El diablo de los números

Sección a cargo de

Fernando Chamizo Lorente

Un teorema de Javier Cilleruelo

por

Fernando Chamizo

1. Unas palabras sobre Javier

Durante muchos años, Javier Cilleruelo estuvo a cargo de esta sección de La Gaceta. Es obligado, por tanto, recordarle ahora cuando tristemente nos ha golpeado su reciente fallecimiento. La mejor manera de hacerlo que se me ocurre es a través de uno de sus resultados. Quizá extrañe al lector que haya escogido una contribución menor dentro de su producción. La razón para ello es que, a mi entender, refleja bien sus gustos y métodos, además de ajustarse bien al formato de esta sección tal como él la concebía.

Según he sabido, y es de justicia, este número de La Gaceta dedica algunos panegíricos a Javier. Mi tributo es fundamentalmente científico, dejando a otros con mejor plectro que hagan aquella difícil tarea. Sin embargo, me gustaría completar esta sección con algunos comentarios más personales.

Javier se dedicaba especialmente, casi exclusivamente, a la teoría elemental de números. Una aclaración obligada siempre que se menciona esta área, posiblemente innecesaria en este ámbito, es que «elemental» no significa aquí «sencilla», sino que utiliza técnicas elementales. Por mencionar un ejemplo conocido, la prueba original [23] del famoso teorema de Szemerédi (las sucesiones con densidad positiva en los naturales contienen progresiones aritméticas arbitrariamente largas) es elemental, en este sentido, pero nadie en su sano juicio diría que es sencilla. Creo que él pensaba que algunos de sus colegas caían en esta confusión entre elemental y sencillo, pero nunca le oí mayores quejas sobre ello. Espero que el carácter simple de esta nota no incida en el equívoco.

De las cualidades científicas de Javier, la que más me impresionaba es que era un torrente de creatividad. Parecía que cada semana tenía una idea nueva ¡y encima funcionaba! Contradiciendo los bien conocidos y discutibles augurios de G. H. Hardy [18]

(cf. [21]), esta facultad no fue decayendo, sino bien al contrario. Impulsado por el perfeccionamiento de sus métodos y por las colaboraciones internacionales que propiciaban la importancia de sus trabajos, su creatividad y productividad fueron creciendo con el tiempo.

Javier tenía una curiosidad genuina por las Matemáticas en general, pero en lo relativo a su formación e investigación mantenía una postura que a mí me parecía herética (y contraria a las recomendaciones de grandes matemáticos contemporáneos, [17]) que se sintetiza en que prefería, según sus propias palabras, aprender las cosas cuando le aparecieran en los problemas. El hecho es que esta actitud le llevó incomparablemente más lejos que a la mayoría de los que seguimos a su alrededor una política totalmente opuesta. Posiblemente su elección optimizaba la efectividad que le daba su enorme creatividad. Hay un rasgo significativo en el perfil de Javier que quizá guiara sus preferencias: le gustaba contar las cosas que hacía. Era buen orador y todavía mejor escribiendo, pero aquí me refiero más a la pequeña tertulia o conversación de café entre compañeros que a la comunicación científica. En ese ámbito, no sólo hay que tener cosas que contar, de las cuales tenía muchas, sino también susceptibles de ser comunicadas sin exigir a la casual audiencia grandes conocimientos previos. Un área con un lenguaje propio y extenso o que se embelesara con la belleza rococó de la abstracción, habría limitado las dotes comunicativas a corta distancia de Javier.

Respecto al contenido de esta nota, un día Javier me dijo que se le había ocurrido una idea para englobar varios resultados aparentemente bien distintos. Al cabo de unos días me pasó un *preprint*. Después de bastante tiempo me dijo que, entrando en comunicación con G. Tenenbaum, supo que había tenido algunas ideas similares y decidieron escribir un trabajo conjunto [13], que reproduce aplicaciones del *preprint* que yo vi. En las siguientes líneas trataré dos de ellas que me servirán para comentar algunas contribuciones de Javier. En el original hay más aplicaciones, todas ellas con un sabor combinatorio, incluyendo una a la teoría de grafos y otra a la teoría de códigos. Lo relevante no son los enunciados, que ya eran conocidos, sino su derivación de un principio sencillo y común de una forma elegante.

2. Acotando el solapamiento

Si dos sucesos A y B tiene probabilidades «grandes», está claro que se deben solapar, en el sentido de que la probabilidad de $A \cap B$ es no nula. La cota para esta probabilidad $P(A \cap B)$ en términos de $P(A) + P(B)$ es muy sencilla:

$$P(A \cap B) = P(A) + P(B) - P(A \cup B) \geq P(A) + P(B) - 1. \tag{1}$$

Claramente esta cota inferior es óptima, siempre que no sea trivial.

Uno puede preguntarse por la generalización a más sucesos, considerando la suma de las probabilidades de los solapamientos. Para evitar las quejas de los más exigentes con el rigor y para tranquilidad del resto, supongamos que el espacio de probabilidad es $(\Omega, 2^{\Omega}, P)$ con Ω finito. El objetivo es acotar cardinales, casos favorables y posibles, más que probabilidades de las difíciles. Dados sucesos E_1, E_2,..., E_k y $\omega \in \Omega$, se

tiene

$$\sum_{1\le i<j\le k} \mathbb{I}_{E_i}(\omega)\mathbb{I}_{E_j}(\omega) = \binom{\#\{j\,:\,\omega\in E_j\}}{2}.$$

Esta identidad, donde $\mathbb{I}_E$ es la función indicadora, es prácticamente obvia. Cuenta de dos maneras diferentes los sucesos a los que pertenece ω. Calculando la esperanza, se obtiene

$$\sum_{1\le i<j\le k} P(E_i\cap E_j) \ge \binom{\sum_{\omega\in\Omega} P(\{\omega\})\#\{j\,:\,\omega\in E_j\}}{2}.$$

Para la desigualdad se ha usado la convexidad de $\binom{x}{2}$, que se ha identificado con la función $x(x-1)/2$. En definitiva, tenemos el teorema de solapamiento:

$$\boxed{\sum_{1\le i<j\le k} P(E_i\cap E_j) \ge \frac{\sum_j P(E_j)}{2}\Big(\sum_j P(E_j)-1\Big).} \tag{2}$$

¿Por qué recuadramos esto? Es simple y para $k=2$ más débil que (1).

Antes de dar uso a (2), diremos que en [13] se prueba una generalización óptima de este resultado. Concretamente, lo que se escribe allí como resultado principal (aunque lo importante del artículo es el ingenio al emplearlo en las aplicaciones) es el siguiente enunciado:

Teorema. *En cualquier espacio de probabilidad* $(\Omega,\mathcal{A},P)$*, se tiene*

$$\sum_{1\le j_1<\ldots<j_m\le k} P(E_{j_1}\cap\cdots\cap E_{j_m}) \ge Q_m\Big(\sum_j P(E_j)\Big), \tag{3}$$

donde $Q_m(x)$ *es la función que interpola linealmente* $\binom{n}{m}$ *y* $\binom{n+1}{m}$ *para* $n\le x<n+1$.

Nótese que cuando $m=k=2$ se recupera (1). La demostración para $m=2$ sigue los pasos que conducen a (2), simplemente observando que la convexidad de Q_m asegura $Q_m\big(E[X]\big)\le E\big[Q_m(X)\big]$, donde $E[\,\cdot\,]$ indica la esperanza. Para $m>2$, la prueba es tan parecida que sería aburrir al lector incluirla aquí.

3. Dos resultados, dos retos

A menudo se dice que la teoría de números es «difícil» porque hay problemas con enunciado muy sencillo y solución muy complicada (¿hay que recordar a alguien el Último Teorema de Fermat?). A mi juicio, su presunta dificultad está mejor representada por la existencia de problemas con enunciado sencillo y solución sencilla pero difícil de encontrar. Por alguna razón no es nada fácil desarrollar una intuición acerca de los números que permita llegar a soluciones que están al alcance de la mano.

Si todavía alguien duda de que la teoría elemental de números no es ninguna trivialidad, que considere los siguientes problemas. Si los resuelve, sin duda, tiene grandes aptitudes aritméticas. Para el resto de los lectores, serán teoremas en lugar de problemas, que probaremos de una manera breve a partir de (2).

Problema 1. Sea $A \subset \{1, 2, \ldots, N\}$ tal que las sumas de cada dos de sus elementos $a + a'$, $a \le a'$, son distintas (es un conjunto de Sidon). Demostrar que $|A| \le N^{1/2} + N^{1/4} + 1$.

Problema 2. Probar que en la circunferencia $x^2 + y^2 = R^2$, un arco de longitud $R^{1/2-\gamma_k}$, con $\gamma_k^{-1} = 4\lfloor k/2 \rfloor + 2$, contiene a lo más k puntos de coordenadas enteras.

4. Conjuntos de Sidon y generalizaciones

Solución del problema 1. Sea n el entero definido por

$$\sqrt{|A|N} < n \le 1 + \sqrt{|A|N}. \tag{4}$$

Para $1 \le j \le n$, tomemos $E_j = A + j$ con el significado obvio y consideremos la distribución uniforme en $\bigcup E_j$. Es decir, si s es el cardinal de este conjunto, cada elemento tiene probabilidad s^{-1}. Así pues, $\sum P(E_j) = |A|ns^{-1}$. Por otro lado, si $x_1, x_2 \in E_{j_1} \cap E_{j_2}$, entonces $x_1 = a_1 + j_1 = a_1' + j_2$ y $x_2 = a_2 + j_1 = a_2' + j_2$, de donde $a_1 + a_2 = a_1' + a_2'$. Por consiguiente $P\big(E_{j_1} \cap E_{j_2}\big) \le s^{-1}$ y (2) implica

$$\frac{1}{2}n(n-1)s^{-1} \ge \sum_{1 \le j_1 < j_2 \le n} P\big(E_{j_1} \cap E_{j_2}\big) \ge \frac{1}{2}|A|ns^{-1}\big(|A|ns^{-1} - 1\big).$$

Por tanto,

$$s \ge \frac{|A|^2 n}{|A| + n - 1} \quad \text{y, por (4),} \quad s \ge \frac{|A|^2\sqrt{N}}{\sqrt{|A|} + \sqrt{N}}.$$

Obviamente, $s \le N + \sqrt{|A|N}$, ya que $\bigcup E_j \subset \{2, 3, \ldots, N + n\}$. De aquí se concluye

$$|A| \le \Big(\sqrt{\sqrt{N} + 1/4} + 1/2\Big)^2 \le N^{1/2} + N^{1/4} + 1. \qquad \square$$

El problema 1 es un resultado de B. Lindström [19]. Quizá el lector se sienta un poco decepcionado al saber que la bella prueba original es también muy breve y elemental. La presentada aquí tiene la ventaja de que implica un resultado sobre conjuntos de Sidon de interés independiente (véase [13]) y, por supuesto, que ilustra la versatilidad del teorema de solapamiento. Una primera impresión tras estas pruebas, y alguna otra, es que la cota se puede mejorar con un análisis más fino. Pues bien, después de tantos años, nadie ha tenido éxito más allá de cambiar $+1$ por $+1/2$. P. Erdős creyó inicialmente que debería existir una cota del tipo $N^{1/2} + C$ para cierta constante C (al parecer, incluso ofreció una de sus famosas recompensas pecuniarias por ello); sin embargo, más adelante cambió de opinión y pensó que la conjetura correcta requeriría reemplazar C por alguna otra función que creciera menos que cualquier potencia positiva de N.

Javier era un reconocido experto en conjuntos de Sidon y sus generalizaciones $B_h[g]$, conjuntos de números naturales $\{a_1, \ldots, a_n\}$ tales que para cada N la ecuación $a_{i_1} + \cdots + a_{i_h} = N$ tiene a lo más g soluciones con $a_{i_1} \le \cdots \le a_{i_h}$. De esta forma, los conjuntos de Sidon son $B_2[1]$. Siempre se pueden construir conjuntos

$B_h[g]$ considerando enteros cada vez más espaciados. Por ejemplo, las potencias de dos forman un conjunto de Sidon. La cuestión fundamental en la teoría es saber cómo de denso puede ser un conjunto $B_h[g]$. El problema tiene dos variantes, dependiendo de si se consideran conjuntos infinitos o no. En ambos Javier hizo contribuciones de primera magnitud. Una buena recomendación para el lector ávido de información sobre estos temas es el artículo que escribió hace unos años para esta sección [4].

Definamos $\beta_g(N)$ como el máximo cardinal de un subconjunto de $\{1, 2, \ldots, N\}$ de modo que un entero tenga a lo más g representaciones como suma de dos de sus elementos. Se conoce que $\lim \beta_2(N)/\sqrt{N} = 1$, por tanto los conjuntos de Sidon más grandes que se pueden construir tienen asintóticamente $\sqrt{N}$ elementos. Se sabe algo similar para $\beta_3(N)$ pero no más allá. Posiblemente el trabajo que más fama dio a Javier fue [12] (escrito en colaboración con I. Ruzsa y C. Vinuesa), cuyo resultado principal es

$$\lim_{g\to\infty} \liminf_{N\to\infty} \frac{\beta_g(N)}{\sqrt{gN}} = \lim_{g\to\infty} \limsup_{N\to\infty} \frac{\beta_g(N)}{\sqrt{gN}};$$

además, estos límites coinciden con $\sup \int_0^1 f$, donde el supremo es sobre las funciones $f \geq 0$ soportadas en $[0, 1]$ cuya autoconvolución satisface $(f * f)(x) \leq 1$. La aparición aquí de estos objetos analíticos no es nada obvia (véase [20]).

En [14] y [11] se dan acotaciones antes de tomar límites en g.

Cuando los conjuntos que se consideran son infinitos, para medir lo densos que son es natural introducir la función contadora $A(N)$ que dice cuántos elementos del conjunto están en $\{1, 2, \ldots, N\}$. El conjunto, que podemos ver como una sucesión, es más denso cuanto mayor sea esta función. Es importante notar que hay una diferencia con el caso finito: allí elegíamos el conjunto una vez fijado N, lo cual da mayor libertad. Se cree, no obstante, que se pueden construir conjuntos de Sidon infinitos casi tan buenos como los finitos, en el sentido de que $A(N) > C_\epsilon N^{1/2-\epsilon}$ para cada $\epsilon > 0$. Hay una construcción simple [4, § 2.1] que lleva a $A(N) > CN^{1/3}$. El exponente $1/3$ permaneció imbatido más de 50 años hasta que Ruzsa consiguió probar en [22] que existe un conjunto de Sidon con $A(N) > C_\epsilon N^{\sqrt{2}-1-\epsilon}$. Javier logró en [5] dar una prueba constructiva (y más sencilla) de este resultado y, en general, demostró que existen conjuntos $B_h[1]$ infinitos tales que $A(N) > C_\epsilon N^{\sqrt{(h-1)^2+1}-h+1-\epsilon}$.

5. Puntos en arcos de circunferencia

Solución del problema 2. Si la circunferencia $x^2 + y^2 = R^2$ contiene puntos de $\mathbb{Z}^2$, obviamente R^2 es entero. Su factorización en primos gaussianos será de la forma

$$R^2 = \prod_{l=1}^{L} \pi_l^{m_l} \bar{\pi}_l^{m_l} \qquad \text{con } \pi_1, \ldots, \pi_L \text{ primos no asociados.}$$

Supongamos que en un arco de longitud $R^{1/2-\gamma}$ hubiera $k+1$ puntos determinados por enteros gaussianos $z_1, \ldots, z_{k+1}$. Necesariamente $z_j = \prod \pi_l^{a_{jl}} \bar{\pi}_l^{m_l - a_{jl}}$, salvo

unidades, con $0 \le a_{jl} \le m_l$ porque ésta es la única forma de tener $z_j \bar{z}_j = R^2$. Definamos

$$E_j = \{\pi_l^{a_{jl}} \,:\, 1 \le l \le L\} \cup \{\bar{\pi}_l^{m_l - a_{jl}} \,:\, 1 \le l \le L\}$$

y asignemos a cada potencia ($\neq 1$) de π_l y de $\bar{\pi}_l$ la probabilidad $\log|\pi_l| / \log(R^2)$. Es sencillo ver que esto define una medida de probabilidad en $\bigcup E_j$. Se tiene

$$P(E_j) = \sum_{l=1}^{L} \frac{a_{jl} \log|\pi_l| + (m_l - a_{jl}) \log|\pi_l|}{\log(R^2)} = \frac{1}{2}.$$

Por otro lado,

$$P(E_i \cap E_j) = \frac{\log\big|\mathrm{mcd}(z_i, z_j)\big|}{\log(R^2)} \le \frac{\log\big|z_i - z_j\big|}{\log(R^2)} < \frac{R^{1/2-\gamma}}{\log(R^2)} = \frac{1}{2}\Big(\frac{1}{2} - \gamma\Big).$$

Así pues, (2) implica

$$\frac{(k+1)k}{2} \cdot \frac{1}{2}\Big(\frac{1}{2} - \gamma\Big) > \frac{k+1}{4}\Big(\frac{k+1}{2} - 1\Big).$$

Por tanto, $\gamma^{-1} > 2k$, que es $4\lfloor k/2 \rfloor + 2$ cuando k es impar. Se deja al lector comprobar que (3) con $m = 2$ permite deducir el caso par. □

El problema 2 es uno de los primeros resultados de Javier, uno de los teoremas de su tesis doctoral, con lo cual le tenía mucho aprecio y dedicó bastante esfuerzo a encontrar mejoras, lo que resultó más difícil de lo esperado.

Es interesante decir algunas palabras acerca del contexto del que surgió el problema y de sus ramificaciones actuales. El origen está en el director de tesis de Javier, A. Córdoba, quien, como analista armónico educado en la escuela de Chicago, conocía de primera mano los lemas de Cantor-Lebesgue de R. Cooke [15] y de A. Zygmund [24], cuyas pruebas involucraban algunas propiedades de puntos de coordenadas enteras en circunferencias. De hecho, Zygmund emplea en su artículo el caso $k = 3$, que es más sencillo (y que Zygmund atribuye a A. Schinzel). Por otro lado, los teoremas de restricción de la transformada de Fourier a curvas estrictamente convexas [16], sugieren análogos para series de Fourier que requerirían que, para cada $\epsilon > 0$, el número de puntos de coordenadas enteras en arcos de longitud $R^{1-\epsilon}$ estuviera acotado uniformemente en R. El problema 2 prueba esta propiedad para arcos de longitud $R^{1/2-\epsilon}$.

Javier no creía que el resultado fuera óptimo, y para él constituyó una sorpresa cuando encontró una sucesión exponencial de radios tales que había 4 puntos en arcos de longitud $CR^{1/3}$ con C cierta constante [8]. Por otro lado, es posible dar sucesiones polinómicas si uno sólo quiere tres puntos [3] y al incrementar k la cadencia *polinómico* → *exponencial* → *nada* suena bien (¿alguna relación con puntos racionales en curvas de géneros $g = 0$, $g = 1$, $g > 1$?), pero a día de hoy el exponente $1/2 - \gamma_k$ no se ha mejorado ni un ápice. Dicho sea de paso, Javier generalizó la situación a otras cónicas [7], [9], [10].

Curiosamente, este problema que vino motivado por el análisis armónico y que Javier estudió como problema de teoría de números, pasados veinte años, ha gozado de un reciente resurgimiento gracias a las citas en trabajos de análisis armónico de J. Bourgain y Z. Rudnick (véase, por ejemplo, [1] y [2]). Resulta que el estudio de las regiones nodales y de las normas de autofunciones en toros planos está ligado a puntos de coordenadas enteras en arcos. Esto último no es tan sorprendente releyendo el original [6] (e incluso [24] y más claramente en [8]), pues parte de la presentación es cambiar una norma cuatro por una norma dos gracias a la estimación de puntos en arcos.

La reciente fama del problema 2 ha propiciado que varios matemáticos, algunos de primerísimo nivel, hayan pensado sobre él. Persiste sin embargo la pregunta de si puede reducirse el exponente y entonces, indudablemente, esta cuestión debería calificarse como difícil. ¿Admite una solución elemental? Estoy seguro de que a Javier le hubiera gustado que fuera así.

Referencias

[1] J. Bourgain y Z. Rudnick, Nodal intersections and L^p restriction theorems on the torus, *Israel J. Math.* **207** (2015), no. 1, 479–505.

[2] J. Bourgain y Z. Rudnick, Restriction of toral eigenfunctions to hypersurfaces and nodal sets, *Geom. Funct. Anal.* **22** (2012), no. 4, 878–937.

[3] J. Cilleruelo, Arcs containing no three lattice points, *Acta Arith.* **59** (1991), no. 1, 87–90.

[4] J. Cilleruelo, Conjuntos de enteros con todas las diferencias distintas, *La Gaceta de la RSME* **11** (2008), no. 1, 151–170.

[5] J. Cilleruelo, Infinite Sidon sequences, *Adv. Math.* **255** (2014), 474–486.

[6] J. Cilleruelo y A. Córdoba, Trigonometric polynomials and lattice points, *Proc. Amer. Math. Soc.* **115** (1992), no. 4, 899–905.

[7] J. Cilleruelo y A. Córdoba, Lattice points on ellipses, *Duke Math. J.* **76** (1994), no. 3, 741–750.

[8] J. Cilleruelo y A. Granville, Lattice points on circles, squares in arithmetic progressions and sumsets of squares, *Additive combinatorics*, 241–262, CRM Proc. Lecture Notes, 43, Amer. Math. Soc., Providence, RI, 2007.

[9] J. Cilleruelo y J. Jiménez-Urroz, Lattice points on hyperbolas, *J. Number Theory* **63** (1997), no. 2, 267–274.

[10] J. Cilleruelo y J. Jiménez-Urroz, Divisors in a Dedekind domain, *Acta Arith.* **85** (1998), no. 3, 229–233.

[11] J. Cilleruelo, I. Z. Ruzsa y C. Trujillo, Upper and lower bounds for finite $B_h[g]$ sequences, *J. Number Theory* **97** (2002), no. 1, 26–34.

[12] J. Cilleruelo, I. Ruzsa y C. Vinuesa, Generalized Sidon sets, *Adv. Math.* **225** (2010), no. 5, 2786–2807.

[13] J. Cilleruelo y G. Tenenbaum, An overlapping theorem with applications, *Publ. Mat.*, vol. extra (2007), Proceedings of the Primeras Jornadas de Teoría de Números, 107–118.

[14] J. Cilleruelo y C. Vinuesa, $B_2[g]$ sets and a conjecture of Schinzel and Schmidt, *Combin. Probab. Comput.* **17** (2008), no. 6, 741–747.

[15] R. Cooke, A Cantor-Lebesgue theorem in two dimensions, *Proc. Amer. Math. Soc.* **30** (1971), 547–550.

[16] K. M. Davis y Y.-C. Chang, *Lectures on Bochner-Riesz means*, London Mathematical Society Lecture Note Series, 114, Cambridge Univ. Press, Cambridge, 1987.

[17] T. Gowers, J. Barrow-Green y I. Leader (editores), *The Princeton companion to mathematics*, Princeton Univ. Press, Princeton, NJ, 2008.

[18] G. H. Hardy, *A mathematician's apology*, reimpresión de la edición de 1967, Cambridge Univ. Press, Cambridge, 1992.

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

[20] G. Martin y K. O'Bryant, The supremum of autoconvolutions, with applications to additive number theory, *Illinois J. Math.* **53** (2009), no. 1, 219–235.

[21] L. J. Mordell, Hardy's "A Mathematician's Apology", *Amer. Math. Monthly* **77** (1970), no. 8, 831–836.

[22] I. Z. Ruzsa, An infinite Sidon sequence, *J. Number Theory* **68** (1998), no. 1, 63–71.

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

[24] A. Zygmund, A Cantor-Lebesgue theorem for double trigonometric series, *Studia Math.* **43** (1972), 173–178.

Fernando Chamizo, Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049 Madrid

Correo electrónico: fernando.chamizo@uam.es