Butlletí de la Societat Catalana de Matemàtiques
Vol. 26, núm. 1, 2011. Pàg. 69–95. DOI: 10.2436/20.2002.01.35

Progressions aritmètiques de tots colors

Ignasi Mundet i Riera

Resum: Aquest article explica, a un nivell divulgatiu, diversos resultats sobre progressions aritmètiques formades per nombres naturals. En la primera part parlem sobre el teorema de Van der Waerden per a progressions aritmètiques, i en donem una demostració. En la segona part, que només inclou demostracions de fets elementals, parlem de la solució de Szemerédi de la conjectura de Erdős i Turán, i del teorema de Green i Tao sobre progressions aritmètiques formades per nombres primers.

Paraules clau: teorema de Van der Waerden, teorema de Szemerédi, teorema de Green i Tao.

Classificació MSC2010: 11B75.

1 Presentació

Aquest article està basat en la conferència impartida per l'autor en l'acte inaugural del curs 2010-2011 de la Facultat de Matemàtiques de la Universitat de Barcelona, el 22 de setembre de 2010. Una primera versió d'aquest text va aparèixer a les *Publicacions de la Universitat de Barcelona*. L'autor ha aprofitat l'oportunitat de presentar-ne una nova versió al *Butlletí* de la Societat Catalana de Matemàtiques per polir i millorar alguns aspectes. La demostració del teorema de Van der Waerden ha estat reescrita de bell nou (tot i ser essencialment la mateixa que s'explica a la versió apareguda a les *Publicacions*). S'han inclòs també en aquesta versió fotografies d'alguns dels matemàtics que es mencionen en el text. Finalment, els diagrames que en la versió de les *Publicacions* apareixien en colors s'han adaptat per aparèixer, en la present edició, combinant diferents tonalitats de gris.

2 Progressions aritmètiques

Per a nosaltres els nombres naturals ($\mathbb{N}$) seran els nombres enters més grans que 0 (és a dir, no considerarem el nombre 0 com a nombre natural). Totes les progressions aritmètiques que considerarem estaran formades per nombres naturals i seran de longitud finita. Per tant, donat un nombre natural n, anomenarem *progressió aritmètica de longitud n* qualsevol conjunt de n nombres naturals amb la propietat que, si escrivim els seus elements en ordre creixent:

$$x_1 < x_2 < \cdots < x_n\,,$$

aleshores se satisfà que

$$x_2 - x_1 = x_3 - x_2 = \cdots = x_n - x_{n-1}\,.$$

En altres paraules, les distàncies entre elements consecutius del conjunt són totes iguals. També direm que els nombres $\{x_1, \ldots, x_n\}$ estan en progressió aritmètica.

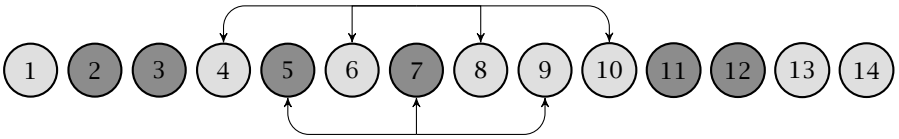
Per exemple, al següent diagrama els nombres en gris formen una progressió aritmètica de longitud 4:

Com que en tot l'article parlarem únicament de progressions aritmètiques, de vegades, per fer la lectura més lleugera, ens hi referirem anomenant-les senzillament *progressions*.

3 Progressions monocromàtiques de longitud 3

Sigui S un conjunt qualsevol de nombres naturals. Triem un nombre natural k i agafem un conjunt C de k colors diferents. Suposem que hem pintat els elements de S usant els colors de C (en altres paraules, suposem que hem triat una aplicació $f\colon S \to C$). Llavors direm que hem especificat una *k-coloració* de S. Cal tenir present que el nombre k es refereix a la quantitat de colors que podem fer servir per colorar, però que en general no demanem que una k-coloració hagi de fer aparèixer, forçosament, cada un dels k colors disponibles; en altres paraules, l'aplicació $f\colon S \to C$ no ha de ser necessàriament exhaustiva. Direm que una progressió aritmètica dins de S és *monocromàtica* si tots els seus elements estan pintats d'un mateix color.

EXEMPLE. En el diagrama següent especifiquem una coloració de $S = \{1, \ldots, 14\}$ usant com a colors dues tonalitats de gris, una de clara i una de fosca. És a dir, prenem $C = \{\text{clar}, \text{fosc}\}$. Els elements indicats per les fletxes de dalt formen una progressió aritmètica monocromàtica de longitud 4, però els indicats per les fletxes de baix formen una progressió aritmètica que no és monocromàtica:

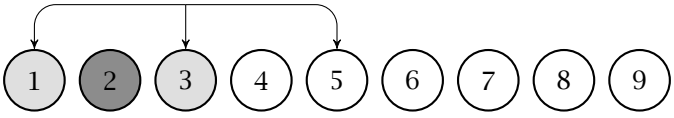


Comencem plantejant-nos el problema següent:

PROBLEMA. *Existeix alguna* 2*-coloració de* $S = \{1, \ldots, 9\}$ *per a la qual no hi hagi cap progressió aritmètica monocromàtica de longitud* 3 *dins de* S*?*

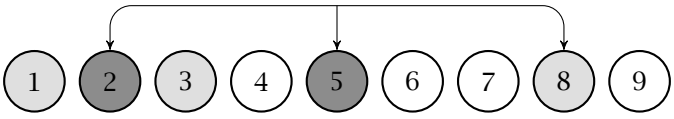
Mirarem de donar una resposta per tempteig. Anirem colorant els elements de S començant pels més petits, anant amb compte, cada vegada que triem un color, de no generar progressions monocromàtiques. Com abans, farem servir com a colors dues tonalitats de gris, $C = \{\text{clar}, \text{fosc}\}$. A l'hora de triar els colors dels tres primers elements l'únic que cal és no pintar-los tots tres del mateix color. Per exemple, podem fer-ho així:

Ara, si volem evitar progressions monocromàtiques, la casella 5 no es pot pintar clara (si la pintéssim clara, els nombres 1, 3 i 5 formarien una progressió aritmètica monocromàtica):



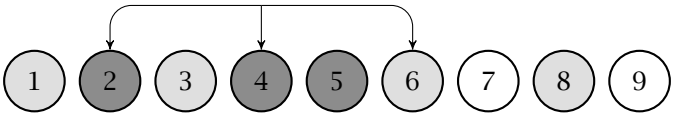
Per tant, pintem la casella 5 de gris fosc:

Per la mateixa raó d'abans, la casella 8 no es pot pintar fosca, així que la pintarem clara:

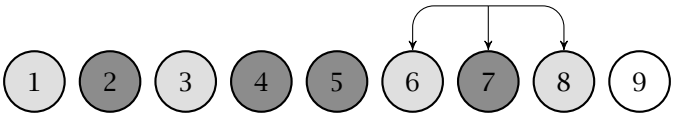


Podem pintar la casella 4 de qualsevol color sense por de crear cap progressió monocromàtica. La pintem, per exemple, de gris fosc:

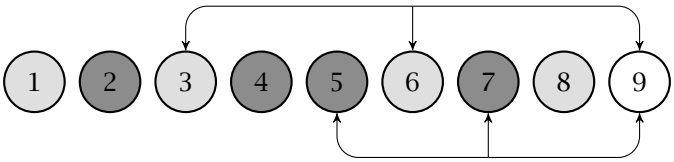
Ara la casella 6 ja no és lliure; cal pintar-la clara:



I hem de pintar la casella 7 de gris fosc:



Arribats a aquest punt, és impossible pintar la casella 9 sense crear una progressió de longitud 3 monocromàtica:



No hem estat capaços de trobar una coloració que evités progressions monocromàtiques. Ara bé, com que a l'hora de pintar algunes de les caselles hem tingut llibertat per triar els colors (concretament, a les caselles $1, 2, 3, 4$), podríem pensar que, potser, triant aquests colors de manera més hàbil, es podria trobar la coloració que buscàvem. Però no és així: és impossible donar una coloració amb dos colors del conjunt $\{1, \ldots, 9\}$ sense progressions aritmètiques monocromàtiques de longitud 3! Això es pot demostrar fàcilment considerant les diverses possibles coloracions. Si el lector s'hi entreté veurà que en qualsevol cas, un cop triats els colors dels quatre primers nombres, els colors dels nombres següents van quedant determinats pel requeriment que no hi hagi progressions monocromàtiques, fins a arribar a una situació com l'anterior, on un dels nombres no pot rebre cap dels dos colors sense donar lloc a una progressió monocromàtica.

En lloc de mostrar detalladament el que acabem de dir, donarem un argument que demostra un resultat una mica més feble, però que té la virtut de poder-se generalitzar a situacions més complexes, com veurem més endavant.

TEOREMA 1. *És impossible donar cap* 2*-coloració del conjunt* $\{1, 2, \ldots, 17\}$ *sense progressions monocromàtiques de longitud 3.*

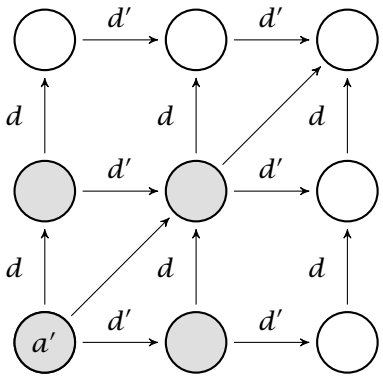
PROVA. Sigui $S = \{1, 2, \ldots, 17\}$, i suposem que existeix una 2-coloració de S,

$$f\colon S \to \{\text{clar}, \text{fosc}\},$$

sense progressions monocromàtiques de longitud 3. Veurem com això ens durà a una contradicció. Donat un element i de $\{1, \ldots, 15\}$ considerem el vector de colors següent: $F(i) = \big(f(i), f(i+1), f(i+2)\big)$. Com que usem dos colors, hi ha $2^3 = 8$ maneres de colorar tres elements consecutius; d'aquestes, hem de substreure les dues coloracions monocromàtiques (clar, clar, clar) i (fosc, fosc, fosc), que immediatament donarien una progressió monocromàtica de longitud 3. Per tant, els vectors $F(1), F(2), \ldots, F(15)$ van prenent valors dins un conjunt de sis elements. Això implica que almenys dos dels vectors $F(1), \ldots, F(7)$ coincideixen: denotem-los per $F(a) = F(a+d)$, on a, d són nombres naturals per als quals $a, a+d \in \{1, \ldots, 7\}$, de manera que $a + 2d \leq 13$. Fixem-nos ara en la cadena $F(a)$. Com que té tres elements que es mouen dins un conjunt de dos colors, un d'aquests colors ha d'estar repetit: suposem que són

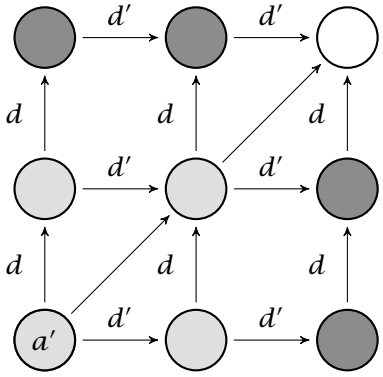
$$f(a') = f(a'+d') = \text{clar},$$

on a', d' són nombres naturals que satisfan $a', a'+d' \in \{a, a+1, a+2\}$, de manera que $a' + 2d' \leq a + 4$. Com que $F(a) = F(a+d)$, tenim també que $f(a') = f(a'+d) = f(a'+d+d')$. Considerem el diagrama següent:



Tot i estar disposats en una matriu 3×3, els discos d'aquest diagrama representen elements del conjunt S. El disc de la cantonada inferior esquerra representa a', i els nombres representats pels altres discos estan determinats pel requeriment que en passar d'un disc a un altre a través d'una fletxa vertical o horitzontal, respectant-ne l'orientació, sumem la quantitat indicada per la fletxa (fent aquestes operacions no sortim mai del conjunt S, ja que $a' + 2d + 2d' \leq a + 4 + 2d \leq 13 + 4 = 17$).

Llavors, les tres files del diagrama, les tres columnes i la diagonal indicada representen progressions aritmètiques de tres elements diferents (la diagonal que no hem dibuixat no té per què correspondre's amb tres elements diferents, a menys que $d \neq d'$).



Ara, per evitar que hi hagi columnes o files monocromàtiques cal que els quatre discos que indiquem a la figura de l'esquerra estiguin pintats de gris fosc. Però llavors és impossible associar un color a la cantonada superior dreta sense crear una progressió monocromàtica: si la pintem clara la diagonal indicada representa una progressió clara de longitud 3, i si la pintem fosca tant la columna dreta com la fila superior representen progressions fosques de longitud 3.

Per tant, la coloració f que havíem pres forçosament ha de tenir alguna progressió monocromàtica de longitud 3, en contradicció amb el que havíem suposat. □

4 El teorema de Van der Waerden

El problema que hem considerat a la secció anterior es pot generalitzar en dues direccions. D'una banda, podem augmentar el nombre de colors: considerar coloracions amb tres, quatre o més colors en lloc de dos com fins ara. D'altra banda, podem considerar coloracions sense progressions aritmètiques monocromàtiques de quatre, de cinc o més elements. Augmentant qualsevol de les dues quantitats (nombre de colors, longitud de les progressions monocromàtiques que cal evitar) la quantitat de nombres enters consecutius que podrem colorar creixerà. Per exemple, si fem servir tres colors és possible colorar el conjunt $\{1,\dots,9\}$ de tal manera que no hi hagi progressions monocromàtiques de longitud tres. Ens podem plantejar, llavors: si n i k són nombres naturals prou grans, podria ser que per a qualsevol N existís una k-coloració de $\{1,\dots,N\}$ sense progessions monocromàtiques de longitud n? La resposta, negativa, ens la dóna el teorema de Van der Waerden.

TEOREMA 2 (VAN DER WAERDEN). *Per a qualssevol nombres naturals n,k existeix un nombre $W(n,k)$ amb aquesta propietat: per a tot nombre natural $N \geq W(n,k)$, qualsevol k-coloració de $\{1,\dots,N\}$ conté almenys una progressió aritmètica monocromàtica de longitud n.*

4.1 Demostració del teorema de Van der Waerden

Farem servir inducció, de la manera que precisem tot seguit. Si n,k són nombres naturals, considerem l'afirmació següent:

$$T(n,k) = \left(\begin{array}{c} \text{«existeix } W(n,k) \text{ amb la propietat que, si } N \geq W(n,k), \\ \text{qualsevol } k\text{-coloració de } \{1,\dots,N\} \text{ conté una progressió} \\ \text{aritmètica monocromàtica de longitud } n\text{»} \end{array} \right)$$

Per exemple, a la secció anterior hem demostrar que $T(3,2)$ és certa, prenent $W(3,2) = 17$ (tot i que, com hem dit, és suficient prendre $W(3,2) = 9$). És clar que el teorema de Van der Waerden equival a afirmar que $T(n,k)$ és certa per a qualssevol nombres naturals n, k.

Comencem observant que, per a qualsevol nombre de colors k, l'afirmació $T(1,k)$ és certa i que de fet podem prendre $W(1,k) = 1$. En efecte, qualsevol nombre és, en tant que subconjunt de $\mathbb{N}$ d'un element, una progressió aritmètica de longitud 1, que en qualsevol coloració serà òbviament monocromàtica. Per tant, per demostrar el teorema de Van der Waerden, és suficient que demostrem el següent:

Pas inductiu. Sigui $n \geq 1$ un enter; suposem que, per a qualsevol enter $l \geq 1$, l'afirmació $T(n,l)$ és certa; aleshores, per a qualsevol enter $k \geq 1$, l'afirmació $T(n+1,k)$ és certa.

És de sentit comú que el teorema de Van der Waerden és conseqüència de la validesa de $T(1,k)$ per a tot k i del que hem anomenat *pas inductiu*; aquest argument és un exemple de demostració per inducció.

Demostrem, doncs, el pas inductiu. Prenem un enter $n \geq 1$ i suposem que, per a qualsevol enter $l \geq 1$, l'afirmació $T(n,l)$ és certa. És a dir, suposem que existeix, per a tot l, un enter $W(n,l)$ amb la propietat especificada per $T(n,l)$ (d'aquesta suposició se'n diu *hipòtesi inductiva*, perquè és la hipòtesi a partir de la qual demostrarem el pas inductiu).

Prenem un nombre natural k. El nostre objectiu és demostrar $T(n+1,k)$ usant la hipòtesi inductiva. (Observem que $T(n+1,1)$ és trivialment certa prenent $W(n+1,1) = n+1$. Per tant, cal que $k \geq 2$ perquè $T(n+1,k)$ no sigui trivial. Tot i això, els arguments que segueixen són vàlids fins i tot quan $k = 1$.) Per a la comoditat del lector, hem organitzat la demostració dividint-la en quatre passos.

Pas 1. Definim una successió de nombres naturals $N_0, N_1, \ldots, N_k$ així:

$$N_0 = 1\,, \qquad N_j = 2W(n, k^{N_{j-1}}) + N_{j-1} \quad \text{per a tot } 1 \leq j \leq k\,.$$

Veurem que qualsevol k-coloració de $S = \{1, \ldots, N_k\}$ conté alguna progressió monocromàtica de longitud $n+1$, de manera que podem prendre $W(n+1,k) = N_k$.

Pas 2. Sigui C un conjunt de k elements (els *colors*), i sigui

$$f\colon S \to C$$

una aplicació qualsevol (la *coloració*). En aquest pas construirem, per a tot enter j dins el conjunt $\{1, 2, \ldots, k\}$:

- tres conjunts $S_j'' \subset S_j' \subset S_j$, i
- una progressió aritmètica

$$\{a_j, a_j + d_j, \ldots, a_j + (n-1)d_j\} \subset S_j''$$

amb la propietat que per a tot $0 \leq t \leq N_{j-1}$ i tot $0 \leq r \leq n-1$ se satisfà que

$$f(a_j + t) = f(a_j + rd_j + t)\,,$$

i que a més a més

$$a_j + nd_j \in S'_j\,. \tag{1}$$

Aquests conjunts, a més, satisfaran que

$$S_1 \subset S_2 \subset \cdots \subset S_k = S\,.$$

Procedirem per inducció descendent, començant amb $j = k$ i fent decréixer j una unitat a cada pas. Definim:

$$\begin{aligned} S_k &= \{1, 2, \ldots, 2W(n, k^{N_{k-1}}) + N_{k-1}\} = \{1, 2, \ldots, N_k\} = S\,,\\ S'_k &= \{1, 2, \ldots, 2W(n, k^{N_{k-1}})\}\,,\\ S''_k &= \{1, 2, \ldots, W(n, k^{N_{k-1}})\}\,. \end{aligned}$$

Considerem ara l'aplicació

$$f_k \colon S''_k \to C^{N_{k-1}}\,, \qquad f_k(t) = \big(f(t), f(t+1), f(t+2), \ldots, f(t+N_{k-1}-1)\big)\,.$$

L'aplicació f_k està ben definida, ja que si $t \in S''_k$ aleshores $t + N_{k-1} - 1 \in S_k = S$. L'observació clau és que podem mirar-nos f_k com una nova coloració, on el conjunt de colors C ha estat substituït pel conjunt $C^{N_{k-1}}$ (que, en general, té moltíssims més elements que C). Per tant, podem aplicar la hipòtesi inductiva (que afirma l'existència de $W(n, l)$ per a qualsevol nombre de colors l, en particular per a $l = k^{N_{k-1}}$) i deduir que existeix una progressió aritmètica

$$\{a_k, a_k + d_k, \ldots, a_k + (n-1)d_k\} \subset S''_k\,,$$

on $d_k \geq 1$, monocromàtica respecte a la coloració f_k. A més a més, de la definició dels conjunts S''_k i S'_k es dedueix que

$$a_k + nd_k \in S'_k\,.$$

En efecte, d'una banda $a_k + (n-1)d_k \in S''_k$, i de l'altra $d_k \leq W(n, k^{N_{k-1}})$, ja que d_k és la diferència d'una progressió aritmètica de longitud ≥ 2 continguda en un conjunt format per $W(n, k^{N_{k-1}})$ enters consecutius; com que S'_k s'obté afegint a S''_k els $W(n, k^{N_{k-1}})$ enters que hi ha a continuació de l'element més gran de S''_k, resulta que $a_k + (n-1)d_k + d_k = a_k + nd_k$ pertany a S'_k.

Sigui ara j un element del conjunt $\{1, 2, \ldots, k-1\}$, i suposem que ja hem definit $S_{j+1}, S'_{j+1}, S''_{j+1}, a_{j+1}, d_{j+1}$. Llavors definim, seguint la mateixa idea d'abans,

$$\begin{aligned} S_j &= \{a_{j+1}, a_{j+1} + 1, \ldots, a_{j+1} + 2W(n, k^{N_{j-1}}) + N_{j-1} - 1\} =\\ &= \{a_{j+1}, a_{j+1} + 1, \ldots, a_{j+1} + N_j - 1\}\\ S'_j &= \{a_{j+1}, a_{j+1} + 1, \ldots, a_{j+1} + 2W(n, k^{N_{j-1}}) - 1\}\\ S''_j &= \{a_{j+1}, a_{j+1} + 1, \ldots, a_{j+1} + W(n, k^{N_{j-1}}) - 1\}\,. \end{aligned}$$

Observem que $S_j \subset S_{j+1}$, ja que:

1. l'element més petit de S_j, a_{j+1}, pertany a $S''_{j+1} \subset S'_{j+1} \subset S_{j+1}$,
2. S_j consta de N_j elements consecutius, i
3. S_{j+1} s'obté afegint a S'_{j+1} els N_j nombres consecutius després del nombre més gran de S'_{j+1}.

Considerem l'aplicació

$$f_j \colon S''_j \to C^{N_{j-1}}, \qquad f_j(t) = \big(f(t), f(t+1), f(t+2), \ldots, f(t+N_{j-1}-1)\big),$$

que està ben definida gràcies als mateixos arguments que hem usat per justificar la definició de f_k juntament amb el fet que $S_j \subset S$. Aplicant la hipòtesi inductiva, deduïm que existeix una progressió aritmètica

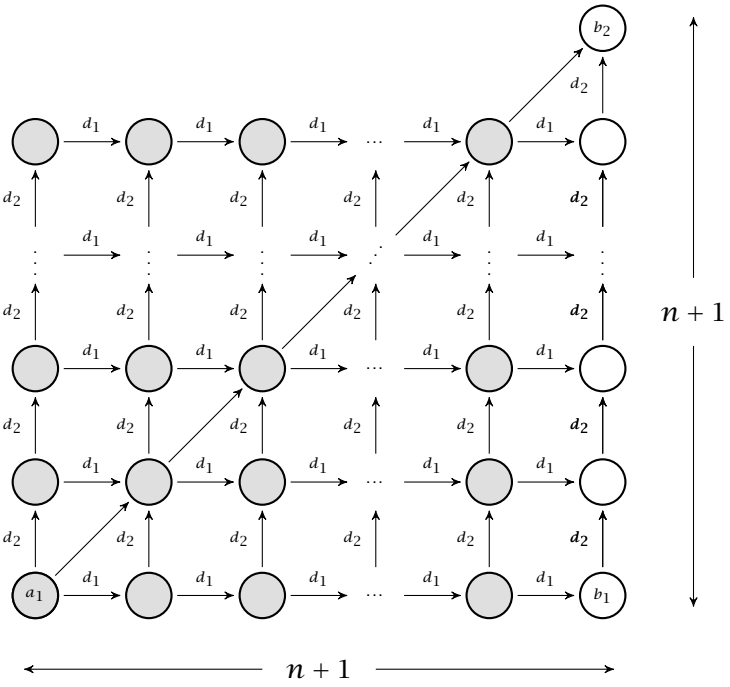
$$\{a_j, a_j + d_j, \ldots, a_j + (n-1)d_j\} \subset S''_j,$$

on $d_j \geq 1$, monocromàtica respecte a la coloració f_j. Pel mateix argument d'abans sabem que a més a més se satisfà que

$$a_j + nd_j \in S'_j,$$

com de fet volíem.

EXEMPLE: EL CAS DE DOS COLORS. Quan $n = 2$, podem representar el resultat de les construccions anteriors de manera semblant a com hem representat gràficament les idees de la demostració del teorema 1:



Cada disc representa un element de S. La cantonada inferior esquerra representa a_1. Quan passem d'un disc a un altre seguint una fletxa etiquetada d_j saltem d'un element de S a l'element que resulta de sumar-hi d_j. Per tant, tant les files, com les columnes, com la diagonal indicada representen progressions aritmètiques dins S. Per entendre com aquesta configuració resulta de la construcció especificada anteriorment, observem que podem mirar-nos les files del diagrama com a elements d'una progressió aritmètica monocromàtica.

Cada fila és alhora una progressió aritmètica, de manera que si ignorem el disc superior de la columna de la dreta (que hem etiquetat b_2) el diagrama és una «progressió aritmètica formada per progressions aritmètiques». En aquest cas la demostració es pot acabar de la manera següent: com que només tenim dos colors, per evitar de formar progressions aritmètiques de longitud $n+1$ de color clar, cal que tots els discos de la columna dreta, llevat possiblement de b_2, siguin foscos. Però llavors, si colorem el disc b_2 de gris fosc, la columna de la dreta forma una progressió artimètica de longitud $n+1$ fosca, i si el colorem gris clar, la diagonal indicada forma una progressió de longitud $n+1$ clara. En qualsevol dels casos, doncs, obtenim una progressió monocromàtica de longitud $n+1$.

Si enlloc de dos colors en fem servir una quantitat $k \geq 3$, l'argument anterior no funciona, ja que podríem fer servir un color diferent del gris clar per als discos de la fila dreta diferents de b_2 i un altre color, diferent de tots dos, per al disc b_2. Això motiva que, en general, haguem de construir una «estructura k-dimensional» anàloga a la que hem representat en el cas $k = 2$.

Pas 3. En els dos lemes següents demostrarem algunes propietats de la construcció anterior que ens permetran concloure la demostració.

LEMA 3. *Per a tot enter* $1 \leq j \leq k$ *se satisfà* $a_1 + nd_1 + nd_2 + \cdots + nd_j \in S_j$.

PROVA. Raonem per inducció ascendent. Quan $j = 1$ cal veure que $a_1 + nd_1 \in S_1$, que és (1). Suposem ara que $j > 1$ i que $a_1 + nd_1 + \cdots + nd_{j-1} \in S_{j-1}$. Per demostrar que $a_1 + nd_1 + nd_2 + \cdots + nd_j \in S_j$ és suficient que demostrem que per a tot element $t \in S_{j-1}$ se satisfà $t + nd_j \in S_j$. Ara bé, tot element t de S_{j-1} es pot escriure de la forma $t = a_j + u$, essent $0 \leq u \leq N_{j-1} - 1$, de manera que $t + nd_j = a_j + nd_j + u$. Gràcies a (1) sabem que $a_j + nd_j \in S'_j$. Però com que $0 \leq u \leq N_{j-1}$, el mateix argument que hem fet servir abans permet deduir, de la darrera inclusió, que $a_j + nd_j + u \in S_j$. □

Per a qualsevol conjunt de coeficients $\lambda = (\lambda_1, \ldots, \lambda_k) \in \Lambda := \{0, \ldots, n\}^k$, escriurem

$$a(\lambda) = a(\lambda_1, \ldots, \lambda_k) := a_1 + \sum_j \lambda_j d_j \,.$$

El lema anterior implica que $a(\lambda) \in S$ per a tot $\lambda \in \Lambda$. Per a tot $\lambda = (\lambda_1, \ldots, \lambda_k) \in \Lambda$ definim

$$\lambda^* := \begin{cases} (0, \ldots, 0) \in \Lambda & \text{si } \lambda_j \leq n-1 \text{ per a tot } j \\ (\lambda_1, \ldots, \lambda_i, 0, \ldots, 0) \in \Lambda & \text{si } \lambda_i = n \text{ i } \lambda_j \leq n-1 \text{ per a tot } j > i \,. \end{cases}$$

LEMA 4. *Per a tot $\lambda \in \Lambda$ se satisfà que $f(a(\lambda)) = f(a(\lambda^*))$.*

PROVA. Sigui $\lambda = (\lambda_1, \ldots, \lambda_k)$. Per comprovar que $f(a(\lambda)) = f(a(\lambda^*))$, és suficient demostrar que

$$f(a(\lambda_1, \ldots, \lambda_{j-1}, \lambda_j, 0, \ldots, 0)) = f(a(\lambda_1, \ldots, \lambda_{j-1}, 0, 0, \ldots, 0)) \tag{2}$$

sempre que $\lambda_j \leq n-1$. Considerem la suma parcial

$$p = a(\lambda_1, \ldots, \lambda_{j-1}, 0, \ldots, 0) = a_1 + \sum_{i=1}^{j-1} \lambda_i d_i .$$

Pel lema 3 sabem que $p \in S_{j-1}$. Com que $\{a_j, a_j + d_j, \ldots, a_j + (n-1)d_j\} \subset S_j''$ és monocromàtica respecte a f_j i $S_{j-1} = \{a_j, a_j + 1, \ldots, a_j + N_{j-1} - 1\}$, resulta que per a tot $t \in S_{j-1}$ i tot $0 \leq r \leq n-1$ se satisfà la igualtat $f(t) = f(t + rd_j)$. En particular, prenent $t = p$ i $r = \lambda_j$ obtenim $f(p + \lambda_j d_j) = f(p)$, que és la igualtat (2) que volíem demostrar. □

Pas 4. Definim, per a tot $0 \leq j \leq k$,

$$b_j = a_1 + \sum_{i=0}^{j} nd_i = a(\overbrace{n, \ldots, n}^{j}, \overbrace{0, \ldots, 0}^{k-j}) .$$

(Quan $k = 2$ els nombres b_1, b_2 coincideixen amb els indicats en el diagrama que hem mostrat al final del Pas 2, mentre que $b_0 = a_1$.) Com que les imatges $\{f(b_0), f(b_1), \ldots, f(b_k)\}$ prenen valors en un conjunt de k elements, hi ha d'haver un parell d'imatges iguals. És a dir, han d'existir $0 \leq pq \leq k$ amb $f(b_p) = f(b_q)$. Considerem ara, per a tot $0 \leq l \leq n$,

$$c_l = a_1 + \sum_{i=0}^{p} nd_i + \sum_{i=p+1}^{q} ld_i = b_p + \frac{l}{n}(b_q - b_p) .$$

Aleshores, pel lema 4, sabem que

$$f(c_0) = f(c_1) = \cdots = f(c_{n-1}) .$$

D'altra banda, $c_0 = b_p$ i $c_n = b_q$. Llavors $f(b_p) = f(b_q)$ implica que $f(c_n) = f(c_0)$. Combinant-ho amb les igualtats anteriors deduïm que

$$f(c_0) = f(c_1) = \cdots = f(c_{n-1}) = f(c_n) .$$

Per tant, els nombres $c_0, c_1, \ldots, c_n$ formen una progressió aritmètica monocromàtica de longitud n. Això acaba la demostració del teorema.

4.2 Comentaris

La demostració original del teorema de Van der Waerden (que és essencialment la que hem donat nosaltres) va aparèixer publicada a [34]. En aquest article Van der Waerden atribueix l'enunciat del teorema a Baudet. Anys després de publicar [34], Van der Waerden va publicar un article on explica el procés que el va dur a trobar la demostració del seu teorema. Aquest article, aparegut originalment en holandès, fou traduït a l'anglès a [35]. El recomanem vivament al lector. Una altra demostració del teorema de Van der Waerden, deguda a Lukomskaia (però que difereix molt poc de la demostració original), apareix a l'excel·lent llibre [19] (que, fem notar de passada, apareixerà properament traduït al català a les Publicacions Electròniques de la Societat Catalana de Matemàtiques).

Bartel Leendert van der Waerden *(Amsterdam, 1903 – Zuric, 1996) va treballar principalment en àlgebra, tot i que va fer contribucions en geometria algebraica, topologia, combinatòria (el teorema que hem vist és la seva contribució més coneguda en aquest camp) i també en teoria de nombres, probabilitat i mecànica quàntica. És conegut especialment pel seu tractat sobre àlgebra [36], publicat el 1930, on exposa per primer cop de manera sistemàtica els resultats fundacionals de Noether, Hilbert, Dedekind i Artin. Encara avui és una referència citada sovint.*

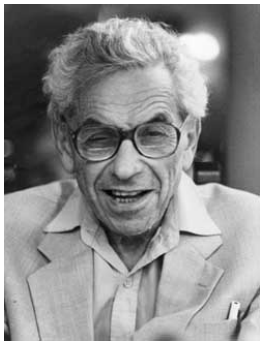
És un exercici fàcil deduir del teorema de Van der Waerden per a coloracions amb dos colors el teorema per a un nombre arbitrari de colors, i això podria inclinar-nos a pensar que el camí més senzill per demostrar el teorema de Van der Waerden passi per demostrar primerament el cas de dos colors. Molt probablement, però, demostrar separadament el cas de dos colors és molt més complicat que fer-ho directament per a un nombre arbitrari de colors (si més no, l'argument que hem usat per demostrar el pas inductiu deixaria de funcionar). Això és un exemple d'un fenomen remarcable i freqüent a les matemàtiques: bona part de la dificultat de progressar rau a enunciar els resultats amb el seu grau *natural* de generalitat, fins a l'extrem que pot donar-se que la manera més fàcil de demostrar un teorema passi per substituir-lo per un resultat més general. Com explica Van der Waerden a [35], un dels avenços crucials cap a la demostració del seu teorema va ser adonar-se (gràcies a un suggeriment d'Artin) que era més natural demostrar directament un teorema per a un nombre arbitrari de colors que limitar-se a coloracions amb dos colors.

Els nombres $W(n,k)$ que hem definit a la demostració del teorema creixen a una velocitat vertiginosa quan fem augmentar n o k, molt més ràpidament que qualsevol funció exponencial. Però, com ha quedat clar quan hem estudiat $T(3,2)$ a la secció 3, els arguments que hem donat no permeten obtenir fites òptimes, i en general l'afirmació $T(n,k)$ és certa per a valors de $W(n,k)$ molt

més petits que els que hem definit. Calcular el valor òptim de $W(n,k)$ (és a dir, el nombre natural $W_{n,k}$ per al qual existeix una k-coloració de $\{1,\ldots,W_{n,k}-1\}$ sense progressions monocromàtiques de longitud n, i no n'existeix cap de $\{1,\ldots,W_{n,k}\}$) és un problema obert del qual se sap ben poca cosa, tot i que s'hi han fet molts progressos des del resultat original de Van der Waerden. Les millors fites superiors conegudes avui dia són degudes a Gowers [11], i són conseqüència de la demostració nova que aquest matemàtic va donar del teorema de Szemerédi (en parlarem més endavant). Les millors fites inferiors que es coneixen van ser trobades per Berlekamp [2], usant teoria de Galois i cossos finits. El lector trobarà una breu discussió sobre aquests temes a l'article de Graham [13].

El teorema de Van der Waerden és un exemple de resultat de la *teoria de Ramsey*. Aquest nom, més que indicar una branca clarament delimitada de les matemàtiques o un conjunt de tècniques, es refereix a tota mena de resultats que afirmen que si trenquem un sistema prou complex i simètric en una quantitat controlada de peces, almenys alguna de les peces preservarà moltes de les simetries del sistema original. Què vol dir exactament a la frase anterior «sistema», «complex» o «simètric» és de mal precisar: és molt més senzill donar una llista de resultats de teoria de Ramsey.

Frank Plumpton Ramsey *(Cambridge, 1903 – Londres, 1930) va ser un dels matemàtics més brillants del Cambridge dels anys vint. Va fer contribucions importants a la fonamentació de les matemàtiques, tant pel cantó matemàtic com pel filosòfic. En l'article [26] sobre decidibilitat d'un fragment de la lògica de primer ordre va provar de passada un lema de combinatòria que va donar lloc a l'anomenada* teoria de Ramsey. *També va escriure sobre la fonamentació de la probabilitat i sobre economia.*



Pál Erdős *(Budapest, 1913 – Varsòvia, 1996), que apareixerà sovint en aquestes notes, va ser un dels matemàtics més notables del segle xx. Autor d'una quantitat ingent d'articles en combinatòria, teoria de nombres, probabilitats i anàlisi, i autèntic mestre en l'art de la resolució de problemes, és el protagonista d'un bon nombre d'anècdotes i llegendes que fan quedar curts els tòpics més habituals sobre el caràcter poc usual dels matemàtics. Qualsevol insistència és poca a l'hora d'aconsellar fullejar, llegir i rellegir els articles del recull [4], molts dels quals donen resultats de la teoria de Ramsey.*

El resultat demostrat per Ramsey té moltes aplicacions. Citem, com a exemple, un bonic corol·lari del teorema de Ramsey, degut a Erdős i Szekeres, que el lector trobarà a [5] o [4]: «Per a tot nombre natural k, existeix un nombre natural $N(k)$ amb la propietat que tot conjunt S de $N(k)$ punts al pla que no contingui cap terna de punts alineats conté un subconjunt de k elements que són els vèrtexs d'un k-gon convex.»

5 El teorema de Szemerédi

5.1 El teorema de Van der Waerden per a coloracions de $\mathbb{N}$

El teorema de Van der Waerden (teorema 2) implica immediatament el resultat següent.

TEOREMA 5. *Sigui k un nombre natural. Per a qualsevol k-coloració de $\mathbb{N}$ existeixen progressions aritmètiques monocromàtiques (finites) arbitràriament llargues.*

Aquest teorema *no* afirma que en tota k-coloració existeixi una progressió aritmètica infinita monocromàtica, que de fet no té per què existir. Per exemple, si colorem els nombres naturals usant dos colors, colorant blocs de nombres consecutius alternant tots dos colors i fent que els blocs siguin cada cop més grans, obtindrem una coloració que no conté cap progressió aritmètica infinita monocromàtica.

És un exercici interessant demostrar que el teorema 5 també implica el teorema 2, de manera que tots dos teoremes són equivalents.

5.2 Subconjunts de densitat positiva: el teorema de Szemerédi

El teorema de Van der Waerden garanteix que, si trenquem el conjunt dels nombres naturals en una quantitat finita de conjunts, almenys algun dels conjunts conté progressions aritmètiques arbitràriament llargues. Però no proporciona cap manera de saber quin dels conjunts té aquesta propietat. Això planteja el problema de donar un criteri que garanteixi que un conjunt donat $A \subset \mathbb{N}$ conté progressions aritmètiques arbitràriament llargues, i que sigui prou lax com per permetre que en qualsevol descomposició del conjunt dels nombres naturals en una quantitat finita de conjunts almenys un dels conjunts satisfaci el criteri.

Erdős i Turán van conjecturar l'any 1936 que un possible criteri és demanar que el conjunt tingui densitat superior positiva. Que un conjunt $A \subset \mathbb{N}$ tingui densitat superior positiva vol dir que existeix un nombre real $\delta > 0$ i una successió de nombres naturals $n_1, n_2, n_3, \dots$ que tendeix cap a infinit, amb la propietat que

$$|A \cap \{1, \dots, n_j\}| \geq \delta \cdot n_j$$

per a tot j, on, si B és un conjunt finit, denotem per $|B|$ la quantitat d'elements de B. És a dir, per a tot j, la proporció d'elements de $\{1, \dots, n_j\}$ que pertanyen a A és $\geq \delta$. És un exercici senzill veure que, si $\mathbb{N} = A_1 \cup \cdots \cup A_k$ és una

descomposició qualsevol, aleshores almenys un dels A_j té densitat superior positiva.

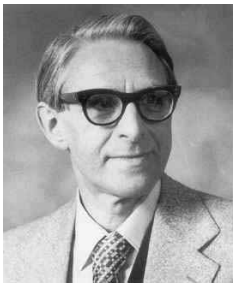
La conjectura proposada per Erdős i Turán l'any 1936 (vegeu [6]) és doncs:

CONJECTURA 6 (ERDŐS, TURÁN). Si $A \subset \mathbb{N}$ té densitat superior positiva, aleshores A conté progressions aritmètiques arbitràriament llargues.

Aquesta conjectura és molt més profunda que el teorema de Van der Waerden. Van passar més de quinze anys abans que Roth n'obtingués els primers resultats parcials, en resoldre l'any 1953 [27] el cas de progressions de longitud 3:

TEOREMA 7 (ROTH). *Si $A \subset \mathbb{N}$ té densitat superior positiva, aleshores A conté infinites progressions aritmètiques de longitud* 3.

El teorema de Roth té un aspecte enganyós: el seu enunciat és tan senzill i es refereix a objectes tan simples, que fàcilment pot semblar menys profund del que realment és. Per demostrar-lo, Roth va fer servir l'anomenat *mètode dels arcs* de Hardy i Littlewood per estimar els coeficients de Fourier de la funció indicadora del conjunt A projectat en un grup quocient $\mathbb{Z}/N\mathbb{Z}$, on N és prou gran. La seva demostració, amb més o menys variacions, es troba avui dia en diversos llibres de teoria additiva de nombres (vegeu per exemple [24, 33]).



Klaus Friedrich Roth *va néixer l'any 1925 a l'actual ciutat polonesa de Wrocław, que a l'època pertanyia a Alemanya, on és coneguda com a Breslau. Als catorze anys va anar a Anglaterra, on va rebre la seva formació com a matemàtic. És conegut sobretot per les seves contribucions a la teoria de nombres, notablement al camp de l'aproximació diofàntica. Especialment per aquests treballs va rebre la medalla Fields l'any 1958.*

El següent progrés significatiu en la conjectura d'Erdős i Turán el va obtenir Szemerédi en demostrar el cas de progressions de longitud 4, l'any 1969. Finalment, l'any 1975, el mateix Szemerédi va ser capaç de resoldre completament la conjectura [31]:

TEOREMA 8 (SZEMERÉDI). *Si $A \subset \mathbb{N}$ té densitat superior positiva, aleshores per a tot nombre natural n el conjunt A conté infinites progressions aritmètiques de longitud n.*

La demostració de Szemerédi és purament combinatòria i elemental, en el sentit que no fa servir eines avançades (com les que usa Roth per demostrar el teorema 7, per exemple), però segueix un argument extraordinàriament subtil i sofisticat. Està considerada una obra mestra cabdal en la combinatòria del segle XX, i alguna de les eines que hi apareixen per primer cop s'han convertit

en les últimes dècades en tècniques fonamentals en la combinatòria (com per exemple l'anomenat *lema de regularitat*).

Endre Szemerédi *(Budapest, 1940), a més de demostrar l'any 1975 la conjectura d'Erdős i Turán, ha fet altres contribucions de primer ordre a la combinatòria, especialment en teoria additiva de nombres i en teoria de grafs. Es va llicenciar a la cèlebre Universitat Eötvös Loránd de Budapest i va obtenir el títol de doctor a la Universitat de Moscou sota la direcció d'Israel Gelfand. Actualment és professor a la Universitat de Rutgers.*

5.3 Un exemple trivial

Una manera de construir conjunts de densitat superior positiva és la següent. Prenem un nombre natural D arbitràriament gran, i construïm $A \subset \mathbb{N}$ triant un element qualsevol dins de cada bloc de la forma

$$B_r = \{(r-1)D + 1, (r-1)D + 2, \dots, (r-1)D + D = rD\},$$

on r recorre el conjunt de nombres naturals. El conjunt obtingut té densitat superior positiva (podem prendre a la definició $\delta = D^{-1}$) i, per tant, pel teorema de Szemerédi, conté progressions aritmètiques arbitràriament llargues. Aquest fet, però, es pot demostrar usant el teorema de Van der Waerden. En efecte, si denotem per $c(r) \in \{1, \dots, D\}$, per a tot nombre natural r, el nombre natural per al qual $(r-1)D + c(r) \in A$, aleshores podem mirar-nos $c\colon \mathbb{N} \to \{1, \dots, D\}$ com una coloració dels nombres naturals amb D colors. El teorema de Van der Waerden diu que $\mathbb{N}$ conté progressions aritmètiques arbitràriament llargues i monocromàtiques respecte a c. Però una progressió aritmètica de longitud d monocromàtica respecte a c dóna lloc a una progressió aritmètica de la mateixa longitud i diferència dD continguda dins A, com el lector pot verificar fàcilment.

Construir subconjunts de $\mathbb{N}$ amb densitat superior positiva per als quals no es pugui demostrar l'existència de progressions aritmètiques sense recórrer al teorema de Szemerédi no és gens senzill. De fet, la dificultat més seriosa a l'hora de demostrar el teorema de Szemerédi apareix en considerar subconjunts $R \subset \mathbb{N}$ amb la propietat que els quocients $|R \cap \{1, \dots, n\}|/n$ van oscil·lant quan $n \to \infty$, i construir conjunts amb el grau *crític* d'oscil·lació és un problema delicat (per als conjunts que hem construït nosaltres aquest quocient convergeix a D^{-1} quan $n \to \infty$ i, per tant, no oscil·la). Vegeu la secció 8 de [32] per a alguns comentaris sobre aquesta qüestió.

5.4 Versió finita del teorema de Szemerédi

De la mateixa manera que el teorema de Van der Waerden admet dues versions equivalents, una referida a coloracions de $\mathbb{N}$ i l'altra a coloracions de conjunts finits de nombres naturals, el teorema de Szemerédi es pot reformular en un resultat equivalent però referit a conjunts finits, de la manera següent.

TEOREMA 9 (SZEMERÉDI). *Per a tot nombre real $\delta > 0$ i tot nombre natural n existeix un nombre natural $S(n,\delta)$ amb la propietat que qualsevol subconjunt $A \subset \{1,\dots,S(n,\delta)\}$ format per almenys $\delta \cdot S(n,\delta)$ elements conté alguna progressió aritmètica de longitud n.*

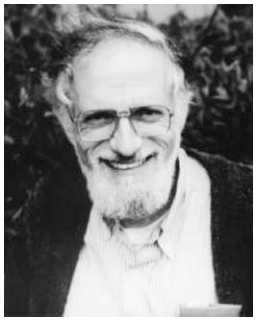
Com en el cas del teorema de Van der Waerden, és un problema molt interessant (i obert) estimar quin és el mínim valor possible per a $S(n,\delta)$. Se'n coneixen, però, fites superiors i inferiors. La millor fita inferior per a $n = 3$ ha estat durant molts anys una fita deguda a Behrend (vegeu la proposició 1.3 a [32]), obtinguda l'any 1946. Fa pocs anys Elkin va millorar lleugerament la fita de Behrend (vegeu l'article de Green i Wolf [17]). Una conseqüència de l'estimació de Behrend és que, quan $\delta \to 0$, $S(3,\delta)$ creix més ràpid que qualsevol funció polinomial en δ^{-1}. Aquest fet explica en part la dificultat de demostrar el teorema de Szemerédi, fins i tot en el cas $n = 3$. Pel que fa a fites superiors, el resultat general més fort que es coneix avui dia és que es pot prendre $S(n,\delta) \leq \exp(\delta^{-c(n)})$, on $c(n) = 2^{2^{n+9}}$. Aquesta fita és conseqüència de la nova demostració del teorema de Szemerédi trobada per Gowers [11], i implica una fita similar per als nombres $W_{n,k}$ dels quals hem parlat a la secció 4.2, ja que $W_{n,k} \leq S(n,k^{-1})$. Per a valors petits de n, existeixen fites encara millors que la de Gowers. La millor estimació per a $n = 3$ a dia d'avui és deguda a Sanders [29] i afirma que si un subconjunt $A \subset \{1,2,\dots,n\}$ no conté cap progressió de longitud 3 aleshores el nombre d'elements de A és com a màxim $C(n(\log\log n)^5/\log n)$, on $C > 0$ és una certa constant independent de n.

5.5 Noves demostracions del teorema de Szemerédi

Poc després que Szemerédi publiqués el seu teorema, Furstenberg a [8] va donar-ne una nova demostració des d'una perspectiva completament diferent, passant sorprenentment per una interpretació del resultat en termes de teoria ergòdica.

La teoria ergòdica va néixer originàriament per estudiar aspectes qualitatius de sistemes dinàmics que tenen tendència a generar desordre, cosa que els fa massa complexos per ser estudiats amb precisió de manera quantitativa (un exemple típic són els sistemes estudiats per la termodinàmica). Inicialment els sistemes dinàmics estudiats per la teoria ergòdica eren diferencials, però més tard la teoria ergòdica es va estendre a l'anomenada *dinàmica simbòlica*, dins de la qual Fursternberg va interpretar el teorema de Szemerédi. Poc després de la publicació de [8] el punt de vista adoptat per Furstenberg va

permetre obtenir generalitzacions del teorema original de Szemerédi, entre aquestes un anàleg per a subconjunts de $\mathbb{N}^d$ amb densitat superior positiva (durant molts anys no es va saber com demostrar aquesta generalització sense recórrer a la teoria ergòdica). La demostració d'aquests resultats, obtinguts en col·laboració amb Katznelson, va ser simplificada posteriorment per Ornstein. Hi ha dues referències excel·lents per llegir sobre aquests resultats: d'una banda la monografia de Furstenberg [9], una lectura deliciosa i altament instructiva i recomanable; de l'altra, l'article [10], on els autors reïxen a donar una exposició notablement clara d'aquests resultats en poques pàgines (però assumint per part del lector un pèl més de rodatge que a [9]).



Hillel Furstenberg *(Berlín, 1935) és l'autor d'un bon nombre de resultats fonamentals en teoria ergòdica, que ha aplicat amb gran virtuosisme en moltes àrees de les matemàtiques, com la teoria de nombres, la probabilitat o els grups de Lie. Als anys cinquanta va publicar a l'*American Mathematical Monthly *una demostració de l'existència d'infinits nombres primers basada en arguments topològics [7]. És conegut pels seus profunds resultats sobre productes de matrius aleatòries, per haver introduït conceptes crucials com la vora de Furstenberg d'espais simètrics o per la demostració de l'existència d'una única mesura invariant sota el flux horocíclic en superfícies de curvatura constant (un dels precursors del cèlebre teorema de Ratner sobre fluxos unipotents). L'any 2007 va rebre el prestigiós Premi Wolf de matemàtiques.*

L'any 2001 Gowers [11] va publicar una nova demostració del teorema de Szemerédi que generalitza les idees principals de la demostració de Roth del cas $n = 3$. Recordem que Roth va obtenir el seu resultat estudiant els coeficients de Fourier de la funció indicadora d'un conjunt $A \subset \mathbb{N}$. La idea bàsica de Roth és detectar progressions aritmètiques de longitud 3 mirant adequadament aquests coeficients de Fourier. Aquesta estratègia es pot estendre, amb dificultats considerables, a progressions de longitud 4 (el mateix Roth ho va dur a terme a [28]), però deixa de funcionar per a progressions de longitud 5 o més. Gowers aconsegueix superar aquesta dificultat considerant versions no lineals dels coeficients de Fourier. A grans trets, la idea bàsica de Gowers és, donat un subconjunt $A \subset \mathbb{N}$ amb densitat superior positiva, mirar si A és suficientment *aleatori* en un cert sentit. Si A no és aleatori, aleshores és senzill trobar-hi progressions aritmètiques (l'exemple que hem donat a la secció 5.3 és un conjunt molt poc aleatori —tot i que a la seva construcció hi hem fet intervenir un cert grau d'aleatorietat— i ja hem vist que amb el teorema de Van der Waerden n'hi ha prou per trobar-hi progressions aritmètiques); i si A és aleatori aleshores, considerant la intersecció de A amb alguna progressió aritmètica prou llarga i ben trobada, obtenim un nou conjunt que té densitat significativament més

gran que A. Llavors repetim l'argument tantes vegades com calgui fins a trobar una progressió aritmètica. Aquest argument iteratiu està present, de fet, en totes les demostracions del teorema de Szemerédi, començant per la demostració original. Una de les novetats de l'article de Gowers és que s'hi dóna una manera de definir rigorosament la noció d'*aleatorietat* fent servir versions no lineals de la teoria de Fourier, que té la virtut de permetre implementar la idea anterior. Amb aquestes eines Gowers aconsegueix, a més de donar una nova demostració del teorema de Szemerédi, obtenir les millors fites conegudes avui dia per als nombres $S(n,\delta)$. A part de l'interès dels resultats demostrats i de les noves tècniques usades, l'article [11] està extraordinàriament ben escrit, i cada un dels ingredients que hi apareixen està molt ben motivat amb exemples que els justifiquen.

William Timothy Gowers *(Wiltshire, Anglaterra, 1963) va demostrar tenir un talent extraordinari per a les matemàtiques des de ben jove. L'any 1981 va rebre una medalla d'or a l'Olimpíada Internacional de Matemàtiques, amb una puntuació de 42 punts sobre 42. Format a Cambridge, va ser estudiant del matemàtic hongarès Béla Bollobás. L'any 1998 va rebre la medalla Fields, per les seves contribucions a l'anàlisi funcional (un dels seus resultats més coneguts és la construcció, per primer cop, d'un espai de Banach de dimensió infinita que no és isomorf a cap dels seus hiperplans). Molts dels seus resultats, inclosos els d'anàlisi funcional, estan basats en arguments molt subtils de teoria de Ramsey.*

Una altra demostració del teorema de Szemerédi va ser obtinguda per Nagle, Rödl i Schacht [21] l'any 2006. Aquesta demostració es pot estendre a subconjunts de $\mathbb{N}^d$ amb densitat superior positiva, cosa que permet redemostrar combinatòriament els resultats que Furstenberg i Katznelson van obtenir usant teoria ergòdica.

Finalment, molt recentment (tot just fa uns mesos) Green i Tao [16] han obtingut una nova demostració del teorema de Szemerédi, basada parcialment en les idees de Gowers.

6 Progressions aritmètiques de nombres primers: el teorema de Green-Tao

6.1 Densitat superior del conjunt dels nombres primers

Els nombres primers han estat, des del temps de la Grècia clàssica, un dels objectes fonamentals d'estudi de la teoria de nombres i per extensió de les matemàtiques. Avui dia se'n saben moltes coses, però encara hi ha moltíssimes

preguntes relacionades amb els nombres primers que no se saben respondre. Algunes tenen un enunciat completament senzill i elemental, com per exemple la que demana si existeixen infinites parelles de primers de la forma $(p, p+2)$ (els primers que són d'aquesta forma solen anomenar-se *primers bessons*).

Un problema que ha rondat pel món de les matemàtiques durant més d'un segle (o possiblement més) és saber si el conjunt dels nombres primers conté progressions aritmètiques arbitràriament llargues. Al segle XVIII Lagrange i Waring van estudiar progressions aritmètiques formades per nombres primers, preguntant-se en particular quant gran ha de ser la seva diferència. Una famosa conjectura de 1923 deguda a Hardy i Littlewood [18] implica en particular l'existència de progressions aritmètiques de nombres primers arbitràriament llargues. L'any 1939 Van der Corput [3] va demostrar que hi ha infinites ternes de nombres primers en progressió aritmètica.

Erdős i Turán van conjecturar el resultat següent, en gran part motivats pel problema de l'existència de progressions aritmètiques arbitràriament llargues de nombres primers (problema que van contribuir a popularitzar):

CONJECTURA 10 (ERDŐS, TURÁN). Si $A \subset \mathbb{N}$ és un subconjunt amb la propietat que la sèrie $\sum_{a\in A} a^{-1}$ divergeix, aleshores A conté progressions aritmètiques arbitràriament llargues.

Aquesta conjectura implica el teorema de Szemerédi (és un exercici interessant demostrar-ho, usant per exemple la divergència de la sèrie harmònica $\sum_{n\in\mathbb{N}} n^{-1}$).

La conjectura d'Erdős i Turán també implica l'existència de progressions aritmètiques arbitràriament llargues de primers, gràcies al fet que

$$\sum_{p} \frac{1}{p} = \infty\,, \tag{3}$$

on la variable p del sumatori recorre el conjunt de tots els nombres primers (usarem aquesta notació, molt habitual a la teoria de nombres, en algunes de les fórmules que apareixeran a continuació). La divergència de (3) es pot demostrar usant la divergència de la sèrie harmònica, el fet que per a tot nombre natural N

$$\sum_{n=1}^{N} \frac{1}{n} \leq \prod_{1<p\leq N} (1 + p^{-1} + p^{-2} + \dots) = \prod_{1<p\leq N} \left(1 - \frac{1}{p}\right)^{-1},$$

i un resultat bàsic d'anàlisi que afirma que, si $I \subset \mathbb{N}$ és un conjunt qualsevol i $\{\alpha_i\}_{i\in I}$ són nombres reals qualssevol continguts dins l'interval $(0,1) \subset \mathbb{R}$, aleshores $\prod_{i\in I}(1-\alpha_i) > 0$ si i només si $\sum_{i\in I} \alpha_i$ convergeix.

La conjectura d'Erdős i Turán roman completament oberta. Podríem plantejar-nos, doncs, si el teorema de Szemerédi ens permet concloure que existeixen progressions aritmètiques arbitràriament llargues de primers. La resposta és que no, ja que el conjunt de nombrers primers, tot i ser un conjunt infinit (com demostra per exemple (3)), no té densitat superior positiva. Per demostrar-ho,

ens serà còmoda la notació següent: donat un nombre natural x denotem per $\pi(x)$ la quantitat de nombres primers menors o iguals a x. Veurem que

$$\lim_{x\to\infty} \frac{\pi(x)}{x} = 0\,, \tag{4}$$

cosa que implica immediatament el que hem dit.

Per trobar una fita superior de $\pi(x)$ farem servir les desigualtats següents, on n és un nombre natural qualsevol:

$$\prod_{n<p\le 2n} p \le \binom{2n}{n} \le 2^{2n}\,. \tag{5}$$

Per demostrar la desigualtat de la dreta, recordem que $\binom{2n}{n}$ és la quantitat de subconjunts de $\{1,\dots,2n\}$ formats per n elements, mentre que 2^{2n} és la quantitat de tots els subconjunts de $\{1,\dots,2n\}$. Òbviament, la primera quantitat no pot ser més gran que la segona. Per demostrar la desigualtat de l'esquerra usem la fórmula següent:

$$\binom{2n}{n} = \frac{2n\cdot(2n-1)\cdot(2n-2)\cdot\ldots\cdot(n+1)}{n\cdot(n-1)\cdot(n-2)\cdot\ldots\cdot 2\cdot 1}\,,$$

i el fet que els nombres primers que satisfan $np \le 2n$ apareixen al numerador però no al denominador: això implica que $\prod_{np\le 2n} p$ divideix $\binom{2n}{n}$, d'on deduïm immediatament la desigualtat. (Observem que en aquest darrer argument estem usant implícitament que $\binom{2n}{n}$ és un nombre natural.)

Prenent logaritmes en base 2 als extrems de (5) deduïm que

$$\pi(2n) - \pi(n) \le \frac{2n}{\log_2 n}\,. \tag{6}$$

Vegem com aquesta desigualtat ens permet demostrar que

$$\pi(2^k) \le \frac{2^{k+2}}{k} \tag{7}$$

per a tot nombre natural k. Farem servir inducció. Observem primerament que si $k \in \{1,2,3,4\}$ llavors (7) se satisfà de manera trivial, ja que d'una banda

$$k \le 4 \qquad \Longrightarrow \qquad \frac{2^{k+2}}{k} = \frac{4}{k}2^k \ge 2^k$$

i de l'altra la quantitat de nombres primers dins el conjunt $\{1,2,3,\dots,2^k\}$ no pot ser més gran que 2^k. Suposem ara que $r > 4$ i que (7) se satisfà per a tot $k \le r-1$. Llavors estimem, usant (6) i la hipòtesi inductiva,

$$\pi(2^{r+1}) \le \pi(2^r) + \frac{2^{r+1}}{r} \le \frac{2^{r+2}}{r} + \frac{2^{r+1}}{r} = \left(\frac{1}{2}+\frac{1}{4}\right)\frac{2^{r+3}}{r} = \frac{3}{4}\frac{2^{r+3}}{r} \le \frac{2^{r+3}}{r+1}\,,$$

ja que per a tot nombre positiu r es tenen les equivalències següents:

$$\frac{3}{4}\frac{1}{r} \leq \frac{1}{r+1} \qquad \Longleftrightarrow \qquad 3r+3 \leq 4r \qquad \Longleftrightarrow \qquad 3 \leq r\,.$$

En general, si $x \geq 1$ és un nombre natural qualsevol, existeix un únic enter k (igual a la part entera de $\log_2 x$) per al qual $2^k \leq x 2^{k+1}$, de manera que podem estimar

$$\frac{\pi(x)}{x} < \frac{\pi(2^{k+1})}{2^k} = 2\frac{\pi(2^{k+1})}{2^{k+1}} \leq 2\frac{4}{k+1}\,.$$

Com que $k = [\log_2 x]$ convergeix cap a ∞ quan $x \to \infty$, la desigualtat anterior implica immediatament (4).

Hi ha moltes altres maneres de demostrar que $\pi(x)/x$ convergeix a 0. Es pot usar, per exemple, el garbell (o sedàs) d'Eratòstenes: suposem que $p_1, p_2, \ldots, p_r$ són els r primers nombres primers (el joc de paraules no és intencionat). El principi d'inclusió-exclusió implica que, per a tot nombre natural n, la quantitat de nombres dins $\{1, 2, \ldots, n\}$ que no són divisibles per cap dels $p_1, \ldots, p_r$ és igual a la suma de $n(1-p_1^{-1})(1-p_2^{-1})\ldots(1-p_r^{-1})$ més un nombre real amb el valor absolut afitat superiorment de manera independent de n. Com que, com hem vist, $\prod_{j=1}^{r}(1-p_j^{-1})$ convergeix a 0 quan $r \to \infty$, obtenim novament el que volíem. L'estratègia que hem seguit anteriorment té, però, un avantatge sobre la que acabem d'esbossar: implica l'existència d'una constant $C > 0$ amb la propietat que, per a tot nombre natural x, se satisfà

$$\pi(x) \leq C\frac{x}{\ln x}$$

(deixem la comprovació d'aquest fet com un exercici per al lector).

La conclusió és que el teorema de Szemerédi no permet afirmar que existeixen progressions aritmètiques arbitràriament llargues de nombres primers. (Notem de passada que aquest exemple mostra que la conjectura d'Erdős i Turán —la conjectura 10— és estrictament més forta que el teorema de Szemerédi.) Òbviament, que el conjunt dels nombres primers no satisfaci la condició del teorema de Szemerédi no implica que el conjunt dels nombres primers no contingui progressions aritmètiques arbitràriament llargues.

La història, però, no s'acaba aquí. L'any 2008 Green i Tao van publicar l'article [15] (els resultats, però, s'havien fet públics ja l'any 2004), on demostren que existeixen progressions aritmètiques arbitràriament llargues de nombres primers, i van obtenir així un dels teoremes més bonics i espectaculars dels últims anys.

Abans de parlar (molt breument) del resultat de Green i Tao, val la pena que ens aturem a comentar algunes qüestions relacionades amb els càlculs que hem fet en aquesta secció. Un cop sabem que el quocient $\pi(x)/x$ convergeix cap a 0 quan x se'n va a ∞ podem preguntar-nos a quina velocitat convergeix o, més precisament, si hi ha alguna funció *senzilla* que doni una bona aproximació de $\pi(x)/x$ (i que, com més gran sigui x, més bona sigui). Voldríem, doncs, tenir una manera d'estimar amb precisió la quantitat de nombres primers $\leq x$.

Estudiant taules de nombres primers, tant Legendre com Gauss van conjecturar a final del segle XVIII i principi del XIX que $x/\ln x$ dóna una bona aproximació de la funció $\pi(x)$:

$$\pi(x) \sim x/\ln x\,.$$

Amb aquesta notació volem dir el següent:

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1\,.$$

En altres paraules, $\pi(x)/x \sim (\ln x)^{-1}$, cosa que respon a la pregunta anterior. Al voltant de 1850, Txebixef va obtenir alguns resultats parcials encaminats a la solució de la conjectura de Legendre i Gauss. En particular, va demostrar l'existència de constants positives C_1 i C_2 per a les quals

$$C_1 \frac{x}{\ln x} \le \pi(x) \le C_2 \frac{x}{\ln x} \tag{8}$$

per a tot nombre natural x. Les mateixes tècniques que el dugueren a aquest resultat li van permetre demostrar també l'anomenat *postulat de Bertrand*, que afirma que, per a tot nombre natural n, existeix algun nombre primer entre n i $2n$. El 1932, a l'edat de dinou anys, Erdős va donar una nova demostració completament elemental del postulat de Bertrand basada en una estimació molt similar a (5). Anàlogament, amb idees semblants es pot demostrar (8): la desigualtat de la dreta és, com hem dit, una conseqüència immediata dels arguments que hem donat anteriorment; pel que fa a la desigualtat de l'esquerra, vegeu per exemple el teorema 4.6 de [1].

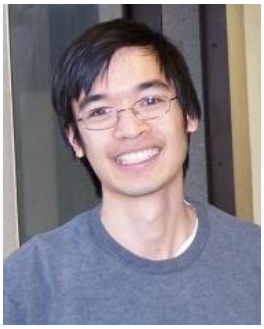
El 1896 la conjectura de Legendre i Gauss va ser demostrada independentment per Hadamard i De la Vallée-Poussin, i es va convertir, doncs, en un teorema (anomenat habitualment *teorema dels nombres primers*). Tots dos treballs feien ús de les idees introduïdes per Riemann l'any 1859. Al llarg dels anys les demostracions originals de Hadamard i De la Vallée-Poussin s'han anat simplificant, fins a l'extrem que actualment existeix una demostració del teorema dels nombres primers d'unes quatre pàgines deguda a Newman, vegeu [23, 24, 37]. Aquestes demostracions tenen en comú que fan servir anàlisi complexa per estudiar la funció ζ de Riemann (al lector interessat en una breu però clara introducció a aquestes qüestions li recomanem l'article de Jordi Quer [25]). Al voltant de 1950, però, Selberg i Erdős van trobar una demostració elemental del teorema dels nombres primers (vegeu per exemple [22]), en el sentit que no fa servir anàlisi complexa. El qualificatiu d'elemental no s'ha de confondre amb el de senzilla (tal com passa amb la demostració original del teorema de Szemerédi).

6.2 El teorema de Green-Tao

Com ja hem dit abans, l'any 2004 Green i Tao van obtenir el resultat següent, publicat el 2008 [15]:

TEOREMA 11 (GREEN, TAO). *Existeixen progressions aritmètiques arbitràriament llargues formades per nombres primers.*

Una de les eines fonamentals en la demostració de Green i Tao és el teorema de Szemerédi (tot i que, com hem vist abans, aquest teorema no es pot aplicar directament al conjunt dels nombres primers). Green i Tao demostren que qualsevol subconjunt dels nombres primers amb densitat superior relativa positiva conté progressions aritmètiques arbitràriament llargues. Dedueixen aquest fet, a través d'un mètode anomenat *principi de transferència*, del teorema de Szemerédi. Un altre ingredient bàsic són uns resultats recents i espectaculars deguts a Goldston, Pintz i Yıldırım sobre la distribució dels nombres primers (vegeu [12, 30]). El lector trobarà a [20] una exposició prou assequible de la demostració de Green i Tao.



Terence Tao *(Adelaide, Austràlia, 1975) és catedràtic de la Universitat de Califòrnia de Los Angeles des de l'edat de vint-i-quatre anys. Als tretze anys va participar per tercer cop a l'Olimpíada Internacional de Matemàtiques, on va obtenir una medalla d'or i va quedar a vuit punts de la puntuació màxima (tots podem tenir un mal dia). Es va doctorar a la Universitat de Princeton, sota la direcció d'Elias Stein. És un matemàtic d'una productivitat extraordinària, amb contribucions excepcionals a l'anàlisi harmònica, la teoria d'equacions en derivades parcials, la combinatòria o la teoria additiva de nombres. Per aquests resultats l'any 2006 va rebre la medalla Fields. És autor d'un bloc de matemàtiques que no em puc estar d'aconsellar:* http://terrytao.wordpress.com/.

Ben Joseph Green *(Bristol, Anglaterra, 1977) va ser estudiant a Cambridge, on també es va doctorar amb una tesi dirigida per W. T. Gowers, després d'un brillant inici de carrera que inclou dues medalles de plata a l'Olimpíada Internacional de Matemàtiques. A part del teorema de Green i Tao, ha obtingut altres resultats, entre els quals una demostració l'any 2003 (obtinguda independentment també per Sapozhenko) de la conjectura de Cameron-Erdős, que afirma que el nombre de subconjunts de* $\{1, \ldots, n\}$ *que no contenen cap terna* x, y, z *que satisfaci* $x + y = z$ *és de l'ordre de* $2^{n/2}$.

Amb aquestes eines Green i Tao van ser capaços de demostrar l'existència de progressions aritmètiques arbitràriament llargues de nombres primers sense haver de demostrar la conjectura d'Erdős i Turán que hem citat a la secció 6.1.

En resultats posteriors Green i Tao han trobat estimacions asimptòticament precises sobre el nombre de progressions aritmètiques formades per nombres primers menors que un cert nombre natural.

El teorema de Green i Tao no és constructiu, en el sentit que no diu com trobar progressions aritmètiques de nombres primers. Buscar progressions aritmètiques de nombres primers, cada cop més llargues, és una de tantes competicions en l'estrany món dels nombres primers. L'eina bàsica, és clar, són els ordinadors. Segons la Viquipèdia, el *rècord* en el moment en què s'estan escrivint aquestes notes és una progressió de longitud 26, trobada el 12 d'abril de 2010 per Benoãt Perichon usant un programa desenvolupat per Jaroslaw Wroblewski i Geoff Reynolds. És aquesta:

$$43142746595714191 + 23681770 \cdot 223092870 \cdot n, \qquad n = 0, 1, \ldots, 25\,.$$

Agraïments

L'autor voldria agrair als editors del *Butlletí* de la Societat Catalana de Matemàtiques el seu interès en la publicació d'aquest text, així com als professors Jorge Jiménez, Josep Pla i Artur Travessa per un bon nombre de suggeriments i correccions que han contribuït a millorar el text. També voldria agrair al revisor d'aquest article amb vista a la seva publicació al *Butlletí* els nombrosos i detallats comentaris que han ajudat a millorar aquest text.

Referències

[1] Apostol, T. M. *Introduction to analytic number theory*. Nova York; Heidelberg: Springer-Verlag, 1976. (Undergraduate Texts in Mathematics)

[2] Berlekamp, E. R. «A construction for partitions which avoid long arithmetic progressions». *Canad. Math. Bull.*, 11 (1968), 409–414.

[3] Corput, J. G. van der «Über Summen von Primzahlen und Primzahlquadraten». *Math. Ann.*, 116 (1939), 1–50.

[4] Erdős, P. *The art of counting. Selected writings*. Editat per Joel Spencer i una dedicatòria de Richard Rado. Cambridge, Mass.: The MIT Press, 1973. (Mathematicians of our time; vol. 5)

[5] Erdős, P.; Szekeres, G. «A combinatorial problem in geometry». *Compos. Math.*, 2 (1935), 463–470.

[6] Erdős, P.; Turán, P. «On some sequences of integers». *J. Lond. Math. Soc.*, 11 (1936), 261–264.

[7] Furstenberg, H. «On the infinitude of primes». *Amer. Math. Monthly*, 62 (1955), 353.

[8] Furstenberg, H. «Ergodic behaviour of diagonal measures and a theorem of Szemerédi on arithmetic progressions». *J. Anal. Math.*, 31 (1977), 204–256.

[9] FURSTENBERG, H. *Recurrence in ergodic theory and combinatorial number theory*. Princeton, N. J.: Princeton University Press, 1981.

[10] FURSTENBERG, H.; KATZNELSON, Y.; ORNSTEIN, D. «The ergodic theoretical proof of Szemerédi's theorem». *Bull. Amer. Math. Soc.*, 7 (1982), 527–552.

[11] GOWERS, W. T. «A new proof of Szemerédi's theorem». *Geom. Funct. Anal.*, 11 (3) (2001), 465–588.

[12] GOLDSTON, D. A.; PINTZ, J.; YILDIRIM, C. Y. «Primes in tuples I». *Ann. of Math. (2)*, 170 (2) (2009), 819–862.

[13] GRAHAM, R. «Some of my favorite problems in Ramsey theory». *Integers*, 7 (2) (2007), A15.

[14] GRAHAM, R.; ROTHSCHILD, B.; SPENCER, J. H. *Ramsey Theory*. Nova York: John Wiley and Sons, 1990.

[15] GREEN, B.; TAO, T. «The primes contain arbitrarily long arithmetic progressions». *Ann. of Math. (2)*, 167 (2) (2008), 481–547.

[16] GREEN, B.; TAO, T. «Yet another proof of Szemeredi's theorem». *Preprint*, arXiv:1002.2254.

[17] GREEN, B.; WOLF, J. «A note on Elkin's improvement of Behrend's construction». Preprint, arXiv:0810.0732.

[18] HARDY, G. H.; LITTLEWOOD, J. E. «Some problems of 'partitio numerorum'; III: On the expression of a number as a sum of primes». *Acta Math.*, 44 (1923), 1–70.

[19] KHINCHIN, A. Y. *Three pearls of number theory*. Reimpressió de la traducció del rus de 1952. Mineola: Dover Publications, 1998.

[20] KLAZAR, M. «Progressions aritmètiques de nombres primers». *Butll. SCM*, 21 (2) (2006), 229–245.

[21] NAGLE, B.; RÖDL, V.; SCHACHT, M. «The counting lemma for regular k-uniform hypergraphs». *Random Structures Algorithms*, 28 (2) (2006), 113–179.

[22] NATHANSON, M. B. *Elementary methods in number theory*. Nova York: Springer, 2000. (Graduate Texts in Mathematics; 195)

[23] NEWMAN, D. J. «Simple analytic proof of the prime number theorem». *Amer. Math. Monthly*, 87 (1980), 693–696.

[24] NEWMAN, D. J. *Analytic number theory*. Nova York: Springer-Verlag, 1998. (Graduate Texts in Mathematics; 177)

[25] QUER, J. «La funció ζ de Riemann». *Butll. SCM*, 22 (2) (2007), 197–228.

[26] RAMSEY, F. P. «On a problem of formal logic». *Proc. Lond. Math. Soc. Series*, 30 (1930), 264–286.

[27] ROTH, K. F. «On certain sets of integers, I». *J. Lond. Math. Soc.*, 28 (1953), 104–109; errata, *ibid.* 29 (1953), 20–26.

[28] ROTH, K. F. «Irregularities of sequences relative to arithmetic progressions, IV». *Period. Math. Hungar.*, 2 (1972), 301–326.

[29] SANDERS, T. «On Roth's theorem on progressions». *Preprint* arXiv: 1011.0104v1.

[30] SOUNDARARAJAN, K. «Small gaps between prime numbers: the work of Goldston-Pintz-Yıldırım». *Bull. Amer. Math. Soc.*, 44 (2007), 1–18.

[31] SZEMERÉDI, E. «On sets of integers containing no k elements in arithmetic progression». *Acta Arith.*, 27 (1975), 199–245.

[32] TAO, T. «The ergodic and combinatorial approaches to Szemerédi's theorem». A: *Additive combinatorics*. Providence, R. I.: Amer. Math. Soc., 2007. (CRM Proceedings & Lecture Notes; 43.), 145–193.

[33] TAO, T.; VU, V. H. *Additive combinatorics*. Cambridge: Cambridge University Press, 2010. (Cambridge Studies in Advanced Mathematics; 105)

[34] VAN DER WAERDEN, B. L. «Beweis einer Baudetschen Vermutung». *Nieuw. Arch. Wisk.*, 15 (1927), 212–216.

[35] WAERDEN, B. L. VAN DER «How the proof of Baudet's conjecture was found». A: *Studies in Pure Mathematics (Presented to Richard Rado)*. Londres: Academic Press, 1971, 251–260.

[36] WAERDEN, B. L. VAN DER *Algebra I and II (Based in part on lectures by E. Artin and E. Noether)*. Nova York: Springer-Verlag, 1991.

[37] ZAGIER, D. «Newman's short proof of the prime number theorem». *Amer. Math. Monthly*, 104 (1997), 705–708.

DEPARTAMENT D'ÀLGEBRA I GEOMETRIA
UNIVERSITAT DE BARCELONA
GRAN VIA DE LES CORTS CATALANES, 585, 08007 BARCELONA
ignasi.mundet@ub.edu