, el conjunto de las potencias de 2 es un conjunto de Sidon infinito. Estos conjuntos aparecieron en los años 30 en el contexto del análisis armónico gracias al trabajo de Simon Sidon en [4], quién llamó la atención de Paul Erdös sobre estos conjuntos y desde entonces han sido de particular interés en teoría de números y combinatoria. Una buena referencia sobre los resultados y las distintas generalizaciones es [2].

Un problema interesante es determinar la cardinalidad del mayor conjunto de Sidon contenido en el intervalo $[1, x]$. Para un conjunto $\mathcal{S}$ de enteros positivos, definimos la función de conteo del conjunto $\mathcal{S}$ como $S(x) = \#\mathcal{S} \cap [1, x]$. No es difícil observar que si $\mathcal{S}$ es un conjunto de Sidon, $S(x) \ll \sqrt{x}$.

Utilizando el algoritmo avaro (*greedy algorithm*) podemos construir un conjunto de Sidon con función de conteo $\gg x^{\frac{1}{3}}$. Este resultado se puede mejorar. En [3] I. Ruzsa construyó un conjunto de Sidon con función de conteo $x^{\sqrt{2}-1+o(1)}$. Su construcción se basa en el hecho de que los números primos son un conjunto de Sidon multiplicativo para los enteros; el conjunto de sus logaritmos es un conjunto de Sidon aditivo de números reales y un redondeo apropiado de ellos da un conjunto de Sidon de enteros.

En este trabajo, siguiendo las ideas de la construcción de Ruzsa (y la simplificación sugerida en [1]), construiremos un conjunto de Sidon con la misma función de conteo. Consideramos los argumentos de los primos gaussianos (los primos en $\mathbb{Z}[i]$) no reales. Esta sucesión es acotada, lo que simplifica la demostración. Algunas cotas técnicas que aparecen en el artículo de Ruzsa se demuestran de manera geométrica. Hemos conservado la notación de Ruzsa para facilitar la comparación con el argumento original. En la sección siguiente discutimos la construcción de un conjunto de Sidon para el caso finito, a fin de motivar la construcción para el caso infinito y en las dos secciones restantes explicamos la construcción del conjunto de Sidon infinito. Esta construcción es probabilística.

El problema de encontrar un subconjunto infinito *grande* de $\mathbb{Z}$ tal que las sumas de cada tres elementos sean distintas (donde por *grande* entendemos que tiene una función de conteo mayor que la que se obtiene con el algoritmo avaro) permanece abierto.

2. Conjuntos de Sidon finitos

En esta sección mostraremos como obtener conjuntos de Sidon finitos. El primer intento natural, como se mencionó en la introducción, es considerar el algoritmo avaro. Definimos $a_1 = 1$ y para $k > 1$ tomamos a_k de manera que $a_k \notin \{a_i + a_j - a_l : 1 \leq i, j, l \leq k-1\}$. Inmediatamente observamos que $a_k \leq (k-1)^3+1$ ya que tenemos a lo más $(k-1)^3$ elecciones prohibidas para $\{i, j, l\}$ y entonces con esta construcción obtenemos un conjunto de Sidon de tamaño $\sim n^{\frac{1}{3}}$ contenido en el conjunto $\{1, 2, \ldots, n\}$. La construcción de un conjunto de Sidon finito mediante el algoritmo avaro se extiende al caso infinito.

El teorema fundamental de la aritmética nos ayuda a mejorar el exponente de n.

Seguimos la notación usual y escribimos $\lfloor y \rfloor$ para el mayor entero menor o igual que y y $\{y\} = y - \lfloor y \rfloor$.

Teorema 1. *El conjunto*

$$\mathcal{X} := \left\{ x_p \in \mathbb{N} : x_p = \left\lfloor \frac{2n}{\log n} \log p \right\rfloor, \quad p \leq \sqrt{\frac{n}{2 \log n}}, \quad p \text{ primo} \right\}$$

es un conjunto de Sidon con $\sim \frac{\sqrt{2n}}{\log^{3/2} n}$ *elementos para* n *suficientemente grande.*

Demostración. Veamos primero que este conjunto es un conjunto de Sidon. Para ver esto, supongamos que se tienen p, q, r, s con $\{p, q\} \neq \{r, s\}$ tales que

$$x_p + x_q = x_r + x_s.$$

sin pérdida de generalidad, $pq > rs$. Como $x_p + x_q - x_r - x_s = 0$,

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

Utilizando el hecho de que, para números reales x, y, z, w se tiene la desigualdad

$$\big|\{x\} + \{y\} - \{z\} - \{w\}\big| \leq 2 \tag{1}$$

obtenemos

$$\frac{2n}{\log n}\log\frac{pq}{rs} \leq 2$$

de donde

$$\frac{\log n}{n} \geq \log\frac{pq}{rs}.$$

Por otro lado

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

lo cual es una contradicción (la primera desigualdad se sigue de que $pq > rs$, la segunda desigualdad se sigue de la desigualdad $\log(1+x) \geq \frac{x}{2}$ para $x < 2$ y la tercera desigualdad se sigue de la definición de r y s).

La segunda afirmación es consecuencia del teorema de los números primos. ☑

El redondeo de los logaritmos de los primos depende de n. Así que no es posible utilizar este argumento para construir un conjunto de Sidon infinito. Ruzsa se inspiró en esta construcción y eliminó la dependencia de n. Introducimos otra construcción de un conjunto de Sidon finito para motivar nuestra variante de la construcción de Ruzsa.

Sea $\mathbb{P}$ el conjunto de los números primos congruentes a 1 módulo 4. Para $p \in \mathbb{P}$, escribimos $p = a^2 + b^2 = (a + bi)(a - bi)$. La descomposición de p como suma de dos cuadrados es única y por tanto su factorización en $\mathbb{Z}[i]$ también lo es salvo unidades $(\pm 1, \pm i)$. Sea $\rho_p = a + bi$ tal que $p = \rho_p \overline{\rho_p}$, con $\overline{\rho_p}$ tal que $\operatorname{Re} \overline{\rho_p} > \operatorname{Im} \overline{\rho_p} > 0$, donde $\operatorname{Re} z$, $\operatorname{Im} z$ denotan las partes real e imaginaria respectivamente del número complejo z. Escribamos $\frac{\overline{\rho_p}}{\rho_p} = e^{2\pi i \phi_p}$ con ϕ_p un número en $[0, 1)$. Denotamos con $|z|$ el valor absoluto del número complejo z. La sucesión $(\phi_p)_{p \in \mathbb{P}}$ es un conjunto de Sidon módulo 2π, pues si tenemos $\phi_p + \phi_q = \phi_r + \phi_s$, esto implicaría que $\overline{\rho_p}\ \overline{\rho_q} \rho_r \rho_s = \rho_p \rho_q \overline{\rho_r}\ \overline{\rho_s}$ lo cual es imposible si $\{p, q\} \neq \{r, s\}$. Se tiene el siguiente teorema.

Teorema 2. *El conjunto*

$$\mathcal{C} := \left\{ c_p \in \mathbb{N} : c_p = \lfloor n\phi_p \rfloor, \quad p \in \mathbb{P}, \quad p \leq \frac{\sqrt{n}}{4} \right\},$$

es un conjunto de Sidon contenido en $\{1, 2, \ldots, n\}$ *con* $\frac{\sqrt{n}}{4 \log n}$ *elementos.*

Demostración. Supongamos que tenemos cuatro elementos en nuestro conjunto tales que

$$c_p + c_q = c_r + c_s$$

con $\{p, q\} \neq \{r, s\}$ y $pq > rs$. Consideramos

$$n(\phi_p + \phi_q - \phi_r - \phi_s) = \{n\phi_p\} + \{n\phi_q\} - \{n\phi_r\} - \{n\phi_s\}. \tag{2}$$

Observemos que

$$\begin{aligned} \left| \frac{\overline{\rho_p}\,\overline{\rho_q}}{\rho_p \rho_q} - \frac{\overline{\rho_r}\,\overline{\rho_s}}{\rho_r \rho_s} \right| &= \left| 1 - \frac{\rho_p \rho_q \overline{\rho_r}\,\overline{\rho_s}}{\overline{\rho_p}\,\overline{\rho_q} \rho_r \rho_s} \right| \\ &= \left| 1 - e^{2\pi i(\phi_p + \phi_q - \phi_r - \phi_s)} \right| \\ &\leq 2\pi \left| \phi_p + \phi_q - \phi_r - \phi_s \right| \\ &\leq \frac{4\pi}{n} \end{aligned}$$

donde la primera desigualdad es inmediata de la interpretación geométrica[1] y la segunda desigualdad se sigue de (1) y (2). Por otra parte,

[1] La longitud de la cuerda que une a 1 y $e^{i\theta}$ es menor o igual que θ, la longitud del arco que subtiende.

$$\left|\frac{\overline{\rho_p}\,\overline{\rho_q}}{\rho_p\rho_q}-\frac{\overline{\rho_r}\,\overline{\rho_s}}{\rho_r\rho_s}\right|=\left|\frac{\overline{\rho_p}\,\overline{\rho_q}\rho_r\rho_s-\overline{\rho_r}\,\overline{\rho_s}\rho_p\rho_q}{\rho_p\rho_q\rho_r\rho_s}\right|$$
$$\geq\frac{1}{\sqrt{pqrs}}$$
$$\geq\frac{16}{n}.$$

De las desigualdades anteriores se tiene

$$\frac{16}{n}\leq\frac{4\pi}{n}$$

que es una contradicción. El teorema de los números primos nos da la cardinalidad de $\mathcal{C}$. ☑

3. La construcción

Sea $\alpha\in[1,2)$ y consideramos el conjunto

$$\{\alpha\phi_p\in\mathbb{R}:p\in\mathbb{P}\}.$$

Sea $\beta>1$ el número real que satisface

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

Sea $K_p>2$ entero tal que

$$2^{(K_p-2)^2}<p^\beta<2^{(K_p-1)^2}.$$

Consideramos el conjunto

$$P_K=\{p\in\mathbb{P}:K_p=K\}.$$

Para $p\in P_K$ sea

$$m_p:=\left\lfloor 2^{K^2}\alpha\phi_p\right\rfloor=\sum_{i=1}^{K^2}\delta_{ip}2^{K^2-i}$$

con $\delta_{ip}\in\{0,1\}$. Estos números, cuando p varía sobre $\mathbb{P}$, son el ingrediente principal para nuestro conjunto de Sidon. Cortamos este número en $\Delta_{1p},\Delta_{2p},\ldots,$ Δ_{Kp} bloques de manera que

$$\Delta_{ip}=\sum_{j=(i-1)^2+1}^{i^2}\delta_{jp}2^{i^2-j}$$

y por tanto tenemos

$$\Delta_{ip} \leq \sum_{j=(i-1)^2+1}^{i^2} 2^{i^2-j} = 2^{2i} - 1. \tag{3}$$

Reacomodemos estos bloques. De manera informal, ponemos los bloques 1 a K, donde el primer bloque corresponde al primer dígito; el segundo bloque, a los siguientes cuatro dígitos; el tercer bloque, a los siguientes nueve y así sucesivamente hasta los últimos K^2 dígitos (de derecha a izquierda) y dejamos tres espacios entre bloques consecutivos. Ponemos un 1 en el segundo espacio de derecha a izquierda del K-ésimo bloque. Este 1 es el dígito principal de nuestro nuevo número y nos da información precisa sobre su tamaño. Por ejemplo, supongamos que obtuvimos el número 0.10101010111010 al redondear alguno de los $\alpha\phi_p$. Al cortarlo se obtienen los bloques

$$\Delta_1 = 1, \Delta_2 = 0101, \Delta_3 = 010111010$$

y después de agregar los tres ceros y el 1 nos queda

$$\mathbf{10}0101110\mathbf{000}0101\mathbf{000}1$$

donde los números en negritas corresponden a los dígitos que insertamos entre bloques consecutivos. Formalmente, si escribimos $t_p := 2^{K_p^2+3K_p+2}$, tenemos el número

$$a_p := \sum_{i=1}^{K_p} \Delta_{ip} 2^{(i-1)^2+3i} + t_p.$$

Sea $\mathcal{A}_\alpha := \cup_{p\in\mathbb{P}}\{a_p\}$. Por la elección de K, como $2^{K_p^2+3K_p+2} < a_p < 2^{K_p^2+3K_p+3}$ observamos que $a_p = p^{\beta+o(1)}$. Veamos cuál es la razón de introducir los bloques de ceros. Consideramos la identidad en números binarios

$$1000\mathbf{0}11 + 100\mathbf{0}10 = 111\mathbf{0}11 + 101\mathbf{0}10$$

donde los cuatro números tienen en la misma posición al dígito 0 que escribimos como en negritas. Al sumar estos números, observemos que el **0** previene de 'llevar' unos a los otros bloques, de manera que en cierto sentido los bloques $1000, 100, 111, 101$ correspondientes a los últimos cuatro dígitos de cada número (de derecha a izquierda) contribuyen a la suma en cada lado de la ecuación de manera independiente que los números que están al otro lado del **0**. De acuerdo con este argumento, deberíamos tener que $1000 + 100 = 111 + 101$ y $11 + 10 = 11 + 10$ lo cual es cierto. El hecho de que la suma sea independiente por bloques nos ayuda a contar el número de veces que la ecuación $x+y = z+w$ tiene soluciones en $\mathcal{A}_\alpha$.

Definición 3. Consideramos el conjunto $\mathcal{A}_\alpha$, para una elección fija de α. Sean $a_p, a_q, a_r, a_s \in \mathcal{A}_\alpha$ con $p, q, r, s \in \mathbb{P}$ tales que

$$a_p + a_q = a_r + a_s \tag{4}$$

con

$$a_p > a_r \geq a_s > a_q. \tag{5}$$

Decimos que la cuádrupla $(p, q, r, s) \in \mathbb{P}^4$ es una *cuádrupla mala*.

La desigualdad (5) es una consecuencia de (4) si asumimos que a_p es máx$\{a_p, a_q, a_r, a_s\}$.

Si tenemos una cuádrupla mala podemos remover el a_i correspondiente al mayor elemento de esta cuádrupla. Haciendo esto para todas las cuádruplas malas, los restantes elementos de $\mathcal{A}_\alpha$ forman un conjunto de Sidon. Nos interesa estimar entonces el número de cuádruplas malas.

La manera en que se construyen los elementos de $\mathcal{A}_\alpha$ ayuda a contar el número de cuádruplas malas.

Lema 4. *(p, q, r, s) es una cuádrupla mala si y solamente si $\Delta_{ip} + \Delta_{iq} = \Delta_{ir} + \Delta_{is}$ para todo i y $t_p + t_q = t_r + t_s$.*

Demostración. Supongamos que las condiciones (4) y (5) se cumplen (el regreso es inmediato de la definición de los a_i). Supongamos entonces que

$$a_p + a_q = a_r + a_s.$$

Como

$$2^{K_p^2+3K_p+2} > \sum_{i=1}^{K_p} \Delta_{ip} 2^{(i-1)^2+3i}$$

y análogamente para q, r, s, la contribución de t_p, t_q, t_r, t_s es independiente de los dígitos restantes de a_p, a_q, a_r, a_s respectivamente, entonces

$$t_p + t_q = t_r + t_s.$$

De (5) se sigue que existen K y L tales que $K_p = K_r = K$ y $K_q = K_s = L$ con $K \geq L$. Aún tenemos que decir algo sobre

$$\sum_{i=1}^{K} \Delta_{ip} 2^{(i-1)^2+3i} + \sum_{i=1}^{L} \Delta_{iq} 2^{(i-1)^2+3i} = \sum_{i=1}^{K} \Delta_{ir} 2^{(i-1)^2+3i} + \sum_{i=1}^{L} \Delta_{is} 2^{(i-1)^2+3i}$$

pero como

$$2^{i^2+3(i+1)} > \sum_{j=1}^{i} \Delta_{ip} 2^{(j-1)^2+3j}$$

y análogamente para q, r, s, vemos que para $i < L$,

$$\sum_{j=1}^{i}(\Delta_{jp} + \Delta_{jq})2^{(j-1)^2+3j} = \sum_{j=1}^{i}(\Delta_{jr} + \Delta_{js})2^{(j-1)^2+3j}$$

y como los términos entre paréntesis no afectan a la otra parte de la suma ya que su suma total es $\leq 2^{2j+1} - 2$, por (3) tenemos que

$$\Delta_{ip} + \Delta_{iq} = \Delta_{ir} + \Delta_{is}.$$

Como para $i > L$ se tiene que $\Delta_{iq}, \Delta_{is} = 0$ se sigue la afirmación. ☑

En la demostración del lema anterior, probamos un resultado útil en términos de los t_p's. Esto nos ayudará a contar el número de cuádruplas malas. Para el lema siguiente, recordemos que $m_p = \left\lfloor 2^{K^2}\alpha\phi_p \right\rfloor$.

Lema 5. *Tenemos que*

$$m_p + m_q = m_r + m_s.$$

Demostración. La primera afirmación se sigue del lema anterior. La segunda afirmación es inmediata por la identidad correspondiente a los bloques que también se probó en el lema anterior. ☑

Buscamos condiciones necesarias sobre las cuádruplas malas (p, q, r, s). Para el siguiente lema, utilizamos el hecho que $\phi_p + \phi_q = \phi_{pq}$.

Lema 6. *Si (p, q, r, s) es una cuádrupla mala, con K y L como antes, entonces*

$$|\phi_{p\overline{r}} - \phi_{s\overline{q}}| < 4 \cdot 2^{-L^2}, \tag{6}$$

$$(K-1)^2 + (L-1)^2 > \beta(L^2 - 5), \tag{7}$$

$$(K-1)^2 + (L-1)^2 > \beta(L-1)^2. \tag{8}$$

Demostración. Sean $\rho_p, \rho_q, \rho_r, \rho_s$ los primos gaussianos con normas $\sqrt{p}, \sqrt{q}$, $\sqrt{r}, \sqrt{s}$ respectivamente. Como $e^{2\pi i\phi_j} = \frac{\overline{\rho_j}}{\rho_j}$, tenemos

$$\begin{aligned}\left|\frac{\overline{\rho_p}\rho_r}{\rho_p\overline{\rho_r}} - \frac{\overline{\rho_s}\rho_q}{\rho_s\overline{\rho_q}}\right| &= \left|\frac{\overline{\rho_p}\ \overline{\rho_s}\rho_r\rho_q - \overline{\rho_r}\ \overline{\rho_q}\rho_p\rho_s}{\rho_p\rho_q\rho_r\rho_s}\right| \\ &\geq \frac{1}{\sqrt{pqrs}}.\end{aligned}$$

Por otro lado,

$$\begin{aligned}\left|\frac{\overline{\rho_p\rho_q}}{\rho_p\rho_q}-\frac{\overline{\rho_r\rho_s}}{\rho_r\rho_s}\right| &= \left|e^{2\pi i(\phi_p+\phi_q)}-e^{2\pi i(\phi_r+\phi_s)}\right| \\ &= \left|1-e^{2\pi i(\phi_p+\phi_q-\phi_r-\phi_s)}\right| \\ &\leq 2\pi\left|\phi_p+\phi_q-\phi_r-\phi_s\right| \\ &< 8\left|\phi_p+\phi_q-\phi_r-\phi_s\right|.\end{aligned}$$

De la definición de los m_i y la desigualdad del triángulo se tiene

$$\alpha\left|\phi_{p\overline{r}}-\phi_{s\overline{q}}\right| < \left|\alpha\phi_p-m_p\right|+\left|\alpha\phi_{\overline{q}}-m_q\right|+\left|\alpha\phi_{\overline{r}}-m_r\right|+\left|\alpha\phi_s-m_s\right| < 4\cdot 2^{-L^2}. \quad (9)$$

Como $\alpha \geq 1$, combinando las desigualdades anteriores obtenemos

$$\frac{1}{\sqrt{pqrs}} < 32\cdot 2^{-L^2}$$

lo que implica

$$2^{L^2-5} < \sqrt{pqrs} < 2^{\frac{(K-1)^2+(L-1)^2}{\beta}}.$$

La tercera desigualdad buscada se sigue de esta para L suficientemente grande. ☑

Para $\rho_q\overline{\rho_s}$ dados, contaremos los pares (p,r) tales que (6) se cumpla. A cada $z \in \mathbb{Z}[i]$ con $z = a+ib$ y $a,b \in \mathbb{Z}$ le asociamos el punto de coordenadas enteras $(a,b) \in \mathbb{R}^2$. Decimos entonces que (a,b) es un punto de coordenadas enteras.

Lema 7. *Sea $z_0 \in \mathbb{R}^2$. Sea $\mathcal{C}$ el círculo con centro z_0 y radio R. El número n de puntos de coordenadas enteras en un sector circular de $\mathcal{C}$ de ángulo θ que corresponden a los elementos de $\mathbb{Z}[i]$ $\{w_1, w_2, \ldots, w_n\}$ tal que para $i = 1, \ldots, n$, $w_i = \rho_{p_i}\overline{\rho_{r_i}}$ para algunos $p_i, r_i \in P_K$ es menor que $\theta R^2 + 1$.*

Demostración. Consideramos el segmento que une z_0 y un punto w_i. Observemos que este segmento no contiene un tercer punto w_j; de ser así, tendríamos que el argumento de w_i es igual al argumento de w_j y por tanto

$$\phi_{p_i} - \phi_{r_i} = \phi_{p_j} - \phi_{r_j}.$$

Pero $\{\phi_{p_i}, \phi_{r_i}\} \neq \{\phi_{p_j}, \phi_{r_j}\}$, esto debido a nuestra observación previa de que el conjunto de argumentos de los primos gaussianos es un conjunto de Sidon. Entonces es posible enumerar los puntos en sentido trigonométrico. Ahora consideramos los triángulos con vértices z_0, w_i y w_{i+1} para $i = 1, \ldots, n-1$. Este es un conjunto de triángulos ajenos y el área total cubierta por ellos es menor que el área del sector circular, que está dada por $\frac{\theta}{2}R^2$. Como todos los triángulos

tienen puntos de coordenadas enteras como vértices, tenemos que el área de cada triángulo es al menos $\frac{1}{2}$ y como tenemos $n-1$ triángulos obtenemos

$$\frac{n-1}{2} \leq \frac{\theta}{2}R^2,$$

de donde se sigue la desigualdad buscada para n. ☑

Consideremos el conjunto

$$\mathcal{A}_{KL} := \{p, r \in P_K, \quad q, s \in P_L, \quad p \neq r, \quad q \neq s : (p, q, r, s) \quad \text{es mala}\}$$

y sea $|\mathcal{A}_{KL}| := A_{KL}$. En el lema siguiente obtendremos una estimación para el número de cuádruplas malas.

Lema 8. *El número de cuádruplas malas es*

$$A_{KL} \ll 2^{\frac{2}{\beta}((K-1)^2+(L-1)^2)-L^2}.$$

Demostración. Para q, s dados, basta contar el número de pares (p, r) con p, r como arriba tal que se tenga la desigualdad del lema anterior. Como $pr < 2^{\frac{2(K-1)^2}{\beta}}$ tenemos que la norma de los puntos de coordenadas enteras que nos interesan es menor que $2^{\frac{(K-1)^2}{\beta}}$. Hacemos $R = 2^{\frac{(K-1)^2}{\beta}}$ y $\theta = 4 \cdot 2^{-L^2}$ y consideramos valores de z_0 correspondientes a enteros gaussianos de la forma $\rho_r\overline{\rho_p}$ con $p, r \in P_K$. Tenemos, por el lema anterior, que para q, s dados, el número de pares (p, r) que nos interesan es a lo más $2^{\frac{2}{\beta}(K-1)^2-L^2+2} + 1 \ll 2^{\frac{2}{\beta}(K-1)^2-L^2+2}$ pues

$$\begin{aligned}(K-1)^2 + (L-1)^2 &> \beta(L^2-5)\\ (K-1)^2 &> (\beta-1)L^2 - 5\beta\\ \frac{2}{\beta}(K-1)^2 &> \frac{2}{\beta}(\beta-1)L^2 - 10\\ &\gg L^2 - 10\end{aligned}$$

por la elección de β, para L suficientemente grande. Como tenemos $2^{\frac{2}{\beta}(L-1)^2}$ posibilidades para los pares (q, s) se sigue que

$$A_{KL} \ll 2^{\frac{2}{\beta}((K-1)^2+(L-1)^2)-L^2}$$

lo que concluye la prueba. ☑

4. El argumento probabilístico

Hasta este momento, el parámetro α no ha sido relevante para los lemas que hemos probado. La cota que obtuvimos para el número de cuádruplas malas no es muy buena para valores pequeños de L. Utilizaremos el parámetro α para solucionar este problema.

Lema 9. *Sea (p,q,r,s) una cuádrupla mala. Entonces*

$$m_p \equiv m_r \mod 2^{K^2-L^2}. \tag{10}$$

Demostración. Sabemos que $\Delta_{ip} + \Delta_{iq} = \Delta_{ir} + \Delta_{is}$. Para $L < i < K$ se tiene que $\Delta_{iq} = \Delta_{is} = 0$, por tanto, $\Delta_{ip} = \Delta_{ir}$. Recordando la construcción de los bloques Δ_{ip} y Δ_{ir}, de los dígitos de m_p y m_r se tiene que los dígitos correspondientes en la expansión binaria de estos dos números coinciden a partir de la posición $L+1$ (de derecha a izquierda). ☑

Sea μ la medida de Lebesgue sobre $\mathbb{R}$. Veremos cómo evadir las cuádruplas malas con una elección apropiada de α.

Lema 10. *Supongamos que $K > L$. Sean $p, r \in P_K$ tales que existe al menos un par $q, s \in P_L$ y un α que satisfacen* (4)*. Entonces*

$$\mu\{\alpha \in [1,2) : (10) \text{ se cumple}\} \ll 2^{L^2-K^2}.$$

Demostración. Recordemos que $[x]-[y] = [x-y]+0$ ó -1. Tenemos entonces que

$$\Big\lfloor 2^{K^2}\alpha(\phi_p - \phi_r)\Big\rfloor \equiv 0, 1 \mod 2^{K^2-L^2}.$$

Ponemos $M := 2^{K^2-L^2}$ y $N := \big\lfloor 2^{K^2}(\phi_p - \phi_r)\big\rfloor$. La congruencia anterior se traduce en $\alpha N = MQ + x$, donde Q es un entero y $x \in (-1,1)$. Fijando Q, los α que se pueden escribir de esta manera están entonces contenidos en un intervalo de tamaño $\frac{2}{N}$. Por otra parte, $Q < \frac{2N}{M} + 1$ pues $\alpha < 2$. Entonces

$$\mu\{\alpha \in [1,2) : (10) \text{ se cumple}\} \ll \frac{2}{N}\left(1 + \frac{N}{M}\right).$$

Basta probar que $N \gg M$. Por (9) se tiene que

$$\big|\phi_p - \phi_r\big| = \big|\phi_s - \phi_q\big| + O\Big(2^{-L^2}\Big).$$

Se sigue de $q^\beta, s^\beta < 2^{(L-1)^2}$ y la desigualdad $|e^z - 1| \leq 2|z|$, para $|z| \leq 1$, que

$$\begin{aligned}\left|\phi_q - \phi_s\right| &= \frac{1}{\pi}\left|\log \frac{\overline{\rho_q}\rho_s}{\overline{\rho_s}\rho_q}\right| \\ &\geq \frac{1}{2\pi}\left|1 - \frac{\overline{\rho_q}\rho_s}{\rho_q\overline{\rho_s}}\right| \\ &= \frac{1}{2\pi}\left|\frac{\overline{\rho_q}\rho_s - \overline{\rho_s}\rho_q}{\rho_q\overline{\rho_s}}\right| \\ &\gg 2^{-\frac{L^2}{\beta}}.\end{aligned}$$

Tenemos entonces que

$$N \gg 2^{K^2 - \frac{L^2}{\beta}}$$

y por tanto

$$N \gg 2^{K^2 - \frac{1}{\beta}L^2} > M.$$

Luego, $\frac{2}{B}\left(1 + \frac{N}{M}\right) \ll \frac{1}{N}\frac{N}{M} = \frac{1}{M}$, lo que concluye la prueba. ☑

Esta nueva cota es buena en el sentido que no demasiados α's contribuyen a completar cuádruplas malas para un par p, r dado cuando L es pequeño. Por otro lado, nuestra cota anterior para el número de cuádruplas malas no es buena cuando L es pequeño, pero es muy buena cuando L está cerca de K. Este hecho nos sugiere que debemos combinar ambas cotas de alguna manera para que en promedio se compensen. Sea

$$T_{KL}(\alpha) = \#\{p, q, r, s : p, r \in P_K,\ r, s, \in P_L,\ p \neq r,\ q \neq s,\ a_p + a_q = a_r + a_s\}.$$

Lema 11. *Para $L \leq K$ tenemos*

$$\int_1^2 T_{KL}(\alpha)\, d\alpha \ll 2^{\frac{2}{\beta}((K-1)^2 + (L-1)^2) - K^2}.$$

Demostración. Escribimos $m = \mu\{\alpha \in [1, 2) : (4) \text{ se cumple}\}$. Como $m = 0$ cuando (6) no se cumple y $\ll 2^{L^2 - K^2}$ en otro caso, sumando sobre los posibles valores de p, q, r, s se obtiene

$$\int_1^2 T_{KL}(\alpha)\, d\alpha \ll 2^{L^2 - K^2} A_{KL}$$

de donde se sigue la desigualdad buscada sustituyendo la cota para A_{KL}. ☑

Definimos $T_K(\alpha) := \#\{p, q, r, s : p, r \in P_K,\ (4) \text{ y } (5) \text{ se cumplen}\}$. De la definición es inmediato que $T_K(\alpha) = \sum_{L \geq K} T_{KL}(\alpha)$.

Lema 12. *Se tiene la estimación siguiente*

$$\int_1^2 T_K(\alpha)\,d\alpha \ll 2^{\frac{1}{\beta}(K-1)^2-2K}.$$

Demostración. Como $T_{KL}(\alpha) \neq 0$ es posible solamente si $(K-1)^2+(L-1)^2 > \beta(L-1)^2$,

$$\begin{aligned}\int_1^2 T_K(\alpha)\,d\alpha &= \sum_{L\leq K}\int_1^2 T_{KL}(\alpha)\,d\alpha\\ &= \sum_{L\in\mathcal{L}}\int_1^2 T_{KL}(\alpha)\,d\alpha\\ &\ll 2^{\frac{2}{\beta}(K-1)^2-K^2}\sum_{L\in\mathcal{L}} 2^{\frac{2(L-1)^2}{\beta}}\\ &\ll 2^C\end{aligned}$$

donde

$$\begin{aligned}C &= \frac{2(K-1)^2}{\beta} - K^2 + \frac{2(K-1)^2}{\beta(\beta-1)}\\ &= \frac{2}{\beta-1}(K-1)^2 - K^2\\ &= \frac{2}{\beta-1}K^2 - \frac{4}{\beta-1}K + \frac{2}{\beta-1}.\end{aligned}$$

De esto se obtiene que el coeficiente principal de la expresión anterior es

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

por la elección de β. Además, el coeficiente lineal es $-\frac{4}{\beta-1} = -2 - \frac{2}{\beta} < -2$. Se tiene entonces que

$$C < \frac{1}{\beta}(K-1)^2 - 2K,$$

lo que concluye la prueba. ☑

Teorema 13. *(Ruzsa, 1998) Existe un conjunto de Sidon infinito $\mathcal{S}$ tal que la función de conteo $S(x)$ satisface*

$$S(x) = x^{\frac{1}{\beta}+o(1)}$$

para $\beta = \sqrt{2}+1$.

Demostración. De la estimación anterior, obtenemos que

$$\sum_K 2^{-(\frac{1}{\beta}(K-1)^2-K)} \int_1^2 T_K(\alpha)\, d\alpha \ll \sum_K 2^{-K}$$

de donde se sigue

$$\int_1^2 \sum_K T_K(\alpha) 2^{-(\frac{1}{\beta}(K-1)^2-K)}\, d\alpha < +\infty.$$

Sea $f(\alpha) = \sum_K T_K(\alpha) 2^{-\frac{1}{\beta}(K-1)^2-K}$. Como $\int_1^2 f(\alpha) d\alpha < +\infty$, para casi todo α, $f(\alpha)$ es finito, i.e. $T_K(\alpha) \ll 2^{\frac{1}{\beta}(K-1)^2-K}$ para K suficientemente grande, (dependiendo de α). Tomamos uno de estos α. Sea $\pi_1(x)$ la cantidad de números primos menores que x que son congruentes a 1 módulo 4. La cardinalidad de P_K está dada por el teorema de Dirichlet:

$$\big|P_K\big| = \pi_1\Big(2^{\frac{(K-1)^2}{\beta}}\Big) - \pi_1\Big(2^{\frac{(K-2)^2}{\beta}}\Big) \sim \frac{2^{\frac{(K-1)^2}{\beta}}}{2(K-1)^2\beta\log 2}.$$

Entonces, para K suficientemente grande, $T_K(\alpha) < \frac{|P_K|}{2}$. Esto significa que si omitimos el elemento más grande de las cuádruplas malas, lo que nos queda tiene cardinalidad mayor que $\frac{|P_K|}{2}$. Si denotamos con Q_K el conjunto de los elementos restantes y tomamos $\mathcal{S}$ como la unión de los conjuntos Q_K entonces $\mathcal{S}$ es un conjunto de Sidon.

Sea $S(x)$ la función de conteo de $\mathcal{S}$. Como $a_p < 2^{(K-1)^2+3(K-1)+2} < 2^{(K+1)^2}$ para $K = \left\lfloor \sqrt{\frac{\log x}{\log 2}} - 2 \right\rfloor$ el conjunto Q_K consiste de enteros menores que x, de donde se sigue que $S(x) \gg \pi_1(2^{\frac{1}{\beta}(K-1)^2}) = x^{\frac{1}{\beta}+o(1)}$. Como también tenemos

$$a_p > 2^{(K-1)^2+3(K-1)+1} > 2^{K^2},$$

tomando $K = \left\lfloor \sqrt{\frac{\log x}{\log 2}} - 1 \right\rfloor$, el conjunto Q_K tiene elementos mayores que x y entonces $S(x) \ll \pi_1\Big(2^{\frac{1}{\beta}K^2}\Big) = x^{\frac{1}{\beta}+o(1)}$. De estas estimaciones se sigue el teorema. ☑

Nuestra construcción está completamente basada en las ideas de Ruzsa. Las simplificaciones técnicas que aporta la simplificación sugerida por Cilleruelo y Ruzsa nos permite apreciar mejor su trabajo.

Agradecimiento. Este trabajo fue escrito bajo la supervisión del Dr. Javier Cilleruelo (Universidad Autónoma de Madrid) durante el DocCourse 2008 in

Additive Combinatorics, que se llevó a cabo en el Centre de Recerca Matematica, Universidad Autónoma de Barcelona como parte de la tesis de maestría del autor. El autor agradece al CRM por su hospitalidad y su ambiente estimulante. Los comentarios del referee anónimo contribuyeron a mejorar este trabajo. Gracias igualmente a Florian Luca, Eugenio Balanzario y Garaev Moubariz por la lectura cuidadosa y sus comentarios.

Referencias

[1] Javier Cilleruelo and Imre Ruzsa, *Real and -padic sidon sequences*, Acta Sci. Math (Szeged) **70** (2004), 505–510.

[2] Kevin O'Bryant, *A Complete Annotated Bibliography of Work Related to Sidon Sequences*, Electronic Journal of Combinatorics (2004).

[3] Imre Ruzsa, *An Infinite Sidon Set*, Journal of Number Theory (1998), 63–71.

[4] Simon Sidon, *Ein Satz Über Trigonometrische Polynome und Seine Anwendungen in der Theorie der Fourier-Reihen*, Math. Annalen **106** (1932), 536–539 (ge).

(Recibido en junio de 2010. Aceptado en septiembre de 2011)

Equipe Combinatoire et Optimisation, Faculté de Mathématiques
Université Pierre et Marie Curie - Paris 6
Tour 15-16 1er etage, 4 Place Jussieu; 75005
Paris, Francia
e-mail: maldonadolo@math.jussieu.fr