El diablo de los números

Sección a cargo de

Javier Cilleruelo Mateo

Problemas combinatorios sobre bases aditivas

por

Alain Plagne

1 Introducción

Todos los lectores del *Diablo* saben que *todo entero positivo puede ser escrito como la suma de cuatro cuadrados*. Este famoso resultado fue demostrado por Lagrange en 1770. Seguramente también conocen el problema de Waring que generaliza el teorema de los cuatro cuadrados de Lagrange y que Hilbert demostró en 1909 [18]: *para todo $k \in \mathbb{N}$, existe un $g(k)$ tal que todo entero positivo puede ser escrito como la suma de $g(k)$ potencias k-ésimas.* Por último, la conjetura de Goldbach (1742) no es menos conocida: afirma que *todos los pares positivos mayores que* 2 *pueden ser escritos como la suma de dos números primos* (este resultado es aún hoy una conjetura).

Todos estos problemas, muy famosos todos ellos, son problemas de bases aditivas, el tema central de este artículo.

Vamos a utilizar las siguiente notación clásica. Si $\mathcal{A}$ y $\mathcal{B}$ son dos conjuntos de números enteros naturales o, en general, dos subconjuntos de un grupo, vamos a escribir $\mathcal{A}+\mathcal{B}$ para designar el conjunto suma de esos dos conjuntos, es decir,

$$\mathcal{A}+\mathcal{B} = \{a+b \ : \ a \in \mathcal{A}, \ b \in \mathcal{B}\}.$$

Escribimos $2\mathcal{A}$ para $\mathcal{A}+\mathcal{A}$ y si $k \in \mathbb{N}$, $k\mathcal{A} = (k-1)\mathcal{A}+\mathcal{A}$. También vamos a definir

$$\mathcal{A}-\mathcal{B} = \{a-b \ : \ a \in \mathcal{A}, \ b \in \mathcal{B}\}.$$

Si $k \in \mathbb{N}$, $k \cdot \mathcal{A}$ es el conjunto de los elementos de $\mathcal{A}$ multiplicados por k. Por ejemplo, $2 \cdot \mathbb{N}$ es el conjunto de los enteros pares. Dados dos conjuntos de números enteros naturales $\mathcal{A}$ y $\mathcal{B}$, escribimos $\mathcal{A} \sim \mathcal{B}$ para significar que la

diferencia simétrica de $\mathcal{A}$ y $\mathcal{B}$ es finita, es decir que $\mathcal{A}$ y $\mathcal{B}$ coinciden desde algún entero en adelante. Además, si m es un entero positivo, definimos

$$\mathcal{A}(m) = \mathcal{A} \cap \{0, 1, 2, \dots, m\}.$$

Por último, definimos la densidad inferior de un conjunto $\mathcal{A}$ como

$$\underline{\mathrm{d}}(\mathcal{A}) = \liminf_{m \to +\infty} \frac{|\mathcal{A}(m)|}{m}.$$

Con estas notaciones, el problema de Waring puede ser reformulado de la siguiente manera: para todo $k \in \mathbb{N}$, existe un $g(k) \in \mathbb{N}$ tal que

$$g(k)\mathcal{P}_k = \mathbb{N}$$

donde $\mathcal{P}_k = \{0, 1, 2^k, 3^k, \dots\}$ es el conjunto de las potencias k-ésimas. En particular, el teorema de Lagrange puede ser reformulado como

$$4\mathcal{P}_2 = \mathbb{N}.$$

Por otro lado, se puede ver fácilmente que hay una infinidad de números enteros que no pueden ser escritos como la suma de tres cuadrados (por ejemplo, los enteros iguales a 7 modulo 8). Por eso se dice que los cuadrados son una base aditiva de orden cuatro.

A menudo, lo que es realmente importante y significativo, no es tanto representar todos los números sino todos ellos a partir de un cierto número n_0. En ese caso diremos que la base es una base asintótica. Por ejemplo, se sabe que 9 cubos son necesarios para representar todos los números naturales (el número 23 no se puede escribir con 8 cubos) y que 9 cubos son suficientes: los cubos forman una base aditiva de orden exactamente 9. Pero es posible demostrar que solamente hay un número finito de números naturales que necesitan 9 cubos. Y también se sabe que sólo un número finito necesitan 8. Dicho de otro modo, *todo entero positivo suficientemente grande puede ser escrito como la suma de siete cubos* (Linnik [22]). Es decir,

$$7\mathcal{P}_3 \sim \mathbb{N}.$$

Pero no se sabe si 7 puede ser disminuido. Por ejemplo, es plausible conjeturar que $4\mathcal{P}_3 \sim \mathbb{N}$, por el contrario es seguro que $3\mathcal{P}_3 \not\sim \mathbb{N}$ (se puede ver, por ejemplo, con un argumento de conteo o considerando los cubos modulo 9, ver [17]).

En adelante, vamos a decir que un conjunto de números naturales $\mathcal{A}$ es una *base* (se sobreentiende que aditiva y asintótica) si existe un número $h \geq 1$ con la propiedad de que todo entero positivo suficientemente grande se puede escribir como la suma de, exactamente, h elementos de $\mathcal{A}$, lo que denotaremos por $h\mathcal{A} \sim \mathbb{N}$. El h mínimo que lo cumpla será llamado el *orden* de $\mathcal{A}$ y denotado ord$\mathcal{A}$. Observamos que la definición no impone que la base aditiva $\mathcal{A}$

contenga 0. Por eso, es importante resaltar que en $h\mathcal{A}$ consideramos sumas de exactamente h elementos.

Como es fácil de imaginar por los ejemplos precedentes, la noción de base aditiva es central en muchos problemas aritméticos (el libro [9] es una buena introducción a este tema).

Pero también existen otros ejemplos de bases muy evidentes que servirán para ilustrar el problema central de este artículo. Por ejemplo, para cada número entero $h \geq 1$, el conjunto

$$\mathcal{M}_h = \{1, h, 2h, 3h, \dots\}$$

es una base de orden h.

En este artículo vamos a estudiar un problema de naturaleza combinatoria que podríamos llamar de *"pérdida de la propiedad de ser base"*. Los lectores que conozcan a Paul Erdős, el gran matemático húngaro, van a reconocer un problema del tipo de los que a él le interesaban: problemas que mezclan aritmética y combinatoria. De hecho fue el propio Erdős quien introdujo este problema.

2 El trabajo de Erdős y Graham

Paul Erdős y Ron Graham, en 1980 [4], se hicieron la siguiente pregunta. Si $\mathcal{A}$ es una base y retiramos uno de sus elementos, $a \in \mathcal{A}$, ¿sigue siendo una base el conjunto residual $\mathcal{A} \setminus \{a\}$? Y, si es así, ¿de qué orden?

La respuesta depende mucho del elemento a que se retire de la base $\mathcal{A}$. Consideremos los conjuntos $\mathcal{M}_h$ mencionados anteriormente. Si retiramos el elemento 1, el conjunto residual está compuesto por múltiplos de h, lo que por supuesto le impide ser una base. Por el contrario, no es difícil ver que si retiramos cualquier otro elemento $a \neq 1$, lo que queda todavía es una base, y además del mismo orden.

Dada una base $\mathcal{A}$, denotaremos por $\mathcal{A}^*$ al subconjunto de $\mathcal{A}$ compuesto por los elementos $a \in \mathcal{A}$ tales que $\mathcal{A} \setminus \{a\}$ es todavía una base, es decir

$$\mathcal{A}^* = \{a \in \mathcal{A},\ \mathcal{A} \setminus \{a\} \text{ es una base}\},$$

y a sus elementos los llamaremos elementos *regulares*. Al complementario $\mathcal{A} \setminus \mathcal{A}^*$ lo llamaremos el conjunto *excepcional* y a sus elementos, los elementos excepcionales.

En el ejemplo anterior (las bases $\mathcal{M}_h$), el único elemento excepcional era el 1. Este no es un caso aislado a la vista del siguiente teorema obtenido por Erdős y Graham [4].

Teorema 1. *Para cada base $\mathcal{A}$, el conjunto excepcional $\mathcal{A} \setminus \mathcal{A}^*$ es finito.*

La prueba de este teorema es un corolario de otro resultado muy interesante cuya demostración se puede ver en detalle en [4]. Se trata de la caracterización de los elementos regulares (o, lo que es lo mismo, de los elementos excepcionales).

Teorema 2. *Sea $\mathcal{A}$ una base. Un elemento $a \in \mathcal{A}$ es regular si y solamente si el máximo común divisor de los elementos del conjunto $\big((\mathcal{A}\setminus\{a\}) - (\mathcal{A}\setminus\{a\})\big)$ es igual a uno, es decir si y solamente si*

$$\text{mcd } \{b - b' \ : \ b, b' \in \mathcal{A}\setminus\{a\}\} = 1.$$

La condición mcd $\{b - b' \ : \ b, b' \in \mathcal{A}\setminus\{a\}\} = 1$ es claramente necesaria porque si fuese un $d > 1$, todos los elementos de $\mathcal{A}\setminus\{a\}$ caerían en la misma clase módulo d, y la suma de exactamente h de ellos siempre tendría el mismo valor módulo d.

La otra implicación descansa en el teorema de Bezout y es de naturaleza elemental aunque algo más elaborada.

Demostración del teorema 1. Escribimos $\mathcal{A} = \{a_1 < a_2 < a_3 < \cdots\}$. Como $\mathcal{A}$ es una base es claro que mcd $(\mathcal{A} - \mathcal{A}) = 1$, lo que implica la existencia de un número t tal que

$$\text{mcd } \{a_{k+1} - a_k \ : \ 1 \le k \le t\} = 1. \tag{1}$$

Entonces, si $a \in \mathcal{A}$ y $a \ge a_{t+2}$,

$$\text{mcd } \{b - b' \ : \ b, b' \in \mathcal{A}\setminus\{a\}\} = 1$$

así que, según el teorema 2, a no puede ser un elemento excepcional. Por consiguiente, el conjunto excepcional está incluido en $\{a_1, a_2, \ldots, a_{t+1}\}$, lo que demuestra en particular que es finito. □

Si el teorema 1 muestra que el conjunto excepcional es finito, no dice nada de lo que pasa con el orden cuando quitamos un elemento regular a la base $\mathcal{A}$. Erdős y Graham [4] demostraron que si a es un elemento regular, el orden de $\mathcal{A}\setminus\{a\}$ no puede ser arbitrariamente grande. Para ser más exactos, probaron que el orden de $\mathcal{A}\setminus\{a\}$ está limitado por una función que depende sólo del orden de $\mathcal{A}$. Más concretamente, definieron

$$X(h) = \max_{h\mathcal{A}\sim\mathbb{N}} \ \max_{a\in\mathcal{A}^*} \ \text{ord}(\mathcal{A}\setminus\{a\}),$$

y obtuvieron en las siguiente cotas para la función $X(h)$.

Teorema 3. *Se tiene que $X(2) = 4$ y para $h \ge 3$*

$$\frac{h^2}{4} + h - 1 \le X(h) \le \frac{5}{4}h^2 + O(h\log h).$$

También conjeturaron [5] que $X(h) \sim \alpha h^2$ (cuando $h \to +\infty$) para algún número real α, pero precisaban que no tenían ninguna idea sobre el posible valor de α.

3 Sobre la función X

En los años siguientes otros autores prosiguieron con el estudio de la función X. Grekos, en su tesis, fue el primero en mejorar el teorema 3 demostrando que

$$\max\left(\left[\frac{h^2+6h+1}{4}\right], \frac{h^2-h}{3}\right) \leq X(h) \leq h^2+h.$$

La primera parte de la cota inferior proviene de la utilización de un argumento de Stöhr [30, 31]. La segunda parte proviene de construcciones explícitas de "buenas" bases de orden h basadas en una teoría del recubrimiento del círculo por los múltiplos de un intervalo (esta teoría fue desarrollada más tarde por Deléglise [2]).

En lo que concierne a la cota superior, es consecuencia de la utilización hábil del siguiente teorema de Kneser [19], que enunciamos de manera explícita por su propio interés.

Teorema 4. *Sean $(\mathcal{A}_i)_{1\leq i\leq n}$ conjuntos de números enteros. Si*

$$\underline{\mathrm{d}}(\mathcal{A}_1+\cdots+\mathcal{A}_n) < \liminf_{m\to+\infty} \frac{|\mathcal{A}_1(m)|+\cdots+|\mathcal{A}_n(m)|}{m},$$

el conjunto $\mathcal{A}_1+\cdots+\mathcal{A}_n$ coincide, desde algún entero en adelante, con la unión de progresiones aritméticas de la misma diferencia. Más exactamente, existe un número entero g tal que $\mathcal{A}_1+\cdots+\mathcal{A}_n \sim (\mathcal{A}_1+\cdots+\mathcal{A}_n)+g\cdot\mathbb{N}$.

Años más tarde (el artículo fue publicado en 1993 pero fue escrito ocho años antes), Nash [23] consiguió mejorar la cota superior de Grekos al obtener

$$X(h) \leq \frac{h^2+3h}{2}. \tag{2}$$

Esta cota superior fue probada utilizando otro teorema de Kneser [19, 20, 21] que describe los pares de conjuntos de un grupo abeliano cuya suma es "pequeña". El siguiente teorema es una muestra del tipo de herramientas utilizadas.

Teorema 5. *Sea G cualquier grupo abeliano. Sean $\mathcal{A}$ y $\mathcal{B}$ dos subconjuntos finitos de G. Si*

$$|\mathcal{A}+\mathcal{B}| < |\mathcal{A}|+|\mathcal{B}|-1,$$

entonces $\mathcal{A}+\mathcal{B}$ es de la forma $(g_1+H)\cup\cdots\cup(g_k+H)$, para algún subgrupo $H\neq\{0\}$, y para algunos $g_1,\ldots,g_k\in G$.

La mejor cota superior conocida para $X(h)$ es muy reciente [27]. Hace uso del método isoperimétrico, que es un instrumento que proviene de la teoría de los grafos [10] y que fue introducido por Y. ould Hamidoune para resolver

diferentes problemas aditivos en los años 90. Desde entonces, han aparecido muchas otras aplicaciónes en teoría aditiva (ver por ejemplo [11, 12, 13, 14, 15, 16]).

La utilización del método isoperimétrico en lugar del teorema de Kneser para los grupos abelianos, permitió al autor demostar [27] que

$$X(h) \leq \frac{h(h+1)}{2} + \left\lceil \frac{h-1}{3} \right\rceil. \tag{3}$$

La prueba de este resultado es mucho más complicada que la prueba de Nash (necesita varias decenas de páginas). Utiliza otros instrumentos combinatorios como por ejemplo el muy hermoso teorema de las tres distancias (al principio conjeturado por Steinhaus, y después demostrado por Sós [29], Świerczkowski [33] y Surányi [32]): este teorema dice que, si consideramos una secuencia finita de elementos distintos del toro $\mathbb{T} = \mathbb{R}/\mathbb{Z}$, $(x_i)_{0\leq i\leq m-1}$, tal que la diferencia $x_{i+1} - x_i$ no dependa de i, entonces como mucho pueden ocurrir tres distancias consecutivas distintas en el sentido geométrico.

Es tiempo de regresar a las cotas inferiores. Si

$$\mathcal{C}_2 = \{0\} \cup (\{1, 4\} + 5 \cdot \mathbb{N}),$$

comprobamos immediatamente que $\mathcal{C}_2$ es una base de orden 2 mientras que el orden de $\mathcal{C}_2 \setminus \{0\}$ es igual a 4. De aquí se deduce que $X(2) \geq 4$. Comparando con la desigualdad (3) para $h = 2$, encontramos la primera afirmación del teorema 3 de Erdős y Graham,

$$X(2) = 4.$$

También, considerando

$$\mathcal{C}_3 = \{0\} \cup (\{1, 6\} + 8 \cdot \mathbb{N}),$$

encontramos $X(3) \geq 7$. Una vez más, con (3), obtenemos $X(3) = 7$.

Generalizando este tipo de construcciónes, el autor demostró en [27] que

$$X(h) \geq \left\lceil \frac{h(h+4)}{3} \right\rceil. \tag{4}$$

Esbozo de la prueba de (4). Consideramos solamente el caso donde 3 divide h. Consideramos $\mathcal{S} = \{1, h+3\}$ en $\mathbb{Z}/g\mathbb{Z}$ donde

$$g = \frac{h^2 + 4h + 3}{3}.$$

Trabajando un poquito, podemos ver que

$$\mathcal{S} \cup 2\mathcal{S} \cup \cdots \cup h\mathcal{S} = \mathbb{Z}/g\mathbb{Z},$$

pero el mínimo entero k tal que $k\mathcal{S} = \mathbb{Z}/g\mathbb{Z}$ es $g - 1$. Entonces, la base $\{0\} \cup (\{1, h+3\} + g \cdot \mathbb{N})$ es una base de orden h. Pero si retiramos el 0 a esta base, lo que queda, $\{1, h+3\} + g \cdot \mathbb{N}$, es una base de orden $g - 1$. □

A fecha de hoy, podemos describir nuestro conocimiento de X por el teorema siguiente.

Teorema 6. *Para cualquier número entero $h \geq 2$, se tienen las desigualdades*

$$\left\lceil \frac{h(h+4)}{3} \right\rceil \leq X(h) \leq \frac{h(h+1)}{2} + \left\lceil \frac{h-1}{3} \right\rceil .$$

4 La función S

Si consideramos las bases $\mathcal{A}$ de orden h que permiten alcanzar grandes valores de $X(h)$ (por ejemplo las bases utilizadas para la prueba de la fórmula (4)), observamos que hay un solo elemento tal que, si lo retiramos, el conjunto residual es de orden $X(h)$. Por ese motivo, Grekos [6, 8] introdujo la función S definida por la fórmula

$$S(h) = \max_{h\mathcal{A}\sim\mathbb{N}} \limsup_{a\in\mathcal{A}^*} \operatorname{ord}(\mathcal{A} \setminus \{a\}) \tag{5}$$

y conjeturó que $S(h) < X(h)$ para todo $h \geq 2$. En [8] demostró que $S(3) \leq 6 < 7 = X(3)$, que prueba la conjetura para $h = 3$.

En [26] el autor demostró la conjetura de Grekos para valores de h suficientemente grandes, probando que

$$S(h) \leq \frac{h^2}{4} + 4h + 2$$

y comparando esta cota con la cota inferior de $X(h)$ en (4).

Finalmente, Cassaigne y el autor [1], utilizando un método radicalmente diferente, consiguieron demostrar completamente la conjetura de Grekos. Es más, probaron [1] que la función S está acotada superiormente por una función lineal de h. Más exactamente,

$$S(h) \leq 2h.$$

Desgraciadamente, esta cota inferior quizás no es óptima. En el caso $h = 2$ es posible mejorarla y probar que $S(2) = 3$. Este es el único valor conocido (no trivial) de la función S.

¿Qué se sabe de las cotas inferiores de S? Está claro que $S(h) \geq h$ pero, ¿se puede mejorar esta cota? La contestación es que sí, como demuestra la siguiente construcción de Nathanson [24]. Si $h \geq 2$, el conjunto $\mathcal{A}_h$ dado por

$$\mathcal{A}_h = \{\sum_{f\in\mathcal{F}} 2^f \ : \ \mathcal{F} \subset \mathbb{N},\ 0 < |\mathcal{F}| < \infty,\ f \equiv f' \pmod h,\ \text{para } f, f' \in \mathcal{F}\}$$

es una base de orden h y para cualquier $a \in \mathcal{A}_h$, $\operatorname{ord}(\mathcal{A}_h \setminus \{a\}) = h + 1$. Esto demuestra que

$$S(h) \geq h + 1.$$

En resumen,

Teorema 7. *Tenemos que $S(2) = 3$ y para cualquier $h \geq 3$,*

$$h + 1 \leq S(h) \leq 2h.$$

En [1] también demostramos que si hubiera un valor de h, digamos h_0, para el cual $S(h_0) > h_0 + 1$ (por ejemplo, es posible que $S(3) = 5$, ¿por qué no?), entonces tendríamos que para cada $h \geq h_0$,

$$S(h) \geq h + (S(h_0) - h_0),$$

lo que mejoraría la cota inferior en el teorema 7. En otras palabras,

Teorema 8. *La función S es estrictamente creciente.*

Esbozo de la prueba. Para verlo, consideramos una base $\mathcal{A}$ de orden h para la cual

$$\limsup_{a \in \mathcal{A}^*} \operatorname{ord}(\mathcal{A} \setminus \{a\}) = S(h).$$

Es claro que $\mathcal{A}$ contiene al menos un elemento impar b. Definimos

$$\mathcal{B} = \{b\} \cup \{2a \ : \ a \in \mathcal{A}\}.$$

Para probar $S(h+1) \geq S(h)$, sólo hay que probar que si c es un elemento de $\mathcal{A}^*$ tal que $c > b$, entonces

$$\operatorname{ord}(\mathcal{B} \setminus \{2c\}) \geq \operatorname{ord}(\mathcal{A} \setminus \{c\}) + 1.$$

Eso lo dejamos para el lector ... □

5 Regreso al conjunto excepcional

En la primera parte hemos demostrado que el conjunto excepcional es siempre finito. En realidad, Grekos [7] demostró que el tamaño de un conjunto excepcional está acotado superiormente por una función que sólo depende del orden de $\mathcal{A}$.

Vamos a denotar

$$E(h) = \max_{\operatorname{ord}\mathcal{A}=h} \left| \mathcal{A} \setminus \mathcal{A}^* \right|.$$

Concretamente Grekos [7] demostró que

$$E(h) \leq h - 1.$$

Más recientemente, junto con Deschamps [3], ha obtenido la desigualdad

$$E(h) \leq 5,7\sqrt{\frac{h}{\log h}}. \tag{6}$$

Además han demostrado la existencia de una familia infinita de valores de h para los cuales $E(h) \gg \sqrt{h/\log h}$.

El último avance está contenido en [28], donde se consigue una estimación asintótica para $E(h)$.

Teorema 9. *Tenemos la estimación asintótica (cuando $h \to +\infty$):*

$$E(h) \sim 2\sqrt{\frac{h}{\log h}}.$$

6 Problemas abiertos

En esta sección queremos invitar a los lectores a pensar en alguna de las siguientes preguntas. Si algún lector es capaz de contestar alguna de ellas, el autor estaría muy contento de que le escribiera.

Problema 1. *¿Existe un número real α para el que $X(h) \sim \alpha h^2$ $(h \to +\infty)$?*

Problema 2. *Mejorar el teorema 6.*

Problema 3. *Calcular $X(4)$. ¿Es 10 o 11?*

Problema 4. *¿Hay una formula simple para $S(h)$? (Por ejemplo, $S(h) = h+1$, o $S(h) = 2h - 1$.)*

Problema 5. *Mejorar el teorema 7.*

Problema 6. *¿Existe un numero real β para el cual $S(h) \sim \beta h$ $(h \to +\infty)$?*

Problema 7. *Calcular $S(3)$. Sabemos sólo que $S(3) \in \{4, 5, 6\}$. Al menos, eliminar uno de esos tres valores.*

7 Agradecimientos

El autor agradece a Valérie Servant y a Javier Cilleruelo su ayuda en la elaboracion lingüística de este artículo.

Referencias

[1] J. Cassaigne y A. Plagne, Grekos' S function has a linear growth, *Proc. Amer. Math. Soc.* **132** (2004) 2833–2840.

[2] M. Deléglise, Recouvrement optimal du cercle par les multiples d'un intervalle, *Acta Arith.* **59** (1991) 21–35.

[3] B. Deschamps y G. Grekos, Estimation du nombre d'exceptions à ce qu'un ensemble de base privé d'un point reste un ensemble de base, *J. Reine Angew. Math.* **539** (2001) 45–53.

[4] P. Erdős y R. L. Graham, On bases with an exact order, *Acta Arith.* **37** (1980) 201–207.

[5] P. Erdős y R. L. Graham, *Old and new problems and results in combinatorial number theory*, Monogr. Enseign. Math. **28**, 1980.

[6] G. Grekos, *Minimal additive bases and related problems*, in "Journées arithmétiques, Exeter (Grande-Bretagne), 1980", edited by J.V. Armitage. London Math. Soc. Lecture Note Series **56**, Cambridge Univ. Press, 1982, 300 – 305.

[7] G. Grekos, *Sur l'ordre d'une base additive*, Séminaire de théorie des nombres de Bordeaux, Année 1987/88, exposé 31.

[8] G. Grekos, *Extremal problems abour additive bases*, Acta Math. Inform. Univ. Ostraviensis **6** (1998), 87 – 92.

[9] H. Halberstam y K. Roth, *Sequences*, Oxford University Press, 1966.

[10] Y. ould Hamidoune, Sur les atomes d'un graphe orienté, *C. R. Acad. Sciences* **284** (1977) 1253–1256.

[11] Y. ould Hamidoune, An isoperimetric method in Additive Theory, *J. Algebra* **179** (1996) 622–630.

[12] Y. ould Hamidoune, Subsets with small sums in Abelian groups I: the Vosper property, *Europ. J. of Combinatorics* **18** (1997) 541–556.

[13] Y. ould Hamidoune, Some results in additive number theory I: The critical pair theory, *Acta Arith.* **96** (2001), 97–119.

[14] Y. ould Hamidoune y A. Plagne, A generalization of Freiman's $3k-3$ theorem, *Acta Arith.* **103** (2002), 147–156.

[15] Y. ould Hamidoune y A. Plagne, A critical pair theorem applied to sum-free sets in abelian groups, *Comment. Math. Helv.* **79** (2004) 183–207.

[16] Y. ould Hamidoune y A. Plagne, *A multiple set version of the* $3k-3$ *theorem*, *Rev. Mat. Iberoam.* **21** (2005) 133–161.

[17] G. H. Hardy y E. M. Wright, *An introduction to the theory of numbers*, 5th edition, Clarendon Press, Oxford University Press, 1979.

[18] D. Hilbert, Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen (Waringsche Problem), *Math. Ann.* **67** (1909) 281–300.

[19] M. Kneser, Abschätzung der asymptotischen Dichte von Summenmengen, *Math. Z.* **58** (1953) 459–484.

[20] M. Kneser, Ein Satz über abelsche Gruppen mit Anwendungen auf die Geometrie des Zahlen, *Math. Z.* **61** (1955) 429–434.

[21] M. Kneser, Summenmengen in lokalkompakten abelschen Gruppen, *Math. Z.* **66** (1956) 88–110.

[22] Yu. V. Linnik, On the representation of large numbers as sums of seven cubes, *Mat. Sb.* **12** (1943) 218–224.

[23] J. C. M. Nash, Some applications of a theorem of M. Kneser, *J. Number Theory* **44** (1993) 1–8.

[24] M. B. Nathanson, Minimal bases and powers of 2, *Acta Arith.* **49** (1988) 525–532.

[25] M. B. Nathanson, *Additive number theory. Inverse problems and the geometry of sumsets*, Graduate Texts in Mathematics **165**, Springer Verlag, 1996.

[26] A. Plagne, Removing one element from an exact additive basis, *J. Number Theory* **87** (2001) 306–314.

[27] A. Plagne, À propos de la fonction X d'Erdős et Graham, *Ann. Inst. Fourier (Grenoble)* **54** (2004) 1717–1767.

[28] A. Plagne, *Sur le nombre d'éléments exceptionnels d'une base additive*, 2004, sometido.

[29] V. T. Sós, On the distribution mod 1 of the sequence $n\alpha$, *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.* **1** (1958) 127–134.

[30] A. Stöhr, Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe I, *J. Reine Angew. Math.* **194** (1955) 40–65.

[31] A. Stöhr, Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe II, *J. reine angew. Math.* **194** (1955) 111–140.

[32] J. Surányi, Über die Anordnung der Vielfachen einer reellen Zahl mod 1, *Ann. Univ. Sci. Budapest Eötvös Sect. Math.* **1** (1958) 107–111.

[33] S. Świerczkowski, On successive settings of an arc on the circumference of a circle, *Fund. Math.* **46** (1959) 187–189.

Alain Plagne
Centre de Mathématiques Laurent Schwartz
École polytechnique
91128 Palaiseau Cedex
Francia
Correo electrónico:plagne@math.polytechnique.fr