El diablo de los números

Sección a cargo de

Javier Cilleruelo

Conjuntos de enteros con todas las diferencias distintas

por

Javier Cilleruelo

1. Introducción

Uno de los problemas favoritos de Erdős, y que mejor ha descrito su gusto por la «aritmética combinatoria», ha sido el de los conjuntos de Sidon.

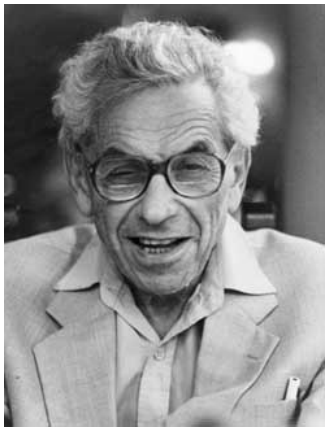
Corría el año 1932 cuando Simon Sidon, el analista húngaro, le preguntó a Erdős sobre conjuntos de enteros positivos con todas las diferencias de dos elementos distintas.

¿Cuántos enteros podemos seleccionar entre los n primeros con esa propiedad?

Estos conjuntos, que Erdős bautizaría como *conjuntos de Sidon,* son el objeto de este ensayo.

Como $a - d = c - b \Leftrightarrow a + b = c + d$, los conjuntos de Sidon se definen indistintamente como aquéllos que tienen la propiedad de que todas las sumas de dos elementos cualesquiera del conjunto son distintas.

Aunque el interés de Sidon por estos conjuntos tenía que ver con cuestiones del análisis de Fourier, el problema cautivó a un joven Erdős por su vertiente aritmética y combinatoria, y se convertiría en un tema recurrente en su investigación hasta que nos abandonara en busca de «El Libro».



La referencia a «El Libro» donde se encuentran las demostraciones más hermosas es constante en la obra de Erdős.

Muchos años después, en la pizarra de su despacho, Antonio Córdoba me habló de los conjuntos de Sidon, también a propósito de un problema del análisis armónico.

Como le pasara a Erdős, y salvando todas las diferencias, fue el sabor combinatorio de estos conjuntos lo que más me sedujo, hasta el punto de llegar a marcar de manera notable mi trayectoria investigadora.

Haremos un recorrido sobre resultados clásicos y otros más recientes concernientes a los conjuntos de Sidon. También nos detendremos en unas aplicaciones inesperadas de los conjuntos de Sidon al último teorema de Fermat en $\mathbb{F}_p$ y al estudio de algunas sucesiones notables en $\mathbb{F}_p$, como los residuos cuadráticos o las potencias de raíces primitivas.

La parte final de este ensayo consiste en una selección de problemas sin resolver sobre los conjuntos de Sidon.

2. Construcciones de conjuntos de Sidon

Intente el lector seleccionar el mayor número de enteros positivos de entre los 35 primeros de tal manera que todas las diferencias entre ellos sean distintas. Seguramente no tendrá ningún problema en seleccionar unos pocos, pero irá encontrándose con dificultades a medida que quiera ir añadiendo más elementos a la colección. Además, una vez que tenga un conjunto que le parezca aceptable, se quedará con la duda de si es posible construir otro con algún elemento más. Al final de esta sección desvelaremos la solución.

¿Cuál es el mayor tamaño que puede tener un conjunto de Sidon $\mathcal{A}$ en $\{1,\dots,n\}$?

Construir conjuntos de Sidon no es difícil. Lo interesante es construirlos con el mayor número de elementos posible. A esta tarea nos dedicaremos en esta sección.

2.1. La sucesión más inocente

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

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

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

2.2. Con la ayuda de los primos

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

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

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

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

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

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

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

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

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

obteniendo así una contradicción.

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

Es posible mejorar un poco más la construcción anterior utilizando los argumentos de los primos de Gauss $\mathbf{p} = a + bi$ en el primer octante, $\mathbf{p} = |\mathbf{p}|e^{2\pi i\phi_{\mathbf{P}}}$, en lugar de los logaritmos de los primos racionales. Procediendo de una manera similar se demuestra fácilmente que el conjunto

$$\mathcal{A} = \{a_{\mathbf{p}} = \lfloor n\phi_{\mathbf{p}}\rfloor,\ |\mathbf{p}| \leq (n/2)^{1/4},\ \mathbf{p} \text{ primo de Gauss}\}$$

es un conjunto de Sidon en $\{1, \dots, n\}$ con $\sim n^{1/2}/(\sqrt{8}\log n)$ elementos, mejorando en un factor $(\log n)^{1/2}/2$ el tamaño de la construcción anterior.

2.3. Conjuntos de Sidon en grupos

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

Aunque la definición de conjunto de Sidon más clásica se refiere a conjuntos de enteros, se extiende de manera natural a cualquier grupo abeliano G, finito o infinito.

Definición 1. *Un conjunto $\mathcal{A}$ en un grupo abeliano $(G, +)$ es un conjunto de Sidon si todas las diferencias no nulas $a - a'$ con $a, a' \in \mathcal{A}$ son distintas.*

[1] Ruzsa [26] explotó esta idea para construir la sucesión infinita de Sidon más densa que se conoce hoy en día. La construcción de Ruzsa merecerá nuestra atención en la sección 4.

En las tres construcciones que presentamos a continuación p es siempre un primo impar y g es una raíz primitiva en $\mathbb{F}_p$. Los tres ejemplos se pueden representar gráficamente (ver figuras más adelante) y el lector puede recrear su vista observando que ninguno de ellos contiene cuatro puntos formando un paralelogramo.

La construcción del ejemplo 3, en particular, nos permitirá construir, después de unas observaciones sencillas, un conjunto de Sidon en $\{1,\dots,n\}$ con $\sim n^{1/2}$ elementos. Sin embargo, las aplicaciones de los conjuntos de Sidon en grupos finitos no acaban ahí, como veremos en la sección 3.

Ejemplo 1. *El conjunto de Sidon más sencillo que se conoce es el conjunto de p elementos*

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

Para ver que es un conjunto de Sidon es suficiente con comprobar que si $(e_1, e_2) \neq (0,0)$, los valores de $x_1, x_2 \in \mathbb{Z}_p$ en la ecuación $(x_1, x_1^2) - (x_2, x_2^2) = (e_1, e_2)$ quedan perfectamente determinados. Observemos que si $e_1 = 0$ y $e_2 \neq 0$ la ecuación no tiene soluciones. Pero si $e_1 \neq 0$, e_1 tiene inverso y entonces

$$\begin{array}{l} x_1 - x_2 = e_1 \\ x_1^2 - x_2^2 = e_2 \end{array} \implies \begin{array}{l} x_1 - x_2 = e_1 \\ x_1 + x_2 = e_2 e_1^{-1} \end{array} \implies \begin{array}{l} x_1 = 2^{-1}(e_1 + e_2 e_1^{-1}) \\ x_2 = 2^{-1}(e_1 + e_2 e_1^{-1}) - e_1. \end{array}$$

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

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

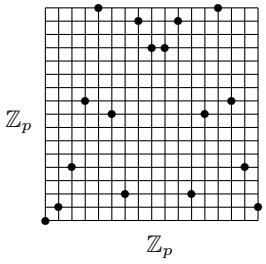
De nuevo es suficiente con comprobar que, excepto cuando $(e_1, e_2) \neq (0,0)$, la ecuación $(x_1, y_1) - (x_2, y_2) = (e_1, e_2)$ sujeta a las condiciones $g^{x_1} + g^{y_1} = 1$ y $g^{x_2} + g^{y_2} = 1$ tiene a lo más una solución. Resolviendo obtenemos fácilmente que $g^{y_2}(g^{e_2} - g^{e_1}) = 1 - g^{e_1}$. Si utilizamos el hecho de que g es una raíz primitiva y que todo elemento distinto de cero tiene inverso, podemos ver que el valor de y_2 queda determinado de manera única, excepto cuando $e_1 = 0$ o $e_1 = e_2$, en cuyo caso no hay ningún valor de y_2 que satisfaga la ecuación. Los restantes valores, y_1, x_1, x_2, quedan determinados a partir de y_2.

Ejemplo 3. *Welch descubrió el conjunto de Sidon de $p-1$ elementos*

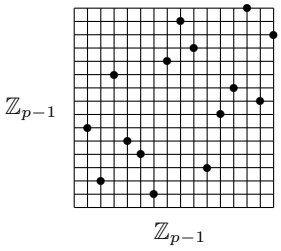
$$\mathcal{A} = \{(x, g^x),\ 0 \leq x < p-1\} \subset \mathbb{Z}_{p-1} \times \mathbb{Z}_p.$$

La ecuación $(x_1, g^{x_1}) - (x_2, g^{x_2}) = (e_1, e_2)$, donde la igualdad en cada componente hay que entenderla en el grupo correspondiente, determina los valores x_1, x_2. Para verlo utilizamos el teorema de Fermat que nos asegura que si $x_1 - x_2 \equiv e_1 \pmod{p-1}$ entonces $g^{x_1 - x_2} \equiv g^{e_1} \pmod{p}$. Resolviendo esta nueva ecuación con la ecuación $g^{x_1} - g^{x_2} \equiv e_2 \pmod{p}$ obtenemos $g^{x_2}(g^{e_1} - 1) \equiv e_2 \pmod{p}$. Por las mismas razones que en el ejemplo anterior, el valor de x_2 queda perfectamente determinado.

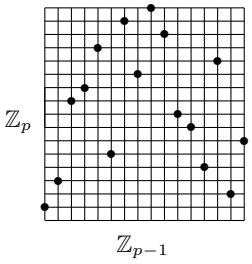
Es fácil comprobar que los tres conjuntos de Sidon descritos tienen tamaño máximo en sus respectivos grupos. Si hubiera un conjunto de Sidon $\mathcal{A} \subset \mathbb{Z}_p \times \mathbb{Z}_p$ con $|\mathcal{A}| = p+1$, el número de diferencias no nulas sería $(p+1)p$. Pero como todas ellas son distintas, no cabrían en un grupo de p^2 elementos. En los otros dos ejemplos el argumento es similar.



Ejemplo 1



Ejemplo 2



Ejemplo 3

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

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

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

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

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

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

Aunque hay otras dos construcciones clásicas de conjuntos de Sidon en grupos de la forma $\mathbb{Z}_m$, ésta, debida a Ruzsa [25], es la más sencilla de describir.

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

Los enteros en $\{1, \ldots, m\}$ que representan los elementos de un conjunto de Sidon en $\mathbb{Z}_m$ forman, en particular, un conjunto de Sidon en $\{1, \ldots, m\}$. Como sabemos de la existencia de conjuntos de Sidon en $\mathbb{Z}_m$ con $\sim m^{1/2}$ para valores particulares de m, por ejemplo para los de la forma $m = p(p-1)$ con p primo, buscaremos el mayor primo p tal que $p(p-1) \le n$.

Uno de los grandes retos en el estudio de la distribución de los números primos consiste en hallar el menor α que garantice que todo intervalo $(x - x^\alpha, x)$ contiene algún primo para x suficientemente grande. Se conjetura que es cierto para cualquier $\alpha > 0$, pero sólo se conoce [3] para $\alpha > 0{,}525$. Utilizaremos este hecho y la construcción anterior para construir un conjunto de Sidon en $\{1, \ldots, n\}$.

Para un n dado suficientemente grande, tomemos un primo p en el intervalo $(n^{1/2} - n^{\alpha/2}, n^{1/2})$. Claramente $p(p-1) \le n$, por lo que los $p-1$ elementos del conjunto $\mathcal{A}$ definido en (1) forman un conjunto de Sidon en $\{1, \ldots, n\}$ con más de $n^{1/2} - n^{\alpha/2}$ elementos, donde podemos tomar cualquier $\alpha > 0{,}525$. Como ya hemos dicho, se conjetura que cualquier $\alpha > 0$ es también válido.

A continuación veremos que esta construcción es esencialmente óptima.

2.4. Cotas superiores para el tamaño de conjuntos de Sidon

Se define $F(n)$ como el mayor número de enteros positivos que podemos seleccionar de entre los n primeros con la propiedad de que todas la diferencias son distintas. Es decir,

$$F(n) = \text{máx}\{|\mathcal{A}|,\ \mathcal{A} \subset \{1, \ldots, n\},\ \mathcal{A} \text{ conjunto de Sidon}\}.$$

La última construcción nos proporcionó la estimación $F(n) \geq n^{1/2} - O(n^{0{,}2625+\epsilon})$.

La notación $g(n) = O(f(n))$ significa que $|g(n)| \leq Cf(n)$ para alguna constante $C > 0$ que no depende de n. También utilizaremos la notación $g(n) \gg f(n)$ para indicar que $g(n) \geq cf(n)$ para alguna constante $c > 0$ que de nuevo no depende de n.

Un sencillo argumento, que no es más el que principio del palomar, permite hallar una primera cota superior para $F(n)$: como el número de diferencias positivas en un conjunto de Sidon es $\binom{|\mathcal{A}|}{2}$, y todas ellas son menores que n, tenemos que $\binom{|\mathcal{A}|}{2} \leq n - 1$, de donde deducimos la cota superior $F(n) \leq \sqrt{2n} + 1$.

Contando sólo las diferencias pequeñas en lugar de todas las diferencias, Erdős y Turán [15], y posteriormente Lindström [20] con un resultado más preciso, consiguieron mejorar esta estimación. La cota obtenida por Lindström,

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

sigue imbatida 40 años después.

Éste es el momento de desvelar la solución al problema propuesto al inicio de la primera sección. El conjunto $\{1, 2, 5, 10, 16, 23, 33, 35\}$, con 8 elementos, es un conjunto de Sidon de tamaño máximo en el conjunto de los 35 primeros enteros positivos. De hecho, aunque es más difícil de demostrar, este conjunto y su reflejo son los únicos con 8 elementos.

Una manera gráfica de comprobar que este conjunto es de Sidon consiste en dibujar su triángulo de diferencias y comprobar que todas ellas son distintas. La primera fila se completa calculando las diferencias entre los términos consecutivos del conjunto. Para ir completando el resto de las filas hay que sumar los dos vecinos de arriba y restar el de más arriba, que supondremos 0 cuando calculemos la segunda fila:

1		3		5		6		7		10		2
	4		8		11		13		17		12	
		9		14		18		23		19		
			15		21		28		25			
				22		31		30				
					32		33					
						34						

Ahora nos queda por ver que realmente no podemos encontrar un conjunto de Sidon de más elementos en este conjunto. Supongamos que hubiera uno de 9 elementos. La suma de las diferencias consecutivas es una suma telescópica que se estima

fácilmente,

$$(a_2 - a_1) + (a_3 - a_2) + \cdots + (a_8 - a_7) + (a_9 - a_8) = a_9 - a_1 \leq 34.$$

Por otra parte, como las 8 diferencias que hemos escrito arriba son todas distintas, su valor debe ser por lo menos $1 + 2 + \cdots + 8 = 36$, lo que nos da la contradicción.

Erdős conjeturó que $F(n) \leq n^{1/2} + O(1)$. Aunque hay evidencias numéricas y de otro tipo que hacen sospechar que esta conjetura no es cierta, nadie ha sido capaz de refutarla. Se cree que la conjetura acertada es la siguiente.

Conjetura 1. *Para todo $\epsilon > 0$, $F(n) \leq n^{1/2} + O(n^{\epsilon})$.*

3. Distribución de los residuos cuadráticos, el último teorema de Fermat en $\mathbb{F}_p$ y otras aplicaciones de los conjuntos de Sidon

Recientemente hemos encontrado [7] unas aplicaciones inesperadas de los conjuntos de Sidon al estudio de problemas clásicos sobre la distribución de algunas sucesiones en $\mathbb{Z}_p$. Los resultados no son nuevos, pero las demostraciones son puramente combinatorias. Todas las demostraciones conocidas hasta la fecha, incluyendo las originales de Vinogradov, utilizan el análisis de Fourier en grupos y necesitan de estimaciones de sumas trigonométricas.

La idea que hay detrás de este nuevo método es que si $\mathcal{A}$ es un conjunto de Sidon de tamaño máximo en un grupo finito G, entonces $\mathcal{A}$ está bien distribuido en subconjuntos de G con ciertas condiciones de regularidad.

Ya vimos que los conjuntos de Sidon descritos en la sección anterior son de tamaño máximo. Serán estos tres conjuntos de los que nos serviremos para las aplicaciones que queremos presentar.

Muchos de los problemas clásicos que trataremos se traducen fácilmente en estimar cuántos elementos de un determinado conjunto de Sidon caen en un subconjunto apropiado.

El siguiente lema va a ser el ingrediente principal en todas las aplicaciones. Aunque podríamos presentar una versión más general, hemos preferido adaptarla a los ejemplos de la sección anterior. Su demostración, que nos ha parecido oportuno omitir en este ensayo dirigido a un público amplio, es puramente combinatoria.

Lema 1. *Sea $\mathcal{A} \subset G$ cualquiera de los tres conjuntos de Sidon descritos en la subsección 2.3. Para cualesquiera subconjuntos $B, C \subset G$, existe un $c \in C$ tal que*

$$\left| |\mathcal{A} \cap B| - \frac{|\mathcal{A}||B|}{|G|} \right| \leq \left(3p \frac{|B|}{|C|} \right)^{1/2} + \Big| |A \cap B_c| - |\mathcal{A} \cap B^c| \Big|,$$

donde $B_c = B \setminus (B + c)$ y $B^c = (B + c) \setminus B$.

El conjunto de Sidon $\mathcal{A}$ y el conjunto B se elegirán de manera adecuada para cada problema, y el conjunto C es un conjunto auxiliar que elegiremos para minimizar la parte derecha de la desigualdad.

Por ejemplo, si B es un subgrupo, elegiremos $C = B$. De esa manera $B_c = B^c = \emptyset$ y obtenemos la estimación

$$\left||\mathcal{A} \cap B| - \frac{|\mathcal{A}||B|}{|G|}\right| \leq (3p)^{1/2}. \tag{2}$$

3.1. El último Teorema de Fermat en $\mathbb{F}_p$

El último teorema de Fermat, finalmente demostrado por Wiles, afirma que la ecuación $x^n+y^n = z^n$, $xyz \neq 0$, no tiene soluciones enteras si $n \geq 3$. Es conocido que sin embargo la ecuación $x^n + y^n \equiv z^n \pmod p$, $xyz \neq 0$, sí que tiene soluciones si p es suficientemente grande. Existe una demostración combinatoria debida a Schur y basada en la teoría de Ramsey que da una estimación muy mala para el tamaño de p a partir del cual la ecuación tiene solución. La demostración clásica que proporciona la mejor estimación que se conoce para p expresa el número de soluciones de la ecuación de Fermat como una suma trigonométrica. A partir de ahí se obtiene un término principal y un error que se puede estimar acotando las sumas trigonométricas restantes.

Veremos cómo se pueden utilizar los conjuntos de Sidon para conseguir este mismo resultado utilizando solamente métodos combinatorios.

Antes, una pequeña observación. Como el grupo multiplicativo $\mathbb{F}_p^*$ es un grupo cíclico de $p-1$ elementos, la ecuación de Fermat se convierte en trivial si $(n, p-1) = 1$, porque todos los elementos de $\mathbb{F}_p^*$ son n-potencias. Es fácil ver que el estudio de la ecuación de Fermat puede reducirse a los casos donde $n \mid (p-1)$.

Teorema 1. *Sea $n \mid (p-1)$, con p primo. La ecuación $x^n+y^n \equiv z^n \pmod p$, $xyz \neq 0$, tiene $p^2 + O(p^{3/2}n^2)$ soluciones.*

En particular, si $p \gg n^4$ la ecuación de Fermat tiene soluciones en $\mathbb{F}_p$.

Demostración. Como todo elemento en $\mathbb{F}_p$ distinto de 0 tiene inverso, cada solución de la ecuación $x^n + y^n \equiv 1 \pmod p$, $xy \neq 0$, genera $p-1$ soluciones de la ecuación original. A su vez, si g es una raíz primitiva, cada solución de la ecuación $g^x + g^y \equiv 1 \pmod p$, $x, y \in n\mathbb{Z}_{p-1}$, corresponde a n^2 soluciones de la ecuación anterior. Resumiendo,

$$\#\{(x,y),\ g^x + g^y = 1,\ x, y \in n\mathbb{Z}_{p-1}\} = \frac{\#\{(x,y,z),\ x^n + y^n = z^n,\ xyz \neq 0\}}{(p-1)n^2}.$$

Pero la cantidad de la izquierda es justamente $|\mathcal{A} \cap B|$, donde $\mathcal{A}$ es el conjunto de Sidon de $p-2$ elementos $\mathcal{A} = \{(x,y),\ g^x + g^y \equiv 1 \pmod p\} \subset \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$ comentado en la subsección 2.4 y B es el subgrupo $B = (n\mathbb{Z}_{p-1}) \times (n\mathbb{Z}_{p-1})$.

Finalmente utilizamos (2) y el hecho de que, en este caso, $\frac{|\mathcal{A}||B|}{|G|} = \frac{p-2}{n^2}$. □

3.2. Distribución de residuos cuadráticos

Si p es primo, la mitad de los restos no nulos (mód p) son cuadrados y la otra mitad no lo son. Los $(p-1)/2$ residuos cuadráticos coinciden con el conjunto $\{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\}$. Por ejemplo, si $p = 13$, los residuos cuadráticos son $1, 3, 4, 9, 10, 12$, y los no cuadráticos $2, 5, 6, 7, 8, 11$.

Si nos dedicamos a calcular los residuos cuadráticos para primos grandes, observaremos que aparentemente están bien distribuidos en $\mathbb{Z}_p$; es decir, que aproximadamente la mitad de los restos en cada intervalo son residuos cuadráticos.

El siguiente resultado es clásico y su demostración utiliza las desigualdades de Pólya-Vinogradov para sumas trigonométricas. La demostración que presentamos aquí es puramente combinatoria.

Teorema 2. *Sea p un número primo. Para todo $\epsilon > 0$, el número de residuos cuadráticos en un intervalo $I \subset \mathbb{Z}_p$ es $|I|/2 + O(p^{1/2+\epsilon})$.*

Demostración. La primera observación es que como $(-x)^2 \equiv x^2 \pmod p$, el número de elementos del conjunto de Sidon $\mathcal{A} = \{(x, x^2),\ x \in \mathbb{Z}_p \setminus \{0\}\}$ que están en $B = \mathbb{Z}_p \times I$ cuenta exactamente dos veces el número de residuos cuadráticos en I. Es decir,

$$\#\{\text{residuos cuadráticos en } I\} = \frac{|\mathcal{A} \cap B|}{2}.$$

Una vez traducido nuestro problema a estimar el número de elementos de un conjunto de Sidon $\mathcal{A}$ que pertenecen a un conjunto B, podemos utilizar el lema 1.

Será conveniente elegir el conjunto auxiliar $C = \mathbb{Z}_p \times [0, |I|/p^{2\epsilon}]$. En esta situación, el lema 1 da lugar a la desigualdad

$$\left| |\mathcal{A} \cap B| - \frac{|\mathcal{A}||B|}{|G|} \right| \leq 2p^{1/2+\epsilon} + \left| |\mathcal{A} \cap B_c| - |\mathcal{A} \cap B^c| \right|$$

para algún $c \in C$. Los nuevos conjuntos B_c y B^c son también conjuntos de la forma $B_c = \mathbb{Z}_p \times I_c$ y $B^c = \mathbb{Z}_p \times I^c$ donde I_c y I^c son intervalos de la misma longitud, pero ahora de longitud $|I_c| = |I^c| \leq |I|p^{-2\epsilon}$. Esto nos permite escribir

$$\left| |\mathcal{A} \cap B_c| - |\mathcal{A} \cap B^c| \right| \leq \left| |\mathcal{A} \cap B_c| - \frac{|\mathcal{A}||B_c|}{|G|} \right| + \left| |\mathcal{A} \cap B^c| - \frac{|\mathcal{A}||B_c|}{|G|} \right|.$$

Ahora iteramos el argumento para estos nuevos conjuntos. En cada paso, los intervalos I reducen su longitud en un factor $p^{-2\epsilon}$. Después de no más de ϵ^{-1} iteraciones, habremos conseguido que los intervalos tengan longitud $|I_c| = |I^c| = 1$, y en cada uno de ellos habrá como mucho un residuo cuadrático. □

3.3. Raíces primitivas

Si g es una raíz primitiva, sus potencias $g, g^2, \ldots, g^{p-1}$ generan todo $\mathbb{Z}_p$ excepto el 0. Si en lugar de considerar todas las potencias, consideramos las primeras, pongamos $g, g^2, \ldots, g^m$, es de esperar que estos elementos estén bien distribuidos en $\mathbb{Z}_p$. De hecho, éste es un algoritmo que se utiliza para generar números aleatorios.

Los conjuntos de Sidon también permiten dar una prueba combinatoria de este hecho.

Teorema 3. *Sea g una raíz primitiva en $\mathbb{F}_p$. Para todo $\epsilon > 0$ y cualesquiera intervalos $I, J \subset \mathbb{Z}_p$, el número de potencias g^x, $x \in I$, que están en J es $|I||J|/p + O(p^{1/2+\epsilon})$.*

Demostración. El problema se traduce en estimar $|\mathcal{A} \cap B|$ donde $\mathcal{A}$ es el conjunto de Sidon $\mathcal{A} = \{(x, g^x),\ x \in \mathbb{Z}_{p-1}\} \subset \mathbb{Z}_{p-1} \times \mathbb{Z}_p$ y B el subconjunto $B = I \times J$. Se procede de manera similar al caso anterior. □

4. Sucesiones de Sidon infinitas

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

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

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

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

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

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

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

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

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

Erdős [27] demostró que no existe tal sucesión. Más concretamente, demostró que si $\mathcal{A}$ es una sucesión de Sidon infinita entonces

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

Como contrapunto a este resultado, Krückeberg [19] demostró la existencia de una sucesión de Sidon con

$$\limsup_{n\to\infty} \frac{\mathcal{A}(n)}{\sqrt{n}} = \frac{1}{\sqrt{2}}$$

y Erdős conjeturó que la constante $1/\sqrt{2}$ puede ser sustituida por 1. Hay buenas razones, sin embargo, para dudar de la veracidad de esta conjetura.

¿Cuál es el menor crecimiento que puede tener una sucesión de Sidon? ¿Para qué valores de α existe una sucesión de Sidon $\mathcal{A}$ con $\mathcal{A}(n) \gg n^{\alpha}$?

Erdős conjeturó que para todo $\alpha < 1/2$.

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

La sucesión de Mian-Chowla definida al principio de la sección 2 satisface $\mathcal{A}(n) \geq n^{1/3}$. Ajtai, Kolmos y Szemerédi [2] demostraron la existencia de una sucesión infinita de Sidon tal que $\mathcal{A}(n) \gg (n \log n)^{1/3}$.

Y así estaban las cosas hasta que, hace diez años, Ruzsa [26] sorprendió con una construcción realmente ingeniosa que demostraba la existencia de una sucesión infinita con

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

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

Imre Ruzsa

Para cada número real $\beta \in (1,2)$ Ruzsa considera la sucesión $\mathcal{A}_\beta = \{a_p,\ p \text{ primo}\}$ donde cada término a_p se construye barajando de una manera muy ingeniosa los dígitos de la expansión binaria de $\beta \log p$, para luego sacar partido al hecho de que los primos forman una sucesión de Sidon multiplicativa. Finalmente demuestra con argumentos probabilísticos que, para casi todo β, a la sucesión $\mathcal{A}_\beta$ le podemos quitar unos pocos elementos para que sea de Sidon.

La parquedad de nuestra breve explicación no hace justicia a los argumentos tan sutiles que Ruzsa utilizó en esta construcción. Si definimos

$$\alpha_1 = \sup\left\{\liminf_{n\to\infty} \frac{\log \mathcal{A}(n)}{\log n},\ \mathcal{A} \text{ Sidon}\right\},$$

los resultados anteriores implican que

$$\sqrt{2} - 1 \leq \alpha_1 \leq 1/2.$$

La cota inferior se deduce de la construcción de Ruzsa, y la cota superior es consecuencia de la estimación trivial $\mathcal{A}(n) \ll n^{1/2}$ para cualquier conjunto de Sidon. Con esta notación la conjetura 2 se traduce en que $\alpha_1 = 1/2$.

Las construcciones de Szemerédi y de Ruzsa son probabilísticas, por lo que no ofrecen una construcción explícita de la sucesión. Incluso en la sucesión de Mian-Chowla, aunque es determinística, el valor de a_n depende del cálculo de todos los anteriores términos. Hasta hace muy poco no se conocía ninguna sucesión de Sidon con un crecimiento polinómico que fuese explícita.

Recientemente [6] hemos construido una sucesión de Sidon explícita con $\mathcal{A}(n) \gg n^{1/3-o(1)}$, cuyo término enésimo es

$$a_n = \sum_{j\geq 1} 2^{\frac{3j^2+j}{2}-2}\left(\lfloor 2^{-j(j-1)/2}(n)_{2^{j(j+1)/2}}\rfloor + 2^{j+1}\lfloor 2^{-j(j-1)}(n^2)_{2^{j(j+1)}}\rfloor\right), \qquad (3)$$

donde $(x)_m$ es el menor residuo no negativo congruente con $x \mod m$.

En la siguiente sección daremos una idea de dónde proviene esta construcción.

5. Conjuntos de Sidon en dimensiones superiores

¿Cuántos puntos de coordenadas enteras podemos situar en el cuadrado $[1,n]^2$ *sin que haya cuatro formando un paralelogramo?*

Los tres ejemplos de conjuntos de Sidon en grupos bidimensionales descritos en la sección 2 son en particular conjuntos de Sidon en $\mathbb{N}\times\mathbb{N}$. Obsérvese que la condición de ser conjunto de Sidon en $\mathbb{N}^2$ es equivalente a no contener cuatro puntos que formen un paralelogramo.

Si definimos $F(n,n) = \max\{|\mathcal{A}|,\ \mathcal{A}\subset[1,n]^2,\ \mathcal{A}\text{ Sidon}\}$, ¿cuál es el valor de $F(n,n)$?

Lindström [22] demostró que $F(n,n) \leq n + O(n^{2/3})$ y conjeturó que

$$F(n,n) \leq n + O(1).$$

Aunque la conjetura análoga para el caso de dimensión uno parece inaccesible hoy en día, hemos podido demostrar [6] que, para infinitos valores de n,

$$F(n,n) > n + \log n \log\log\log n,$$

refutando así la conjetura de Lindström. Probablemente $F(n,n) < n + O(n^\epsilon)$ para todo $\epsilon > 0$. Pero si esta conjetura fuese cierta será realmente difícil de demostrar porque, como hemos obervado en [6], implicaría la conjetura de Vinogradov; a saber, que para todo $\epsilon > 0$ y para todo primo p suficientemente grande, el menor residuo cuadrático mód p es menor que p^ϵ.

En el caso de sucesiones de Sidon infinitas en $\mathbb{N}^2$ se ha demostrado [6] que, análogamente a lo que ocurría en dimensión uno, para toda sucesión de Sidon infinita se tiene que $\liminf_{n\to\infty} \mathcal{A}(n,n)/(n/\log n) < \infty$.

En [6] también se describe una manera explícita de transformar sucesiones de Sidon infinitas en $\mathbb{N}^d$ en sucesiones de Sidon en $\mathbb{N}$, y viceversa, de manera eficiente; es decir, sin perder mucha densidad. Si definimos $\mathcal{A}([1,n]^d) = |\mathcal{A}\cap[1,n]^d|$ y

$$\alpha_d = \sup\left\{\liminf_{n\to\infty}\frac{\log\mathcal{A}([1,n]^d)}{\log n},\ \mathcal{A}\text{ Sidon en }\mathbb{N}^d\right\},$$

la transformación a la que nos referimos permite demostrar que $\alpha_d = d\alpha_1$. Esto nos permite concluir que el problema de encontrar sucesiones de Sidon infinitas es equivalente en todas las dimensiones.

El interés de este resultado es que las construcciones de conjuntos de Sidon parecen ser más sencillas en dimensiones superiores. Por ejemplo, la sucesión infinita $\mathcal{A} = \{(n, n^2),\ n \in \mathbb{N}\}$ es una sucesión de Sidon en $\mathbb{N}^2$ que se convierte, mediante una variante de la transformación anterior, en la sucesión descrita en (3).

6. Conjuntos B_h

La noción de conjunto de Sidon se extiende de manera natural a conjuntos donde todas las sumas de h elementos del conjunto son distintas. Los conjuntos de Sidon son precisamente los conjuntos B_2, y se los denomina de las dos maneras.

¿Cuál es el mayor tamaño que puede tener un conjunto B_h en $\{1, \ldots, N\}$?

Para $h \geq 3$ se desconoce cuál es el comportamiento asintótico de esta cantidad, a la que denominaremos $F_h(N)$. Es decir,

$$F_h(N) = \text{máx}\{|\mathcal{A}|,\ \mathcal{A} \subset \{1, \ldots, N\},\ \mathcal{A} \in B_h\}.$$

Se conjetura que $F_h(N) \sim N^{1/h}$ para todo $h \geq 2$, pero sólo se sabe para el caso $h = 2$.

Para q una potencia de un primo, Bose y Chowla [4] construyeron un conjunto B_h en $\mathbb{Z}_{q^h-1}$ con q elementos que, emulando el argumento utilizado en la sección 2 para los conjuntos de Sidon, nos proporciona la cota inferior

$$N^{1/h}(1 + o(1)) \leq F_h(N).$$

La cota superior es mucho más esquiva. El número de sumas ordenadas de h elementos es $\binom{|\mathcal{A}|+h-1}{h}$, y como todas las sumas son $\leq hN$, el principio del palomar nos da una primera cota superior (trivial), $F_h(N) \leq (h \cdot h!)^{1/h} N^{1/h}$.

En 1969 Lindström [21] demostró que $F_4(N) \leq 8^{1/4} N^{1/4}$. La euforia del que escribe estas líneas cuando, después de 30 años de la cota de Lindström, consiguió mejorarla [5] hasta $F_4(N) \leq (7{,}83)^{1/4} N^{1/4}$ duró poco. En su primer artículo, Ben Green [16] rebajó esta cota hasta $F_4(N) \leq 7^{1/4} N^{1/4}$.

6.1. Sucesiones B_h infinitas

Si las dificultades para obtener buenas estimaciones de conjuntos B_h finitos con $h \geq 3$ son grandes, no lo son menos para sucesiones infinitas.

Si $\mathcal{A} \in B_h$ es una sucesión infinita, entonces $\mathcal{A}(n) \leq F_h(n) \ll n^{1/h}$, por lo que cabe preguntarse si existe alguna tal que $\mathcal{A}(n) \gg n^{1/h}$.

Para h par se sabe que la respuesta es negativa, pero para h impar el problema está completamente abierto, incluso para el primer caso $h = 3$.

La sucesión de Sidon de Mian-Chowla se puede generalizar fácilmente a sucesiones B_h. Definimos $a_1 = 1$ y, por recursión, definimos a_n como el menor entero positivo tal que $a_n \neq a_{i_1} + \cdots + a_{i_h} - (a_{i_{h+1}} + \cdots + a_{i_{2h-1}})$, $i_1, \ldots, i_{2h-1} \leq n-1$. Como a lo más hay $(n-1)^{2h-1}$ enteros prohibidos, necesariamente $a_n \leq (n-1)^{2h-1} + 1$.

En términos de la función contadora esta sucesión satisface $\mathcal{A}(n) \gg n^{1/(2h-1)}$ y no se conoce ninguna construcción más densa que ésta. La construcción de Ruzsa para el caso $h = 2$ no ha conseguido adaptarse para $h \geq 3$.

Conjetura 3. *Para todo $\epsilon > 0$ existe una sucesión $\mathcal{A} \in B_h$ tal que $\mathcal{A}(n) \gg n^{1/h-\epsilon}$.*

7. Los conjuntos $B_2[g]$ y la conjetura de Erdős-Turán

Dado un conjunto de enteros $\mathcal{A}$ se define $r(\mathcal{A}, n)$ como el número de representaciones de n de la forma $n = a + a'$, con $a \leq a'$, $a, a' \in \mathcal{A}$. Por ejemplo, podemos definir los conjuntos de Sidon como aquéllos tales que $r(\mathcal{A}, n) \leq 1$ para todo n.

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

La respuesta es que no. Los analistas apreciarán sin duda el siguiente argumento de Dirac [11]. Sea la función $f(z) = \sum_{a \in \mathcal{A}} z^a$, $|z| < 1$. Entonces

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

donde $\tilde{r}(\mathcal{A}, n)$ cuenta el número de representaciones de $n = a + a'$, $a, a' \in \mathcal{A}$. Observando que $\tilde{r}(\mathcal{A}, n) = 2r(\mathcal{A}, n) - 1$, si $n = 2a$ para algún $a \in \mathcal{A}$, y $\tilde{r}(\mathcal{A}, n) = 2r(\mathcal{A}, n)$ en otro caso, podemos escribir

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

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

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

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

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

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

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

Aquí es donde hace su aparición la que se considera la conjetura más importante en la teoría aditiva de números.

Conjetura 4 (Erdős-Turán). *Si $r(\mathcal{A}, n) \geq 1$ para todo $n \geq 1$, la función $r(\mathcal{A}, n)$ no está acotada uniformemente en n.*

Aunque parece que se está muy lejos de demostrar esta conjetura por la que Erdős ofrecía 500 dólares, hay sin embargo algunos resultados prometedores. Nesetril y Serra [24] han hecho uso de la teoría de Ramsey para demostrar que la conjetura de Erdős-Turán es cierta para una clase muy extensa de sucesiones.

Finalizamos esta sección con una variante de la conjetura.

¿Existe alguna sucesión de enteros positivos $\mathcal{A}$ con la propiedad de que todo entero positivo se puede representar de manera única como diferencia de dos elementos de $\mathcal{A}$?

A estos conjuntos se les denomina conjuntos de diferencias perfectas y su construcción es muy sencilla.

Empecemos con $\mathcal{A}_1 = \{0, 1\}$, que nos sirve para representar el 1. Para representar el 2 añadiremos dos nuevos elementos $\{x, x + 2\}$ que no den lugar a diferencias que ya teníamos. Por ejemplo $\mathcal{A}_2 = \mathcal{A}_1 \cup \{4, 6\}$. En el paso k, si la diferencia k ya había aparecido anteriormente no añadimos ningún elemento, $\mathcal{A}_k = \mathcal{A}_{k-1}$. Y si no había aparecido todavía, definimos $\mathcal{A}_k = \mathcal{A}_{k-1} \cup \{x, x + k\}$ donde x es el menor entero positivo tal que los dos nuevos elementos añadidos no dan lugar a diferencias repetidas. El conjunto $\mathcal{A} = \cup_k \mathcal{A}_k$ es un conjunto de diferencias perfectas.

Lo difícil en este problema es construir un conjunto de diferencias perfectas lo más denso posible. Dado que los conjuntos de diferencias perfectas son en particular conjuntos de Sidon, no podemos esperar ningún resultado mejor sobre la densidad de estos conjuntos de los que se tienen para los conjuntos de Sidon.

Pero sí nos podemos servir de los conjuntos de Sidon para construir conjuntos de diferencias perfectas densos; de hecho casi tan densos como cualquier conjunto de Sidon dado. En [8] se demuestra que para cualquier conjunto de Sidon B existe un conjunto de diferencias perfectas $\mathcal{A}$ tal que $\mathcal{A}(x) \gg B(x/3)$. En particular, existe un conjunto $\mathcal{A}$ de diferencias perfectas con $\mathcal{A}(x) \gg x^{\sqrt{2}-1-o(1)}$.

7.1. Sucesiones $B_2[g]$

Se dice que un conjunto $\mathcal{A}$ es un conjunto $B_2[g]$, o simplemente $\mathcal{A} \in B_2[g]$, si $r(\mathcal{A}, n) \leq g$ para todo n. Y se define

$$F(N, g) = \text{máx}\{|\mathcal{A}|,\ \mathcal{A} \subset \{1, \ldots, N\},\ \mathcal{A} \in B_2[g]\}.$$

El caso $g = 1$ corresponde a los conjuntos de Sidon y ya hemos visto en una sección anterior que $F(N, 1) \sim N^{1/2}$.

Para $g \geq 2$ el problema se complica mucho más. Durante mucho tiempo las únicas estimaciones conocidas eran la que se obtiene de manera trivial utilizando el principio del palomar (para la cota superior) y la que se obtiene pegando conjuntos de Sidon de la manera obvia,

$$(gN)^{1/2} \leq F(N, g) \leq 2(gN)^{1/2}.$$

Ni siquiera se sabe si existe $\lim_{N\to\infty} \frac{F(N,g)}{N^{1/2}}$. Pero los nuevos métodos utilizados en [9] han ido depurándose para obtener sucesivas mejoras de estas estimaciones. Si llamamos

$$\alpha(g) = \liminf_{N\to\infty} \frac{F(N,g)}{N^{1/2}}, \qquad \beta(g) = \limsup_{N\to\infty} \frac{F(N,g)}{N^{1/2}},$$

los mejoras sucesivas han sido las siguientes:

$$\begin{array}{ll} \frac{\beta(g)}{\sqrt{g}} \geq 1 & ([18]) \\ \geq 1{,}06 - \epsilon_g & ([9]) \\ \geq \frac{11}{\sqrt{96}} - \epsilon_g & ([23]) \\ \geq \frac{2}{\sqrt{\pi}} - \epsilon_g & ([10]) \end{array} \qquad \begin{array}{ll} \frac{\alpha(g)}{\sqrt{g}} \leq 2 & (\text{trivial}) \\ \leq 1{,}864 & ([9]) \\ \leq 1{,}844 & ([16]) \\ \leq 1{,}839 & ([23]) \\ \leq 1{,}789 & ([28]) \end{array}$$

donde $\epsilon_g \to 0$ cuando $g \to \infty$. Es decir,

$$\frac{2}{\sqrt{\pi}} - \epsilon_g \leq \frac{\beta(g)}{\sqrt{g}} \leq \frac{\alpha(g)}{\sqrt{g}} \leq 1{,}789.$$

Como este ensayo está lleno de conjeturas, también me permito yo hacer una:

CONJETURA 5. $\liminf_{g\to\infty} \frac{\beta(g)}{\sqrt{g}} = \limsup_{g\to\infty} \frac{\alpha(g)}{\sqrt{g}} = 2/\sqrt{\pi}$.

8. PROBLEMAS SIN RESOLVER

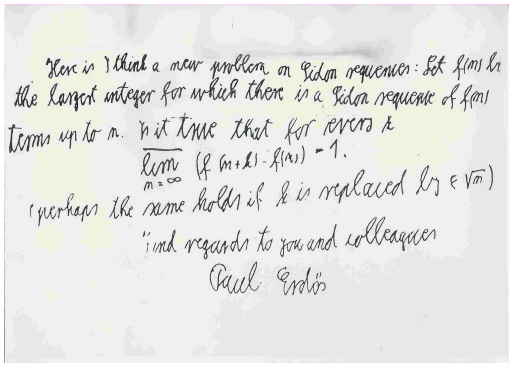
Un artículo donde el principal protagonista es Erdős no puede dejar de contener una sección dedicada a problemas abiertos. Erdős propuso muchos problemas en su vida, y solía ofrecer una cantidad por la resolución de algunos de ellos, en función de la dificultad de cada problema.

Hace años recibí una carta de Erdős donde me contestaba muy amablemente sobre una consulta que le hice referente a sucesiones de Sidon en los cuadrados. No puedo evitar reproducir el fragmento de la carta donde se despedía, como era su estilo, proponiendo un nuevo problem.

Here is I think a new problem on Sidon sequences: Let $f(n)$ be the largest integer for which there is a Sidon sequence of $f(n)$ terms up to n. Is it true that for every k

$$\overline{\lim_{n\to\infty}} \, (f(n+k) - f(n)) = 1?$$

(perhaps the same holds if k is replaced by $\epsilon\sqrt{n}$).


Here is I think a new problem on Sidon sequences: Let f(n) be the largest integer for which there is a Sidon sequence of f(n) terms up to n. Is it true that for every k
lim (f(n+k) - f(n)) = 1.
(perhaps the same holds if k is replaced by ε√n)
Kind regards to you and colleagues
Paul Erdős

Exponemos a continuación una amplia lista de problemas abiertos, así como diversos comentarios sobre su estado actual.

1. *Conjetura de Erdős-Turán: Sea $\mathcal{A}$ una sucesión infinita de enteros positivos. Si $r(\mathcal{A}, n) \geq 1$ para todo n, entonces $r(\mathcal{A}, n)$ no está acotada superiormente.*

Erdős y Renyi, con métodos probabilísticos, demostraron la existencia de una sucesión cumpliendo $1 \leq r(\mathcal{A}, n) \ll \log n$.

Ruzsa ha construido una sucesión $\mathcal{A}$ tal que $1 \leq r(\mathcal{A}, n)$ para todo n y $\sum_{n \leq x} r^2(\mathcal{A}, n) \ll x$.

El análogo multiplicativo de la conjetura de Erdős-Turán es cierto: *Si $p(\mathcal{A}, n) \geq 1$ para todo n, entonces $p(\mathcal{A}, n)$ no está acotada superiormente.* Ahora $p(\mathcal{A}, n)$ cuenta el número de representaciones de n de la forma $n = aa'$, con $a, a' \in \mathcal{A}$.

2. *Conjetura: Si $\mathcal{A}$ es una sucesión infinita de enteros positivos y $\mathcal{A}(x) \gg x^{1/2}$ entonces $r(\mathcal{A}, n)$ no está acotada.*

Obsérvese que, si $r(\mathcal{A}, n) \geq 1$ para todo n, entonces $\mathcal{A}(x)^2 \geq \sum_{1 \leq n \leq x} r(A, n) \geq x$, por lo que esta conjetura implica en particular la conjetura de Erdős-Turán.

3. *Conjetura: Para todo $\epsilon > 0$ existe una sucesión de Sidon tal que $\mathcal{A}(n) \gg n^{1/2-\epsilon}$*

Ruzsa ha demostrado que tal sucesión existe para el exponente $\sqrt{2} - 1 - \epsilon$.

Erdős y Renyi [14] demostraron que, para todo $\epsilon > 0$, existe un g y una sucesión $\mathcal{A} \in B_2[g]$ tal que $\mathcal{A}(x) \gg x^{1/2-\epsilon}$. Este trabajo inauguró el uso de los métodos probabilísticos en la teoría aditiva de números.

4. *¿Existe alguna sucesión infinita $\mathcal{A} \in B_3$ tal que $\mathcal{A}(n) \gg n^{1/3}$?*

Para h par se sabe que no existe ninguna sucesión $\mathcal{A} \in B_h$ tal que $\mathcal{A}(x) \gg x^{1/h}$. No se sabe la respuesta para ningún h impar, aunque se cree que tampoco existen.

5. *Conjetura: Existe una sucesión de Sidon $\mathcal{A}$ tal que* $\limsup \frac{\mathcal{A}(n)}{n^{1/2}} = 1$.

Esta conjetura de Erdős puede ser falsa. Quizás sólo se puede llegar a $1/\sqrt{2}$.

6. *¿Cuál es el conjunto de Sidon de mayor tamaño en $\mathbb{Z}_n$?*

Se sabe con exactitud para $n = q^2 + q + 1$, $n = q^2 - 1$ y $n = p(p-1)$. Para cualquier otro n no se conoce absolutamente nada que no sea trivial. Es fácil observar que cualquier conjunto de Sidon en $\{1, \ldots, [n/2]\}$ es, en particular, un conjunto de Sidon en $\mathbb{Z}_n$, por lo que $\mathbb{Z}_n$ contiene al menos un conjunto de Sidon de $\sim \sqrt{n/2}$ elementos.

7. *¿Existe una sucesión $\mathcal{A} \in B_h$ tal que $\limsup_{n \to \infty} \mathcal{A}(n)/n^{1/h} > 0$?*

Krükeberger construyó una sucesión B_2 para la que este límite es $1/\sqrt{2}$. Aunque en [17] se afirma que esta construcción se puede generalizar fácilmente para todo $h \geq 3$, eso no es cierto.

8. *Encontrar un polinomio $p(x)$ tal que la sucesión $p(1), p(2), \ldots, p(n), \ldots$ sea de Sidon.*

Se cree que $p(x) = x^5$ es uno de ellos.

9. *Demostrar que $F(n) \leq n^{1/2} + O(n^{\epsilon})$, o al menos mejorar la estimación $F(n) \leq n^{1/2} + n^{1/4} + 1$.*

Incluso demostrar que $F(n) \leq n^{1/2} + 0{,}999n^{1/4}$ sería algo verdaderamente notable.

10. *Demostrar que* $F(n,n) < n + O(n^{\epsilon})$ *para todo* $\epsilon > 0$.
Se sabe cierto para $\epsilon = 2/3$.

11. *¿Es cierto que todo conjunto de* n *enteros contiene un conjunto de Sidon de tamaño* $\sim n^{1/2}$*?*
Se sabe [1] que todo conjunto de n enteros contiene un subconjunto de Sidon de más de $\frac{2}{25}n^{1/2}$ elementos.

12. *¿Existe un conjunto de Sidon convexo* $\mathcal{A} \subset \{1,\dots,n\}$ *con* $|\mathcal{A}| \gg n^{1/2}$*?*
Por conjunto convexo se entiende un conjunto con diferencias consecutivas crecientes. Se cree que no existe ningún conjunto de estas características.

13. *¿Cuál es el mayor tamaño de un conjunto de Sidon* $\mathcal{A} \subset \{1^2,\dots,n^2\}$?
Se sabe que existe alguno con $\gg n^{2/3}$ elementos. No se sabe si puede haberlos de tamaño $\gg n^{1-\epsilon}$.

14. *¿Cuál es el mayor tamaño de un conjunto de Sidon* $\mathcal{A} \subset \{1,\dots,n\}$ *con la propiedad de que todos los productos de dos elementos del conjunto son también distintos?*
Es decir, se pregunta por conjuntos que sean simultáneamente conjuntos de Sidon aditivos y multiplicativos. Ruzsa conjetura que el tamaño debería ser $\sim n^{1/2}$.

15. *¿Cuál es el crecimiento de la sucesión de Mian-Chowla?*

16. *¿Cuántos subconjuntos de Sidon hay en* $\{1,\dots,n\}$*?*
Si llamamos $F(n)$ al tamaño del mayor conjunto de Sidon en $\{1,\dots,n\}$ y $S(n)$ al número de subconjuntos de Sidon en $\{1,\dots,n\}$ se tiene la estimación trivial, $2^{F(n)} \leq S(n) \leq \sum_{j=1}^{F(n)} \binom{n}{j}$. Como sabemos que $F(n) \sim n^{1/2}$, la estimación anterior se traduce en $n^{1/2} \ll \log S(n) \ll n^{1/2}\log n$. Cualquier mejora de estas estimaciones sería interesante.

Agradecimientos: Quisiera agradecer a Fernando Chamizo, Adolfo Quirós y Carlos Vinuesa las oportunas observaciones y correcciones al manuscrito preliminar.

Referencias

[1] H. L. Abbot, Sidon sets, *Canadian Mathematical Bulletin* **32** (1990), 335–341.

[2] M. Ajtai, J. Kolmos y E. Szemeredi, A dense infinite Sidon sequence, *European Journal of Combinatorics* **2** (1981), 1–11.

[3] R. C. Baker, G. Harman y J. Pintz, The difference between consecutive primes, II, *Proceedings of the London Mathematical Society* **83** (2001), 532–562.

[4] R. C. Bose y S. Chowla, Theorems in the additive theory of numbers, *Commentarii Mathematici Helvetici* **37** (1962/1963), 141–147.

[5] J. Cilleruelo, New upper bounds for B_h sequences, *Advances in Mathematics* (2001) **159**, n.º 1, 1–17.

[6] J. Cilleruelo, Sidon sets in higher dimensions. *En preparación.*

[7] J. Cilleruelo, Sidon sets and the distribution of powers in $\mathbb{F}_p$. *En preparación.*

[8] J. Cilleruelo y M. Nathanson, Perfect difference sets constructed from Sidon sets, *Combinatorica. En prensa.*

[9] J. Cilleruelo, I. Ruzsa y C. Trujillo, Upper and lower bounds for finite $B_2[g]$ sequences, *Journal of Number Theory* **97** (2002), n.º 1, 26–34.

[10] J. Cilleruelo y C. Vinuesa, $B_h[g]$ sequences and the Schinzel's conjecture. *En preparación.*

[11] G. A. Dirac, Note on a problem in additive number theory, *Journal of the London Mathematical Society* **26** (1951), 312–313.

[12] P. Erdős, Carta personal fechada el 22 de marzo de 1991.

[13] P. Erdős, On a problem of Sidon in additive number theory, *Acta Scientiarum Mathematicarum Univ. Szeged* **15** (1953/54), 255–259.

[14] P. Erdős y A. Renyi, Additive properties of random sequences of positive integers, *Acta Arithmetica* **6** (1960), 83–110.

[15] P. Erdős y P. Turán, On a problem of Sidon in additive number theory and some related problems, *Journal of the London Mathematical Society* **16** (1941), 212–215; Addendum (por P. Erdős), *ibid.* **19** (1944), 208.

[16] B. Green, The number of squares and $B_h[g]$ sequences, *Acta Arith.* **100** (2001), 365–390.

[17] H. Halberstam y K. F. Roth, *Sequences, vol. I*, Oxford University Press, 1966 (2nd ed., Springer-Verlag, New York, 1983).

[18] M. Kolountzakis, The density of $B_h[g]$ sequences and the minimun of dense cosine sums, *Journal of Number Theory* **56** (1996), 4–11.

[19] F. Krückeberg, B_2-Folgen und verwandte Zahlenfolgen, *Journal für die reine und angewandte Mathematik* **206** (1961), 53–60.

[20] B. Lindström, An inequality for B_2-sequences, *Journal of Combinatorial Theory* **6** (1969), 211–212.

[21] B. Lindström, A remark on B_4-sequences, *Journal of Combinatorial Theory* **7** (1969), 276–277.

[22] B. Lindström, On B_2-sequences of vectors, *Journal of Number Theory* **4** (1972), 261–265.

[23] G. Martin y K. O'Bryant, Constructions of generalized Sidon sets, *Journal of Combinatorial Theory, Ser. A* **113** (2006), n.º 4, 591–607.

[24] J. Nesetril y O. Serra, The Erdős-Turán property for a class of bases, *Acta Arithmetica* **115** (2004) n.º 3, 245–254.

[25] I. Ruzsa, Solving a linear equation in a set of integers I, *Acta Arithmetica* **65** (1993), 259–282.

[26] I. Ruzsa, An infinite Sidon sequence, *Journal of Number Theory* **68** (1998), 63–71.

[27] A. Stör, Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe. I, II, *Journal für die reine und angewandte Mathematik* **194** (1955), 40–65, 111–140.

[28] G. Yu, An upper bound for $B_2[g]$ sets, *Journal of Number Theory* **122** (2007), 211–220.

Javier Cilleruelo, Dpto. de Matemáticas, Facultad de Ciencias, Universidad Autónoma de Madrid, 28049-Cantoblanco (Madrid)

Correo electrónico: franciscojavier.cilleruelo@uam.es