El diablo de los números

Sección a cargo de

Javier Cilleruelo Mateo

Problemas aditivos y grafos de Cayley

por

Oriol Serra

Algunos problemas de naturaleza combinatoria en teoría de números pueden ser abordados por medio de la teoría de grafos. Ésta proporciona un medio geométrico de representación, con su aportación de soporte intuitivo, y la flexibilidad de una estructura combinatoria simple en cuya desnudez algunos resultados básicos se evidencian con más claridad.

Quizás uno de los ejemplos paradigmáticos de este tipo de aplicaciones sea el teorema de Szemerédi que afirma que, para una longitud dada $t \geq 3$ y un número real dado $\delta > 0$, existe un entero $l(\delta, t)$ tal que cualquier conjunto A de enteros en el intervalo $[0, l]$, $l \geq l(\delta, t)$, con densidad $|A|/l \geq \delta$ contiene una progresión aritmética de longitud t. Este resultado fue conjeturado por Paul Erdös, y le costó la suma más elevada de cuantas ha dejado con recompensa en su singular hábito de valorar la dificultad de los problemas por medio de cantidades de dinero. Su demostración se basa en el llamado Lema de Regularidad de Szemerédi, que exhibe una propiedad universal de cualquier grafo relacionada con la densidad de las aristas en subgrafos bipartitos.

En este breve relato se describe la aplicación de una de las nociones centrales de la teoría de grafos, la conectividad, al análisis de ciertos problemas de la teoría aditiva de números. Para ilustrar esta aplicación se describe una demostración de uno de los teoremas clásicos en el área, el teorema de Cauchy-Davenport. Esta demostración ilustra los aspectos esenciales de la estrategia de aplicación de resultados de conectividad en grafos a la teoría aditiva. El desarrollo de esta estrategia ha dado lugar a un buen número de resultados que han aparecido en la última década. Por su proximidad conceptual, se describe también una aplicación de la noción de conectividad en grafos de Cayley al análisis de problemas aditivos desarrollada por Plünecke en la década de los 60, cuyas aplicaciones siguen apareciendo con regularidad en la literatura.

Problemas Aditivos

Algunos de los problemas clásicos en teoría de números pueden encuadrarse en el marco de los problemas aditivos. Así, el célebre problema de Waring (cualquier entero positivo se puede expresar como suma de $h(k)$ potencias k-ésimas de enteros) o la no menos célebre conjetura de Goldbach (cualquier número par es la suma de dos primos) son ejemplos de problemas aditivos.

Motivado por la solución de Hilbert al problema de Waring, Khintchine propuso en 1932 la célebre conjetura $\alpha + \beta$ que puede formularse del modo siguiente. Se define una medida de densidad como $\sigma(A) = \inf\{\frac{|A\cap[1,n]|}{n}, n \in \mathbb{N}\}$. Entonces, dados dos conjuntos A, B de enteros positivos, se tiene que

$$\sigma(A+B) \geq \min\{1, \sigma(A) + \sigma(B)\}.$$

La conjetura fue finalmente demostrada en 1942 por Mann. Davenport probó en 1935 un p-análogo del teorema $\alpha + \beta$: para p primo y conjuntos $A, B \subset \mathbb{Z}_p$, se satisface

$$|A+B| \geq \min\{p, |A| + |B| - 1\}.$$

Esta desigualdad había sido utilizada por Cauchy en 1813 para analizar el problema de Waring en $\mathbb{Z}_p$, y se conoce ahora como el teorema de Cauchy-Davenport.

Dicho teorema constituye uno de los ejemplos característicos de una clase de problemas aditivos que se formulan en general para grupos abelianos: dados dos conjuntos finitos A, B de un grupo abeliano, se trata de determinar cotas inferiores para $|A+B|$.

Para este caso general de grupos abelianos Kneser obtuvo en 1955 un resultado global que sigue constituyendo un teorema clave para esta clase de problemas. Un conjunto A en un grupo abeliano G se dice que es *periódico* de período K si existe un subgrupo $K < G$ tal que $A + K = A$. El teorema de Kneser establece que para cualquier par de conjuntos finitos $A, B \subset G$ existe un subgrupo finito K tal que $A + B$ es periódico de período K y

$$|A+B| \geq |A+K| + |B+K| - |K|.$$

En particular, puesto que para p primo el grupo cíclico $\mathbb{Z}_p$ no tiene subgrupos propios, se obtiene el Teorema de Cauchy-Davenport.

En diversas situaciones se pueden caracterizar los conjuntos para los que se alcanzan las cotas anteriores. Un ejemplo característico es el teorema obtenido por Vosper en 1956, según el cual la igualdad

$$|A+B| = |A| + |B| - 1$$

en el teorema de Cauchy-Davenport se satisface solamente si ambos conjuntos A y B son progresiones aritméticas con la misma diferencia (o algunos casos que se pueden considerar 'degenerados'). Este tipo de resultados, en los que se deduce la estructura de dos conjuntos cuyo conjunto suma tiene pocos elementos, se conocen como 'teoremas inversos' en teoría aditiva.

En el caso de los enteros (o más generalmente en cualquier grupo abeliano ordenado), se satisfacen los análogos de los teoremas de Cauchy-Davenport y de Vosper, y la demostración es sencilla. Uno de los teoremas inversos más importantes es el teorema de Freiman que establece que si A es un conjunto finito de enteros tal que

$$|A + A| \leq c|A|$$

para alguna constante c, entonces A está contenido en una estructura vecina a la de una progresión aritmética, lo que Freiman llama una progresión aritmética multidimensional. Ello consiste en un conjunto de enteros de la forma

$$\{x_1 d_1 + \cdots + x_k d_k, 1 \leq x_i \leq n_i\}$$

(o una traslación de dicho conjunto). La potencia del teorema de Freiman está en el hecho de que el número de progresiones involucradas, k, y sus longitudes, n_i, están acotados por funciones que dependen sólo de la constante c.

Grafos de Cayley

Una posible representación geométrica de los problemas aditivos mencionados anteriormente consiste en identificar los elementos del grupo G con vértices de un grafo orientado. Para un subconjunto dado B del grupo, el grafo contiene arcos desde cada vértice x hacia los vértices de la forma $x + b$ para cada $b \in B$. El grafo orientado resultante se denomina 'grafo de Cayley de G con respecto a B', y lo denotaremos aquí por G_B. El uso de tales grafos para el análisis de propiedades de grupos finitos fue popularizado por Cayley a finales del siglo XIX. En la figura 1 se pueden ver algunos ejemplos.

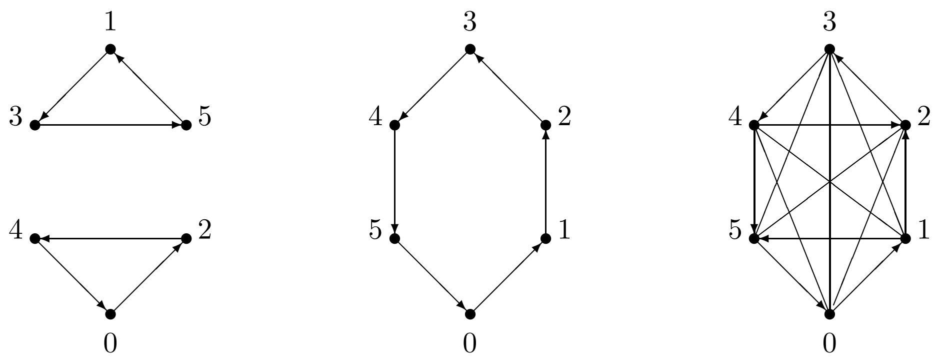

Figura 1: Grafos de Cayley $(\mathbb{Z}_6)_{\{2\}}$, $(\mathbb{Z}_6)_{\{1\}}$ y $(\mathbb{Z}_6)_{\{1,3,4\}}$.

En términos de los grafos de Cayley, el problema de la acotación inferior del cardinal de la suma de conjuntos está íntimamente relacionado con la noción de conectividad del grafo. Esta noción se describe usualmente como el mínimo número de vértices cuya supresión deja dos vértices x e y en el grafo de modo que no hay ningún camino (orientado) desde el primero hacia el segundo. Así, en los ejemplos de la figura 1, la conectividad de $(\mathbb{Z}_6)_{\{2\}}$ es cero, la de $(\mathbb{Z}_6)_{\{1\}}$ es uno y la de $(\mathbb{Z}_6)_{\{1,3,4\}}$ es 2 (para este último caso, la supresión de los vértices $1, 4$ deja el vértice 0 desconectado de 5, por ejemplo).

Para los problemas que nos ocupan es preferible describir la conectividad de un modo ligeramente distinto. En general, un grafo orientado es un par $\Gamma = (V, A)$ formado por un conjunto V (de vértices) y un subconjunto A del producto cartesiano $V \times V$ (cada par $(x, y) \in A$ es un arco de x a y). Para cada conjunto X de vértices, la frontera ∂X se define como el conjunto de vértices del complemento $V \setminus X$ de X que son terminales de arcos con origen en algun vértice de X,

$$\partial X = \{y \in V \setminus X : (x, y) \in A \cap (X \times V)\}.$$

Cuando X se reduce a un solo elemento, entonces $|\partial\{x\}|$ es el grado de x (esta definición difiere de la habitual en teoría de grafos, donde no se consideran los arcos que son lazos, arcos de la forma (x, x)). Cuando todos los vértices tienen el mismo grado r, se dice que el grafo es regular de grado r. El grafo de Cayley G_B es pues, regular de grado $|B| - 1$ si $0 \in B$.

Si $X \cup \partial X$ es un subconjunto propio de V, la supresión de los vértices de ∂X ciertamente corta los caminos de X hacia vértices en $V \setminus (X \cup \partial X)$. Así pues, la conectividad de Γ se define como

$$\kappa(\Gamma) = \min\{|\partial X| : |X \cup \partial X| < |V|\}.$$

Esta definición se extiende también al caso de grafos infinitos localmente finitos, es decir, aquellos en los que el grado de sus vértices está acotado. Para el caso de los grafos completos (cada vértice está unido por arcos con todos los demás, incluido posiblemente él mismo), la condición $|X \cup \partial X| < |V|$ no se satisface para ningún conjunto X de vértices. Se define entonces la conectividad como el grado del grafo, $|V| - 1$.

El valor de la conectividad de un grafo no se altera si se añaden lazos a todos los vértices, arcos de la forma (x, x). Para el caso de un grafo de Cayley G_B, la adición de lazos se corresponde a la del elemento 0 en B. Puesto que el problema de acotación de $|A + B|$ en un grupo abeliano es invariante por traslaciones, se suele suponer que $0 \in A \cap B$.

Entonces, en el grafo de Cayley G_B,

$$|A + B| = |A| + |\partial A|.$$

Así pues, para un conjunto dado B, el menor valor posible de $|X + B| - |X|$ para subconjuntos $X \subset G$ es la conectividad del grafo $\kappa(G_B)$. La relevancia de la conectividad en la teoría de grafos explica, en parte, la de los problemas de acotación de $|A + B|$ en teoría aditiva. La conectividad de un grafo está acotada superiormente por su grado mínimo, $\min\{|\partial x| : x \in V\}$. Puesto que el grafo de Cayley G_B (con $0 \in B$) es regular de grado $|B| - 1$, se tiene siempre

$$\min\{|A + B| - |A| : A \subset G\} = \kappa(G_B) \leq |B| - 1.$$

Si el grafo tiene connectividad máxima, $\kappa(G_B) = |B| - 1$, entonces, para cualquier conjunto A se satisface

$$|A + B| \geq \min\{|G|, |A| + \kappa(G_B)\} \geq \min\{|G|, |A| + |B| - 1\}.$$

Este es precisamente el enunciado del teorema de Cauchy-Davenport, que se corresponde con el que afirma que el grafo de Cayley de un grupo cíclico de orden primo tiene conectividad máxima. En particular, este punto de vista explica la ubicuidad de la desigualdad $|A + B| \geq |A| + |B| - 1$ en la teoría aditiva en general.

Los grafos de Cayley son ejemplos importantes de grafos vértice transitivos, aquellos para los que existe un grupo de automorfismos (biyecciones que preservan el conjunto de arcos) que actúa transitivamente en el conjunto de vértices: para cada par de vértices existe un automorfismo del grafo que envía uno de ellos al segundo. Esta simetría se describe gráficamente diciendo que el grafo se ve igual desde cada uno de sus vértices. Para el caso de los grafos de Cayley, el conjunto de traslaciones constituye un grupo de automorfismos transitivo: para cada elemento $a \in G$, la traslación $\phi_a(x) = x + a$ es una biyección que preserva el conjunto de arcos.

Para el análisis de la conectividad de grafos, Mader introdujo en la década de los 60 la noción de fragmentos y átomos. Un fragmento de un grafo Γ es un conjunto no vacío de vértices cuya frontera tiene cardinal mínimo, la conectividad del grafo $\kappa(\Gamma)$. Un átomo es un fragmento de cardinal mínimo. La denominación proviene del hecho de que dos átomos distintos de un grafo deben ser disjuntos. Este hecho se deduce de la submodularidad del operador frontera,

$$|\partial(X \cup Y)| + |\partial(X \cap Y)| \leq |\partial X| + |\partial Y|, \; X, Y \subset V.$$

Si X e Y son átomos no disjuntos, los términos de la derecha de la desigualdad no deben ser mayores que los de la izquierda, y son estrictamente menores que $|\partial(X \cap Y)|$, lo que contradice la submodularidad (hay que considerar el caso adicional en el que $(X \cup Y) \cup \partial(X \cup Y) = V$ para completar el razonamiento). Mader consideraba sólo grafos no orientados. Estos son espacios métricos en los que las nociones topológicas (componentes conexas, fragmentos) tienen un sentido más intuitivo que en el caso orientado. Hamidoune [4] generalizó los resultados de Mader al caso orientado, que exige la consideración de átomos positivos y átomos negativos. Para el caso de los grafos de Cayley abelianos esta distinción no es necesaria, por lo que sigue siendo válida la afirmación que dos átomos distintos son disjuntos. Puesto que se trata de grafos vértice transitivos, siendo el conjunto de traslaciones un grupo transitivo de automorfismos, si A es un átomo con más de un elemento y $\{0, a\} \in A$, entonces

$A+a$ es también un átomo que tiene intersección no vacía con A, por lo que $A+a=A$ para todo $a\in A$. En otras palabras, los átomos que contienen 0 en un grafo de Cayley abeliano son subgrupos del grupo base. En particular, si G es un grupo cíclico de orden primo, entonces los átomos deben tener cardinal 1. Esta afirmación es equivalente a que la conectividad de $(\mathbb{Z}_p)_B$ es el grado, $|B|-1$, de modo que se obtiene así el teorema de Cauchy-Davenport.

El mismo punto de vista puede ser utilizado para la obtención de teoremas inversos, es decir, la caracterización de los llamados pares críticos A, B para los cuales se alcanzan las cotas inferiores del cardinal de la suma de dos conjuntos. Siguiendo con el ejemplo anterior, veamos como puede obtenerse el teorema de Vosper que caracteriza los pares críticos del teorema de Cauchy-Davenport. Para ello se introducen la nociones de r-fragmentos y r-átomos. Un grafo $\Gamma=(V,A)$ es r-separable si existe un subconjunto de vértices $X\subset V$ de cardinal al menos r tal que $|V|-|X\cup\partial X|\geq r$. Denotemos por $\mathcal{B}_r$ a la familia de tales subconjuntos. La conectividad r-isoperimétrica del grafo es entonces

$$\kappa_r(\Gamma)=\min\{|\partial X| : X\in\mathcal{B}_r\}.$$

Un r-fragmento es un subconjunto de $\mathcal{B}_r$ cuya frontera tiene cardinal mínimo, $\kappa_r(\Gamma)$. Un r-átomo es un r-fragmento de cardinal mínimo. Con un argumento análogo al descrito anteriormente para probar que los átomos (o 1-átomos) de $(\mathbb{Z}_p)_B$ tienen cardinal 1, se prueba en [14] que, si A, B son subconjuntos de $\mathbb{Z}_p$ tales que $|A+B|=|A|+|B|-1<p-1$, entonces los 2-átomos de $(\mathbb{Z}_p)_B$ tienen cardinal 2. Ello implica que, si $D=\{0,d\}$ es uno de tales 2-átomos, entonces

$$|D+B|-|D|\leq|A+B|-|A|=|B|-1,$$

por lo que (X,B) es también un par crítico. En este caso sencillo resulta fácil deducir que B debe ser una progresión aritmética de diferencia d. Por simetría, el conjunto A es también una progresión aritmética, digamos de diferencia d'. No resulta difícil entonces deducir que las dos diferencias deben coincidir, con lo que se obtiene el teorema de Vosper.

Las demostraciones precedentes ilustran el punto de vista del uso de propiedades combinatorias de grafos para el análisis de problemas aditivos. La aportación de esta línea de trabajo consiste en la simplicidad y generalidad de la estructura combinatoria de los grafos y en el uso de un referente geométrico que en muchos casos proporciona base intuitiva al análisis de estos problemas. En la década de los 90, Hamidoune, Lladó y este autor dedicaron una serie de trabajos a la exploración sistemática de este punto de vista para la obtención de resultados en el área de la teoría aditiva. Algunos de los más significativos entre ellos son la extensión del teorema de Brailovsky-Freiman [1] sobre la caracterización de la estructura de conjuntos en grupos libres de torsión que tienen producto pequeño [6], la demostración de la conjetura de Diderrich sobre el tamaño crítico de conjuntos tales que las sumas de sus subconjuntos cubre todo el grupo [3], la extensión a grupos abelianos del problema de Erdös -Heilbronn sobre el número de sumas distintas de elementos distintos de un conjunto [7], o la determinación asintótica del orden de un bisector en grafos de Cayley abelianos [8].

Grafos de Plünecke

Una orientación similar que encuentra en la conectividad de grafos una herramienta útil para el análisis de problemas aditivos había sido desarrollada en la década de los 60 por Plünecke, quizás con resultados más espectaculares. El problema que preocupaba a Plünecke era el de las componentes esenciales.

La densidad de Schnirelman de un conjunto de enteros no negativos A se define como

$$\sigma(A) = \inf \left\{ \frac{|A| \cap [1,n]}{n}, n \in \mathbb{N} \right\}.$$

Se satisface $0 \leq \sigma(A) \leq 1$. Un conjunto de enteros B es una componente esencial si $\sigma(A+B) > \sigma(A)$ para cualquier conjunto A con $0 < \sigma(A) < 1$. De la desigualdad fundamental de Schnirelman

$$\sigma(A+B) \geq \sigma(A) + (1-\sigma(A))\sigma(B),$$

se deduce que cualquier conjunto B con densidad positiva conteniendo el 0 es una componente esencial. Sin embargo, hay conjuntos de densidad cero, como el conjunto de cuadrados, que constituyen también componentes esenciales.

El teorema de Lagrange afirma que todo entero positivo es la suma de cuatro cuadrados. Se dice entonces que el conjunto de cuadrados es una base aditiva de orden 4. Mejorando un resultado anterior de Erdös, Plünecke [12] probó que para cualquier base aditiva de orden $h \geq 2$ (todo entero positivo se expresa como suma de a lo sumo h elementos en B) y para cualquier conjunto A con $0 < \sigma(A) < 1$, se satisface

$$\sigma(A+B) \geq \sigma(A)^{1-1/h}.$$

Para obtener este resultado Plünecke se basó en grafos que poseen una propiedad característica de los grafos de Cayley abelianos. Dado un grafo de Cayley abeliano G_B y un subconjunto no vacío $A \subset G$, consideremos el conjunto $V_i = A + iB$ de vértices que pueden ser alcanzados desde algún vértice de A por un camino de longitud i en G_B. Denotemos por $\partial_i(X) = X + iB \subset V_i$ para cualquier subconjunto no vacío $X \subset A$. El coeficiente i-ésimo de amplificación de G_B con respecto a A se define como

$$D_i = \min \left\{ \frac{|\partial_i(X)|}{|X|}, \emptyset \neq X \subset A \right\},$$

de modo que para cualquier $X \subset A$ se tiene $|\partial_i(X)| \geq D_i|X|$. Las desigualdades de Plünecke establecen el sorprendente resultado que, para $h \geq 2$,

$$D_1 \geq D_2^{1/2} \geq \cdots \geq D_h^{1/h}. \tag{1}$$

Plünecke estableció la validez de estas desigualdades para una clase más amplia de grafos, llamados ahora grafos de Plünecke, que verifican una propiedad que abstrae la de conmutatividad en los grafos de Cayley abelianos. Ruzsa [13] dio en 1989 una demostración de las desigualdades de Plünecke basada en uno de los teoremas clásicos de la teoría de grafos, el teorema de Menger (1929), que establece que la conectividad $\kappa(\Gamma)$ de un grafo coincide con el mínimo número de caminos disjuntos entre pares de vértices no adyacentes.

Como una aplicación inmediata de las desigualdades de Plünecke se obtienen acotaciones del tamaño de las esferas en un grafo de Cayley abeliano G_B con $0 \in B$ finito. Tomando $A = \{0\}$, se tiene

$$|hB| = D_h \leq D_i^{h/i} = |iB|^{h/i},\ i = 1, \ldots, h.$$

Para la aplicación de estas desigualdades al resultado sobre componentes esenciales, Plünecke utilizó la denominada función de impacto, que para cada número real $\theta \in [0, 1]$ y cada conjunto de enteros no negativos B se define como

$$\phi(\theta, B) = \inf\{\sigma(A + B), A \subset \mathbb{N}, \sigma(A) > \theta\}.$$

Las desigualdades (1) se utilizan entonces para probar que, para cada conjunto de enteros no negativos B con $0 \in B$,

$$\phi(\theta, iB) \geq \theta^{1-i/h}\sigma(hB + 1)^{i/h},\ i = 1, \ldots, h.$$

En particular, si B es una base aditiva de orden $h \geq 2$, entonces $\sigma(hB + 1) = 1$, de modo que tomando $\theta = \sigma(A) \in (0, 1)$ se obtiene de la desigualdad anterior

$$\sigma(A + B) \geq \phi(\theta, B) \geq \theta^{1-1/h} = \sigma(A)^{1-1/h}.$$

Epílogo

Estas páginas han pretendido poner de manifiesto la relevancia de aspectos combinatorios de problemas en teoría de números cuya expresión en términos de grafos puede aportar técnicas y resultados útiles, además de un nuevo elemento de comprensión. Este punto de vista forma parte de la herencia matemática de Paul Erdös, el gran matemático húngaro cuyas indagaciones en la simplicidad esencial del mundo de los números ha dejado una huella profunda en la actividad de no pocos matemáticos de nuestro tiempo.

Paul Erdös

Para lectores interesados en la teoría aditiva, algunas de las referencias más interesantes sobre este área de la teoría de números se encuentran el libro de Mann [9], los volúmenes de Nathanson [10,11] y el volumen editado por Deshouillers, Landreau y Yudin [2] que recoge algunos de los resultados recientes más interesantes del área.

Resulta interesante mencionar aquí que el tipo de interacción entre la teoría de grafos y la teoría de números que se describe en estas páginas ha supuesto también un avance considerable en el análisis de funcionamiento de cierta clase de redes de interconexión de uso muy común, las denominadas redes de lazos, cuyas propiedades han sido extensamente estudiadas en el ámbito de la ingeniería informática. El lector interesado puede encontrar una excelente monografía de Hamidoune [5] centrada en este aspecto de la cuestión.

Bibliografía

[1] Brailovsky, L.V., Freiman, G. A., On a product of finite subsets in a torsion free group, *J. Algebra* **130** (1990), 462–476.

[2] Deshouillers, J., Landreau, B., Yudin, A. A. Structure Theory of Set Addition, *Asterisque* **258**, Societé mathématique de France (1999).

[3] Gao, W., Hamidoune, Y. O., Lladó, A., Serra, O. On spanning subset sum. Sometido a *Combinatorica.*

[4] Hamidoune, Y. O., Sur les atomes d'un graphe orienté, *C. R. Acad. Sci. Paris Sér. A-B* **284** (1977), no. 20, A1253–A1256.

[5] Hamidoune, Y. O., Additive group theory applied to network topology, *Combinatorial network theory*, 1–39, Appl. Optim., 1, Kluwer Acad. Publ., Dordrecht, (1996).

[6] Hamidoune, Y. O., Lladó, A., Serra, O. On subsets with small product in torsion-free groups. *Combinatorica* **18** (1998), 529–540.

[7] Hamidoune, Y. O., Lladó, A., Serra, O. On restricted sums. *Combinatorics, Probability and Computing,* **9** (2000), 513–518.

[8] Hamidoune, Y. O., Serra, O. On small cuts separating an abelian Cayley graph into equal parts. *Mathematical Systems Theory,* **29** (1996), 407–409.

[9] Mann, H. B., Addition Theorems. Interscience Tracts in Pure and Applied Mathematics, **18**, John Wiley & Sons 1996.

[10] Nathanson, M. B., Additive Number Theory: The Classical Bases. GTM **164**, Springer, 1996.

[11] Nathanson, M. B., Additive Number Theory: Inverse Theorems and the Geometry of Sumsets. GTM **165**, Springer, 1996.

[12] Plűnecke, H., Eigenschaften und Abschätzungen von Wirkungsfunktionen, *Gesellschaft fűr Mathematik und Datenverarbeitung* **22**, Bonn 1969 iii+173 pp.

[13] Ruzsa, I. Z., An application of graph theory to additive number theory. *Scientia, Ser. A,* **3** (1987), 97–109.

[14] SERRA, O., ZÉMOR, G., On a generalization of a theorem by Vosper. *Integers: Electronic Journal of Number Theory,* **0** (2000), # A10.

Oriol Serra
Dept Matematica Aplicada i Telematica
Campus Nord, Modul C3
Universitat Politecnica de Catalunya
C/ Jordi Girona, 08034 Barcelona
correo electrónico: `oriol@mat.upc.es`