Universidad Nacional Autónoma de México

y

Universidad Michoacana de San Nicolás de Hidalgo

Posgrado Conjunto en Ciencias Matemáticas
UNAM-UMSNH

Un conjunto de Sidon infinito

T E S I S

Que para obtener el grado de Maestro en Ciencias Matemáticas
Presenta:

Juan Pablo Maldonado López

Director: Dr. Florian Luca

Morelia, Michoacán - 27 de febrero de 2010.

Índice general

Agradecimientos

A mi familia, por su apoyo constante.

Agradezco a los sinodales por su revisión cuidadosa, sugerencias y críticas y a Javier Cilleruelo, el asesor no oficial de esta tesis.

Estoy agradecido con los profesores del IFM, la UNAM y Fismat por su amistad y su ejemplo (o contraejemplo). Mis alumnos de Fismat me enseñaron mucho durante este tiempo, con su energía y entusiasmo. Gracias a todos ellos.

Imposible olvidar a *las chicas del cubo*. Gracias por su alegría y su tolerancia ante mi descarada y exageradamente larga invasión de su territorio.

A Ahtziri, por este largo tiempo en el que convivimos mucho, peleamos mucho, pero sobre todo aprendimos mucho el uno del otro, dentro y fuera de las matemáticas. Gracias por esta amistad tan extraña y especial.

También a Marcos, por convencerme de que me fuera a Barcelona y por estar siempre ahí para una cerveza (o las necesarias). A Javier, mi confesor oficial y psicoterapeuta de tiempo completo.

A Carlos Mendoza, por alegrarme el día con sus correos cuando estuve en Europa. Ya fue hermoso que nos hayamos entendido por tanto tiempo.

Y, *last but not least*, a Brenda y su adicción a cocinar para todos. Gracias a ella y a quienes nos acompañaron en las distintas convivencias y viajes por hacer agradable mi tiempo en Morelia dentro y fuera de la Universidad.

Introducción

Un conjunto de enteros positivos $\mathcal{S}$ es un *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 (ver [**7**]), quien llamó la atención de Paul Erdős sobre estos conjuntos y desde entonces han sido de particular interés en teoría de números y combinatoria.

Estamos interesados en la cardinalidad del mayor conjunto de Sidon contenido en el intervalo $[1, x]$. Para un conjunto $\mathcal{S}$ de enteros positivos, la función de conteo del conjunto $\mathcal{S}$ es $S(x) := \#\mathcal{S} \cap [1, x]$. Se sabe que si $\mathcal{S}$ es un conjunto de Sidon, $S(x) \sim \sqrt{x}$. Una buena referencia sobre este y otros resultados sobre conjuntos de Sidon es [**5**].

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. I. Ruzsa construyó un conjunto de Sidon con función de conteo $x^{\sqrt{2}-1+o(1)}$, mientras x tiende al infinito [1] en [**6**]. 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, construiremos un conjunto de Sidon con la misma función de conteo. Consideramos los argumentos de los primos gaussianos (los primos en $[i]$) no reales. Esta sucesión es acotada, lo que simplifica la construcción. 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 el capítulo siguiente introducimos los enteros gaussianos y algunas de sus propiedades. En el tercer capítulo damos una cota superior para $S(x)$ debida a Erdős y Turán en [**2**]. En el capítulo 4, discutimos la construcción de un conjunto de Sidon para el caso finito, a fin de motivar la construcción para el caso infinito y en el capítulo restante explicamos la construcción del conjunto de Sidon infinito. Esta construcción está completamente basada en las ideas de Ruzsa y nuestro trabajo es una pequeña variante de su idea.

[1] $o(1)$ es una función que tiende a 0 cuando x tiende al infinito.

A pesar de su apariencia abstracta y obscura, el problema de la construcción de conjuntos de Sidon es importante en las aplicaciones. Los conjuntos de Sidon fueron bautizados en ingeniería con el nombre de *reglas de Golomb*. Una regla de Golomb es una regla con marcas de manera que las distancias entre dos marcas son distintas. El conjunto de distancias de un extremo de la regla a las marcas es un conjunto de Sidon. Las reglas de Golomb se utilizan en problemas relacionados con transferencia de señales [**1**].

En general, no se sabe mucho de conjuntos de Sidon infinitos. El problema de encontrar un subconjunto infinito *grande* de 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. Las mejores cotas que se conocen se deben a Ben Green [**3**].

Utilizamos la notación usual y escribimos $\lfloor y \rfloor$ para el mayor entero menor o igual que y y $\{y\} = y - \lfloor y \rfloor$ y seguimos la notación de Landau, escribiendo $f(x) = o(g(x))$ si $\frac{f(x)}{g(x)} \to 0$ cuando $x \to \infty$ y $f(x) = O(g(x))$ si $\lim_{x\to\infty} \frac{f(x)}{g(x)} < +\infty$. Tambien utilizaremos el símbolo de Legendre $\left(\frac{a}{p}\right)$ donde p es primo como

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{a} \equiv 0 \mod p \\ +1, & \text{a} \equiv x^2 \mod p \text{ para algún } x \in /p \\ -1, & \text{en otro caso.} \end{cases}$$

Capítulo 1

Los enteros gaussianos

Los enteros gaussianos son el conjunto

$$[i] := \{z \in : z = a + ib, a, b \in\}$$

llamados así en honor de K.F. Gauss. En este capítulo hablaremos de las propiedades básicas, entre ellas la noción de primalidad y la factorización única.

1. Propiedades básicas

Este conjunto hereda las operaciones de suma y producto de . Al igual que en los enteros usuales, el cociente de dos enteros gaussianos no es necesariamente un entero gaussiano, como muestra el ejemplo siguiente

$$\frac{3+2i}{1-6i} = \frac{3+2i}{1-6i} \cdot \frac{1+6i}{1+6i} = \frac{-9}{37} + \frac{20i}{37}.$$

Tiene sentido entonces la definición siguiente.

Sean $a + bi$ y $c + di$ enteros gaussianos. Decimos que $a + bi$ divide a $c + di$ si existe un entero gaussiano $e + fi$ tal que

$$c + di = (a + bi)(e + fi).$$

Cuando $a + bi$ y $c + di$ son enteros ordinarios, se trata de la divisibilidad usual. Para los enteros, el teorema fundamental de la aritmética nos dice que cualquier entero se escribe de manera esencialmente única como producto de números primos. Por *esencialmente única* entendemos dos cosas: salvo permutaciones y salvo factores ± 1. Los números ± 1 son los únicos enteros que tienen inversos multiplicativos. Al escribir un entero N como el producto de primos $p_1, p_2, \ldots p_k$, vemos que también podemos escribirlo como $(-p_1)p_2 \ldots (-p_i) \ldots p_k$. Estas dos descomposiciones las consideramos como equivalentes. Para poder enunciar un teorema de factorización única en los enteros

gaussianos necesitamos describir a los primos pero también a aquellos elementos con inverso multiplicativo. Estos elementos se llaman *unidades*.

Describiremos a las unidades en $[i]$. Para esto introducimos la noción de norma.

Sea $x + yi$ un entero gaussiano. Decimos que la *norma* de $x + yi$ es $x^2 + y^2$ y lo denotamos por

$$N(x + iy) = x^2 + y^2.$$

La definición de norma es simplemente el cuadrado del valor absoluto usual en .

LEMA 1.1. *Sean α, β enteros gaussianos. La norma satisface*

i) $N(\alpha) = 0 \iff \alpha = 0$;
ii) $N(\alpha\beta) = N(\alpha)N(\beta)$.

DEMOSTRACIÓN. Trivial a partir de la observación anterior.

Una consecuencia de este lema es que el producto de enteros gaussianos distintos de cero es distinto de cero.

Ahora estamos listos para caracterizar las unidades.

LEMA 1.2. *Las unidades de $[i]$ son $1, -1, i, -i$*

DEMOSTRACIÓN. Sea $a + bi$ una unidad. Esto es, existe $c + di$ tal que

$$(a + bi)(c + di) = 1.$$

Tomando norma de ambos lados y usando la propiedad *ii*) del lema anterior,

$$(a^2 + b^2)(c^2 + d^2) = 1.$$

De aquí obtenemos

$$a^2 + b^2 = c^2 + d^2 = 1,$$

pero a, b, c, d son enteros. A partir de aquí es fácil verificar que las únicas soluciones son las que se proponen.

Una consecuencia útil es el hecho de que un entero gaussiano α es una unidad si y solamente si su norma es 1.

2. Los primos gaussianos

De manera análoga a lo que sucede en los enteros, decimos que un entero gaussiano es primo si no puede escribirse como producto de dos enteros gaussianos tales que ninguno de ellos sea una unidad.

Observemos que si $\gamma \in [i]$ es tal que $N(\gamma)$ es un número primo, entonces γ mismo debe ser un primo en los enteros gaussianos de acuerdo a la definición. Si no lo fuera, existirían α, β enteros gaussianos tales que

$$\gamma = \alpha\beta,$$

y por tanto

$$N(\gamma) = N(\alpha)N(\beta),$$

pero esto es imposible si $N(\gamma)$ es primo y ninguno de α, β es una unidad.

El siguiente teorema, cuya demostración puede encontrarse en muchos libros de teoría de números, nos será útil para caracterizar los primos gaussianos.

Teorema 1.3. *Sea p un primo de la forma $4m + 1$. Existen enteros únicos u, v tales que $p = u^2 + v^2$. Además, u y v si $u > |v| > 0$.*

Tenemos una descripción completa de los primos gaussianos en el siguiente teorema.

Teorema 1.4. ***Clasificación de los primos gaussianos:*** *Los primos gaussianos, son, hasta unidades, de uno de estos tipos*

i) $1 + i$ *es un primo gaussiano.*
ii) *Sea p un primo ordinario. Si $p \equiv 3 \mod 4$ entonces p es un primo gaussiano.*
iii) *Sea p un primo ordinario tal que $p \equiv 1 \mod 4$. Escribimos p como la suma de dos cuadrados, $p = u^2 + v^2$. Entonces $u + vi$ es un primo gaussiano.*

Demostración. Primero veamos que todos los números de la lista anterior son primos gaussianos. De acuerdo a una observación previa, es inmediato que $1 + i$ es primo pues su norma es 2. Veamos qué pasa con los números del tipo *ii*). Sea p un primo ordinario tal que $p \equiv 3 \mod 4$. Supongamos

que p se puede escribir como $(a+bi)(c+di)$, donde ninguno de los factores es una unidad. Entonces, tomando normas,

$$p^2 = (a^2 + b^2)(c^2 + d^2).$$

Para que esta ecuación tenga soluciones enteras no triviales, necesariamente tiene que pasar que

$$a^2 + b^2 = p,\ c^2 + d^2 = p,$$

lo cual es imposible porque si reducimos ambas ecuaciones módulo 4, el lado izquierdo es $0, 1, 2$. Entonces p no puede ser factorizado en los enteros gaussianos. Para los primos del tipo *iii*), utilizamos el teorema (1.3). Falta probar que todo primo gaussiano es de alguno de estos tres tipos. Para probar esto, utilizaremos el lema siguiente.

Lema 1.5. *Sea $\alpha = a + bi \in [i]$.*

a) *Si 2 divide a $N(\alpha)$, entonces $1 + i$ divide a α.*
b) *Sea p un primo del tipo ii). Supongamos que p divide a $N(\alpha)$ dentro de los enteros ordinarios. Entonces p divide a α dentro de los enteros gaussianos.*
c) *Sea $u + vi$ un primo gaussiano del tipo iii) y sea $u - vi$ su conjugado (dentro de los números complejos). Si p divide a $N(\alpha)$ dentro de los enteros ordinarios, entonces al menos uno de $u + vi$ y $u - vi$ divide a α dentro de los enteros gaussianos.*

Demostración. Empecemos con *a*). Como 2 divide a $N(\alpha) = a^2 + b^2$, entonces a, b tienen la misma paridad. Esto nos dice que $a + b$ y $-a + b$ son ambos pares también, de donde el cociente

$$\frac{a + bi}{1 + i} = \frac{(a + b) + (-a + b)i}{2}$$

es un entero gaussiano. Entonces α es divisible por $1 + i$. Para la parte *b*), si p divide a a y a b, entonces no hay nada que probar. Supongamos que no. Esto nos dice que

$$a^2 \equiv -b^2 \mod p,$$

de donde, calculando el símbolo de Legendre,

$$\left(\frac{a}{p}\right)^2 = \left(\frac{a^2}{p}\right) = \left(\frac{-b^2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{b}{p}\right)^2.$$

Como $p \equiv 3 \mod 4$, tenemos que $\left(\frac{-1}{p}\right) = -1$ y de aquí

$$\left(\frac{a}{p}\right)^2 = -\left(\frac{b}{p}\right)^2,$$

que es una contradicción. Luego entonces, p divide a a y a b.

Para el caso c), tenemos que

$$N(\alpha) = a^2 + b^2 = pK$$

donde $K \geq 1$ es un entero. Tenemos que probar que alguno de los dos números

$$\frac{(au + bv) + (-av + bu)i}{p} \quad \text{o} \quad \frac{(au - bv) + (av + bu)i}{p} \tag{2.1}$$

son enteros gaussianos. Para esto, observemos que

$$(au + bv)(au - bv) = a^2u^2 - b^2v^2 = a^2u^2 - b^2(p - u^2) = (a^2 + b^2)u^2 - pb^2 = pKu^2 - pb^2$$

de aquí deducimos que al menos uno de $au + bv$ y $av + bu$ es múltiplo de p. Una cuenta similar nos dice que

$$(-av + bu)(av + bu) = pKu^2 - pb^2,$$

de donde al menos uno de $-av + bu$ y $av + bu$ es múltiplo de p. Tenemos entonces cuatro casos a considerar

1. $au + bv$ y $-av + bu$ son múltiplos de p.
2. $au + bv$ y $av + bu$ son múltiplos de p.
3. $au - bv$ y $-av + bu$ son múltiplos de p.
4. $au - bv$ y $av + bu$ son múltiplos de p.

El caso 1 es trivial pues implica que el primer cociente que escribimos en (2.1) es entero. De la misma manera, el segundo cociente que escribimos es entero en el caso 4. Para los casos 2 y 3, debemos trabajar un poco más. Consideremos el caso 2. (el caso 3. es análogo). Tenemos que p divide tanto a $au + bv$ como a $av + bu$, de donde p divide a

$$(au + bv)b - (av + bu) = (b^2 - a^2)v$$

de donde, como p no divide a v (pues $p = u^2 + v^2$), tenemos que p divide a $b^2 - a^2$. Como p divide también a $a^2 + b^2$ por hipótesis, es fácil checar que p divide a a y a b y por tanto ambos números en (2.1) son enteros. Regresando al teorema original, supongamos que α es un primo gaussiano.

Como $N(\alpha) \neq 1$, existe al menos un primo p que divide a $N(\alpha)$. Si $p = 2$, la parte a) del lema anterior nos dice que $1 + i$ divide a α. Como α es primo, entonces es igual (salvo unidades) a $1 + i$, de donde α es un primo del primer tipo. Para el caso en que $p \equiv 3 \mod 4$, la parte b) del lema anterior nos dice que p divide a α, así que α es un primo del tipo ii) hasta unidades. Por último, si $p \equiv 1 \mod 4$ escribimos p de la forma $p = u^2 + v^2$ y entonces α es divisible por $u + iv$ o por $u - iv$. Esto nos dice que α es un primo del tercer tipo y concluye la prueba de nuestro teorema.

3. Factorización única de los enteros gaussianos

Para probar el teorema fundamental de la aritmética, utilizamos una propiedad muy importante de los números primos: *si un número primo divide a un producto, entonces divide a uno de los factores.* Esto se sigue de la propiedad de la división euclideana de los enteros: Si a y b son enteros, podemos encontrar enteros únicos q y r tales que $a = bq + r$ para $0 \leq r < b$. En los enteros gaussianos, no es evidente que se pueda efectuar la división entre dos de ellos y obtener un residuo *más chico*. Probaremos que efectivamente esto pasa en el siguiente lema.

Lema 1.6. *Sean α y $\beta \in Z[i]$ tales que $\beta \neq 0$. Existen γ y $\rho \in [i]$ tales que*

$$\alpha = \beta\gamma + \rho$$

con $N(\rho) < N(\beta)$.

Demostración. En esta prueba es muy útil pensar geométricamente y proceder algebraicamente. Consideremos el número complejo $\frac{\alpha}{\beta}$. Veamos a este número complejo dentro de un cuadrado de la retícula $L := \times i$. Sea $\gamma \in L$ el vértice de este cuadrado más cercano a $\frac{\alpha}{\beta}$. Como la distancia de $\frac{\alpha}{\beta}$ a γ es máxima cuando $\frac{\alpha}{\beta}$ se encuentra en el centro del cuadrado y en dicho caso la distancia es $\frac{\sqrt{2}}{2}$, tenemos que

$$N\Big(\frac{\alpha}{\beta} - \gamma\Big) \leq \frac{1}{2}$$

de donde se sigue que

$$N(\alpha - \beta\gamma) \leq \frac{1}{2}N(\beta).$$

Escogiendo a ρ como $\alpha - \beta\gamma$ se concluye el resultado.

El siguiente lema también está basado en una propiedad de los enteros.

LEMA 1.7. *Sean α, β enteros gaussianos. Sea $S_{\alpha,\beta}$ el conjunto*

$$\{z \in : z = \alpha x + \beta y, x, y \in\}$$

y sea $\delta \in S_{\alpha,\beta}$ el elemento de norma mínima positiva. Entonces δ divide a α y β.

DEMOSTRACIÓN. Dividiendo α entre δ obtenemos que

$$\alpha = \delta\gamma + \rho$$

para γ, ρ como en el lema anterior. Sean $a, b \in$ tales que $\delta = a\alpha + b\beta$. Entonces,

$$\rho = \alpha - \delta\gamma = \alpha(1 - a\gamma) - b\gamma\beta$$

de donde $\rho \in S_{\alpha,\beta}$ pero $N(\rho) < N(\delta)$, de donde se sigue que $\rho = 0$.

El siguiente lema nos dice que los primos gaussianos se comportan de manera parecida a los primos usuales.

LEMA 1.8. *Sea π un primo gaussiano, sean α, β enteros gaussianos tales que π divide a $\alpha\beta$. Entonces π divide a al menos uno de α o β. En general, si π divide a un producto $\alpha_1\alpha_2 \ldots \alpha_k$ entonces π divide a al menos uno de los α_i, $i = 1, \ldots, k$.*

DEMOSTRACIÓN. Utilizaremos el lema anterior con α y π. Sea δ tal que

$$\delta = a\alpha + b\pi$$

con $N(\delta)$ de norma mínima y positiva en $S_{\alpha,\pi}$. Como δ divide a α y π, y π es primo, entonces δ es una unidad o una unidad por π. Si $\delta = u\pi$, con u una unidad, entonces π también divide a α y hemos terminado. Supongamos entonces que δ es una unidad. Consideremos

$$\delta\beta = a\alpha\beta + b\pi\beta.$$

De aquí se sigue que π divide a $\delta\beta$ y por ser δ unidad, entonces π divide a β. Esto termina la primera parte del lema. La segunda parte es directa utilizando inducción matemática.

Estamos listos para demostrar el teorema de factorización única para los enteros gaussianos. Para poder dar una formulación precisa, introducimos la noción de *normalización*.

Sea $z = x + yi \in$. Decimos que z está normalizado si $x > 0, y \geq 0$.

Multiplicando por unidades (que corresponden a rotaciones de $\frac{\pi}{2}$ alrededor del origen) podemos normalizar a cualquier entero gaussiano.

Teorema 1.9. *Sea $\alpha \in [i]$ distinto de cero. Entonces α puede escribirse de la forma*

$$\alpha = u\pi_1\pi_2 \dots \pi_k$$

donde u es una unidad y π_i son primos gaussianos normalizados para $i = 1, \dots k$. Esta descomposición es única salvo permutaciones.

Demostración. Probaremos por contradicción que cualquier entero gaussiano tiene una factorización en primos. Sea α un entero gaussiano de norma mínima que no se factoriza como producto de primos. Notemos que α no puede ser unidad ni primo. Entonces existen dos enteros gaussianos β y γ, ninguno de ellos unidad, tales que

$$\alpha = \beta\gamma.$$

Entonces,

$$N(\alpha) = N(\beta)N(\gamma),$$

Pero $N(\beta), N(\gamma)$ son ambos mayores que 1. Se sigue que $N(\beta), N(\gamma) < N(\alpha)$, contradiciendo la minimalidad de α.

Ahora procederemos también por contradicción para probar que la factorización es única. Sea α un entero gaussiano de norma mínima con dos factorizaciones en primos normalizados

$$\alpha = u\pi_1 \dots \pi_k = v\pi'_1 \dots \pi'_s,$$

donde u y v son unidades. Es claro que α no puede ser unidad. Entonces $k \geq 1$ en la primera factorización. De aquí se sigue que π_1 divide al producto $v\pi'_1 \dots \pi'_s$. Entonces π_1 divide a uno de los factores, por el lema anterior. Sin pérdida de generalidad, π_1 divide a π'_1, entonces

$$\pi_1 = w\pi'_1,$$

donde w es una unidad. Pero como escogimos a los primos normalizados, entonces w debe ser igual a 1. Cancelando π_1 en ambas factorizaciones, tenemos que $\frac{\alpha}{\pi_1}$ es un entero gaussiano con dos factorizaciones distintas en primos normalizados y de norma menor que $N(\alpha)$, contradiciendo la minimalidad de α. Esto concluye la prueba del teorema.

Capítulo 2

La cardinalidad de un conjunto de Sidon

En este capítulo mostraremos algunos resultados sobre la cardinalidad de un conjunto de Sidon.

Sea $\mathcal{S} \subset [1, n]$ un conjunto de Sidon y $S(n)$ su función de conteo. Mostramos primero una cota trivial para $S(n)$.

LEMA 2.1. $S(n) \leq \sqrt{2n}$

DEMOSTRACIÓN. Escribimos $s = S(n)$. Las sumas de dos elementos de $\mathcal{S}$ son a lo más s^2 y todas las sumas de dos elementos de $\mathcal{S}$ están en el intervalo $[1, 2n]$ de donde se obtiene la desigualdad.

El siguiente teorema da una mejor estimación para $S(n)$. Este teorema apareció por primera vez en [**2**] y la prueba fue mejorada en [**4**]. En la siguiente sección daremos la demostración de Lindström de un teorema de Erdős y Turán sobre el tamaño de $S(n)$.

TEOREMA 2.2. *(Erdős-Turán 1941) Con la notación anterior,*

$$S(n) \leq n^{\frac{1}{2}} + n^{\frac{1}{4}} + 1.$$

DEMOSTRACIÓN. Sea $\mathcal{S} = \{s_1, s_2, \ldots s_m\}$ con $1 \leq s_1 < s_2 < \ldots < s_m$ un conjunto de Sidon contenido en $[1, n]$. Consideramos la suma

$$T := \sum_{0<j-i<k} (s_j - s_i)$$

donde k es un parámetro que vamos a determinar más tarde. En T aparecen

$$N := (m-1) + (m-2) + \ldots + (m-k) = mk - \frac{k(k+1)}{2}$$

diferencias distintas, entonces se tiene que

$$T \geq 1 + 2 + \ldots N > \frac{N^2}{2} \geq \frac{N^2}{2}.$$

Por otro lado, T es una suma telescópica y después de las cancelaciones nos queda

$$T = (s_m - s_1) + 2(s_{m-1} - s_2) + \ldots + k(s_{m-k+1} - s_k) < \frac{nk(k+1)}{2},$$

de donde

$$\frac{n(k+1)}{k} > \left(m - \frac{k(k+1)}{2}\right)^2 \iff \sqrt{\frac{n(k+1)}{k}} + \frac{k+1}{2} > m.$$

Utilizando el hecho de que

$$\sqrt{1+x} = 1 + \frac{1}{2}x + O(x^2)$$

(por la fórmula de Taylor alrededor de 0), se tiene

$$m < \sqrt{\left(1 + \frac{1}{k}\right)} + \frac{k+1}{2} < \sqrt{n} + \frac{\sqrt{n}}{2k} + \frac{k+1}{2}$$

de donde se obtiene la estimación buscada tomando $k = \lfloor n^{\frac{1}{4}} \rfloor$.

Capítulo 3

Conjuntos de Sidon finitos

En este capítulo mostraremos como obtener conjuntos de Sidon finitos. El primer intento natural, como mencionamos antes, 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.

Teorema 3.1. *El conjunto*

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

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 $x_p + x_q - x_r - x_s = 0$,

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

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

$$|\{x\} + \{y\} - \{z\} - \{w\}| \leq 2, \tag{0.1}$$

obtenemos

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

de donde

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

Como

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

donde la primera desigualdad se sigue de que $pq > rs$, la segunda desigualdad se sigue de $\log(1+x) \geq \frac{x}{2}$ para $x < 2$ y la tercera desigualdad se sigue de la definición de r y s, se obtiene una contradicción con la desigualdad anterior. La cardinalidad de $\mathcal{X}$ 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 ¶ el conjunto de los números primos congruentes a 1 módulo 4. Para $p \in ¶$, 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 $[i]$ también lo es salvo unidades $(\pm 1, \pm i)$. Sea $\rho_p = a + bi$ tal que $p = \rho_p\bar{\rho_p}$, con $\bar{\rho_p}$ tal que $a > -b > 0$. [1] Escribamos $\frac{\bar{\rho_p}}{\rho_p} = e^{2\pi i\phi_p}$ con ϕ_p un número en $[0,1)$. Denotamos con $|z|$ el valor absoluto del número complejo z y con $\arg z$ su argumento, tomando aquel valor del argumento que está en $[0, 2\pi)$. La sucesión $(\phi_p)_{p\in¶}$ es un conjunto de Sidon módulo 2π, pues si tenemos $\phi_p + \phi_q = \phi_r + \phi_s$, esto implicaría que $\bar{\rho_p}\bar{\rho_q}\rho_r\rho_s = \rho_p\rho_q\bar{\rho_r}\bar{\rho_s}$ lo cual es imposible si $\{p,q\} \neq \{r,s\}$. Se tiene el siguiente teorema.

Teorema 3.2. *El conjunto*

$$C := \Big\{c_p \in\colon c_p = \lfloor n\phi_p\rfloor, p \in ¶,\ p \leq \frac{\sqrt{n}}{4}\Big\},$$

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

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

[1] Esto es válido porque z es primo gaussiano si y solamente si $\pm iz, \pm z, \pm i\bar{z}, \pm\bar{z}$ también lo son. Escogemos uno de ellos con esta propiedad.

$$c_p + c_q = c_r + c_s$$

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

$$n(\phi_p + \phi_q - \phi_r - \phi_s) = \{n\phi_p\} + \{n\phi_q\} - \{n\phi_r\} - \{n\phi_s\} \tag{0.2}$$

Observemos que

$$\left|\frac{\bar{\rho}_p\bar{\rho}_q}{\rho_p\rho_q} - \frac{\bar{\rho}_r\bar{\rho}_s}{\rho_r\rho_s}\right| = \left|1 - \frac{\rho_p\rho_q\bar{\rho}_r\bar{\rho}_s}{\bar{\rho}_p\bar{\rho}_q\rho_r\rho_s}\right| = \left|1 - e^{2\pi i(\phi_p+\phi_q-\phi_r-\phi_s)}\right| \leq 2\pi|\phi_p + \phi_q - \phi_r - \phi_s| \leq \frac{4\pi}{n}$$

donde la primera desigualdad es inmediata de la interpretación geométrica[2] y la segunda desigualdad se sigue de (0.1) y (0.2). Por otra parte,

$$\left|\frac{\bar{\rho}_p\bar{\rho}_q}{\rho_p\rho_q} - \frac{\bar{\rho}_r\bar{\rho}_s}{\rho_r\rho_s}\right| = \left|\frac{\bar{\rho}_p\bar{\rho}_q\rho_r\rho_s - \bar{\rho}_r\bar{\rho}_s\rho_p\rho_q}{\rho_p\rho_q\rho_r\rho_s}\right| \geq \frac{1}{\sqrt{pqrs}} \geq \frac{16}{n}.$$

De las desigualdades anteriores se tiene

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

que es una contradicción. El teorema de los números primos en progresiones aritméticas nos da la cardinalidad de C.

[2]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.

Capítulo 4

La construcción

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

$$\{\alpha\phi_p \in : \ p \in ¶\}.$$

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

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

y $K_p > 2$ el entero que satisface

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

Consideramos el conjunto

$$P_K = \{p \in ¶ : K_p = K\}.$$

Para $p \in P_K$ sea

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

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

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

y por tanto tenemos

$$\Delta_{ip} \leq \sum_{j=(i-1)^2+1}^{i^2} 2^{i^2-j} = 2^{2i} - 1. \tag{0.3}$$

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 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 $_\alpha := \cup_{p\in¶}\{a_p\}$. 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 siguiente 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 $\mathcal{A}_\alpha$.

Consideramos el conjunto $_\alpha$, para una elección fija de α. Sean $a_p, a_q, a_r, a_s \in_\alpha$ con $p, q, r, s \in ¶$ tales que

$$a_p + a_q = a_r + a_s \tag{0.4}$$

con

$$a_p > a_r \geq a_s > a_q. \tag{0.5}$$

Decimos que la cuadrupla $(p, q, r, s) \in ¶^4$ es una *cuadrupla mala*.

La desigualdad (0.5) es una consecuencia de (0.4): si decimos que a_p es máx$\{a_p, a_q, a_r, a_s\}$, entonces a_q necesariamente es el menor de ellos y hasta un cambio de variable podemos decir que $a_r \geq a_s$.

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

La manera en que se construyen los elementos de $_\alpha$ ayuda a contar el número de cuadruplas malas.

Lema 4.1. *(p, q, r, s) es una cuadrupla 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 (0.4) y (0.5) 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

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

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 (0.5), 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 $i < L$,

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

Como los términos en paréntesis no afectan a la otra parte de la suma ya que su suma total es $\leq 2^{2j+1} - 2$ por (0.3), 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 cuadruplas malas. Para el lema siguiente, recordemos que $m_p = \left\lfloor 2^{K^2} \alpha \phi_p \right\rfloor$

LEMA 4.2. *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 cuadruplas malas (p, q, r, s). Para el siguiente lema, utilizamos el hecho que $\phi_p + \phi_q = \phi_{pq}$.

LEMA 4.3. *Si (p, q, r, s) es una cuadrupla mala, con K y L como antes, entonces*

$$|\phi_{p\bar{r}} - \phi_{s\bar{q}}| < 4 \cdot 2^{-L^2}, \tag{0.6}$$

$$(K-1)^2 + (L-1)^2 > \beta(L^2-5), \tag{0.7}$$

$$(K-1)^2 + (L-1)^2 > \beta(L-1)^2. \tag{0.8}$$

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

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

Por otro lado,

$$\left|\frac{\bar{\rho}_p\bar{\rho}_q}{\rho_p\rho_q} - \frac{\bar{\rho}_r\bar{\rho}_s}{\rho_r\rho_s}\right| = \left|e^{2\pi i(\phi_p+\phi_q)} - e^{2\pi i(\phi_r+\phi_s)}\right| = \left|1 - e^{2\pi i(\phi_p+\phi_q-\phi_r-\phi_s)}\right| \leq 2\pi|\phi_p+\phi_q-\phi_r-\phi_s| < 8|\phi_p+\phi_q-\phi_r-\phi_s|.$$

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

$$\alpha|\phi_{p\bar{r}} - \phi_{s\bar{q}}| < |\alpha\phi_p - m_p| + |\alpha\phi_{\bar{q}} - m_q| + |\alpha\phi_{\bar{r}} - m_r| + |\alpha\phi_s - m_s| < 4 \cdot 2^{-L^2}. \tag{0.9}$$

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 (0.6) se cumpla. A cada $z \in [i]$ con $z = a + ib$ y $a, b \in$ le asociamos el punto de coordenadas enteras $(a, b) \in^2$. Decimos entonces que (a, b) es un punto de coordenadas enteras.

Lema 4.4. *Sea $z_0 \in^2$. Sea el círculo con centro z_0 y radio R. El número n de puntos de coordenadas enteras en un sector circular de de ángulo θ que corresponden a los elementos de $[i]$ $\{w_1, w_2 \ldots w_n\}$ tal que para $i = 1, \ldots n$, $w_i = \rho_{p_i}\bar{\rho}_{r_i}$ 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 $\{\phi_{p_i}, \phi_{r_i}\} \neq \{\phi_{p_j}, \phi_{r_j}\}$ a partir de 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 $i = 1, \dots n-1$. 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

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

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

Lema 4.5. *El número de cuadruplas 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

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

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.

1. 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 cuadruplas malas no es muy buena para valores pequeños de L. Utilizaremos el parámetro α para solucionar este problema.

Lema 4.6. *Sea (p, q, r, s) una cuadrupla mala. Entonces*

$$m_p \equiv m_r \mod 2^{K^2-L^2}. \tag{1.1}$$

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 . Veremos como evadir las cuadruplas malas con una elección apropiada de α.

Lema 4.7. *Sea $K > L$ dado y $p, r \in P_K$ tal que existe al menos un par $q, s \in P_L$ y un α tal que* (0.4). *Entonces*

$$\mu\{\alpha \in [1, 2) : (1.1) \text{ se cumple}\} \ll 2^{L^2-K^2}.$$

Demostración. Recordemos que $\lfloor x \rfloor - \lfloor y \rfloor = \lfloor x - y \rfloor + 0$ ó -1. Tenemos entonces que

$$\left\lfloor 2^{K^2} \alpha(\phi_p - \phi_r) \right\rfloor \equiv 0, 1 \quad \text{mód } 2^{K^2 - L^2}.$$

Ponemos $M := 2^{K^2-L^2}$ y $N := \lfloor 2^{K^2}(\phi_p - \phi_r) \rfloor$. 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

$$\mu\{\alpha \in [1, 2) : (1.1) \text{ se cumple}\} \ll \frac{2}{N}\Big(1 + \frac{N}{M}\Big).$$

Basta probar que $N \gg M$. Por (0.9) se tiene que

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

Como

$$\left|\phi_q - \phi_s\right| \geq \frac{1}{2\pi}\left|1 - \frac{\bar{\rho_q}\rho_s}{\rho_q\bar{\rho_s}}\right| = \frac{1}{2\pi}\left|\frac{\bar{\rho_q}\rho_s - \bar{\rho_s}\rho_q}{\rho_q\bar{\rho_s}}\right| \gg 2^{-\frac{L^2}{\beta}},$$

donde la última desigualdad se sigue de $q^\beta, s^\beta < 2^{(L-1)^2}$. 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, $\frac{2}{N}(1 + \frac{N}{M}) \ll \frac{1}{N}\frac{N}{M} = \frac{1}{M}$, lo que concluye la prueba. Esta nueva cota es buena en el sentido que no demasiados α's contribuyen a completar cuadruplas malas para un par p, r dado cuando L es pequeño. Por otro lado, nuestra cota anterior para el número de cuadruplas 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 4.8. *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 $m = \mu\{\alpha \in [1,2) : (0.4) \text{ se cumple}\}$. Como $m = 0$ cuando (0.6) 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 $T_K(\alpha) :=$ $\#\{p, q, r, s : p, r \in P_K, (0.4) \text{ y } (0.5) \text{ se cumplen}\}$. De la definición es inmediato que $T_K(\alpha) = \sum_{L\geq K} T_{KL}(\alpha)$.

Lema 4.9. *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 $(K-1)^2 + (L-1)^2 > \beta(L-1)^2$, haciendo como $\mathcal{L}$ el conjunto de tales L,

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

donde

$$C = \frac{2(K-1)^2}{\beta} - K^2 + \frac{2(K-1)^2}{\beta(\beta-1)} = \frac{2}{\beta-1}(K-1)^2 - K^2 = \left(\frac{2}{\beta-1} - 1\right)K^2 - \frac{4}{\beta-1}K + \frac{2}{\beta-1}$$

de donde 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 4.10. *(Ruzsa, 1998) Existe un conjunto de Sidon infinito $\mathcal{S}$ tal que la función de conteo $S(x)$ satisface*

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

cuando $x \to +\infty$ *para* $\beta = \sqrt{2} + 1$.

Demostración. De la estimación anterior, obtenemos

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

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

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

entonces, para K suficientemente grande, $T_K(\alpha) < \frac{|P_K|}{2}$. Esto significa que si omitimos el elemento más chico de las cuadruplas 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 $S(x) \geq \pi_1(2^{\frac{1}{\beta}(K-1)^2}) = x^{\frac{1}{\beta}+o(1)}$. 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 $S(x) \leq \pi_1(2^{\frac{1}{\beta}K^2}) = x^{\frac{1}{\beta}+o(1)}$. De estas estimaciones se sigue el teorema.

Bibliografía

[1] W. Babcock, *Intermodulation Interference in Radio Systems: Frequency of Occurrence and Control by Channel Selection*, Bell System Technical Journal **31** (1953), 63-73.

[2] P. Erdős, P. Turán, *On a Problem of Sidon in Additive Number Theory and On Some Related Problems,* Journal of the London Mathematical Society **16** (1941) 212-215.

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

[4] B. Lindström *A remark onB_4-sequences,* Journal of Combinatorial Theory **7** (1969) 276-277.

[5] K. O'Bryant *A complete annotated bibliography of work related to Sidon sequences*, Electronic Journal of Combinatorics, **DS11**, (2004), 39pp.

[6] I. Ruzsa *An infinite Sidon set*, J. Number Theory **68** (1998), 63-71.

[7] S. Sidon *Ein Satz uber über trigonomietrische Polynome und seine Anwendgungen in der Theorie der Fourier-Reihen*, Math. Annalen **106** 1932, 536-539.