Javier Cilleruelo: el arte de contar

por

Antonio Córdoba

Javier Cilleruelo (Soria 1961–Madrid 2016), o Francisco Javier Cilleruelo Mateo si escribimos su nombre completo, ha tenido una vida relativamente corta para estos tiempos que corren, pero creo que ha sido una vida buena y fructífera. Su actividad profesional ha girado en torno a la Universidad Autónoma de Madrid y al Instituto de Ciencias Matemáticas, que fueron las bases desde las que supo mantener una brillante proyección internacional.

Además de tres monografías sobre diversos aspectos de la Teoría de los Números, Javier ha publicado alrededor de ochenta artículos de investigación, y su producción ha ido *in crescendo* con el paso del tiempo. Incluso durante el último y duro año de su enfermedad ha llevado a cabo, entre otros, un trabajo en colaboración con los dos Fernández, José Luis y Pablo, acerca de los puntos visibles del retículo (mezclando dos de sus temas favoritos: la teoría de los números y la probabilidad [9]), y esa otra filigrana matemática que es su resultado con Florian Luca ([11]): todo entero positivo es la suma de tres capicúas.

Es tradicional, en estas circunstancias, poner de manifiesto las situaciones y las anécdotas compartidas. En mi caso son tantas que sería excesivo mencionarlas, pero sí quiero decir que me siento orgulloso de haber dirigido su tesis doctoral y colaborado en artículos, libros y proyectos de investigación. Desde que empezó conmigo su tesina de licenciatura, allá por 1984, hasta sus últimos momentos, hemos mantenido una conversación frecuente, casi diaria, en torno a todas las aventuras matemáticas a las que su privilegiada mente lo ha ido llevando. Tanto en las que hemos sido colaboradores como también en todas las demás, por cuanto a él le satisfacía tenerme al día de lo que estaba investigando en cada momento y yo disfrutaba con ello. En ocasiones me contaba con orgullo los progresos de su hijo Carlos, y sé también de lo afortunado que se consideraba por tener a su lado a Estrella, su esposa. Pero Javier no era una persona a quien le gustara mucho hablar de sí mismo, y aunque pueda parecer algo extraño dada nuestra prolongada amistad, no conozco demasiados detalles de su vida, y fue a través de otros miembros de su familia que supe de la gran tragedia que marcó su más tierna infancia: el fallecimiento de su padre en un accidente de tráfico cuando realizaba el trayecto Aranda de Duero–Valladolid.

Apenas le interesaban, por aburridos, los trajines de la vida académica, pero su semblante se transformaba cuando el tema de conversación giraba en torno a problemas aritméticos y combinatorios. Quienes le tratamos con asiduidad echaremos de menos, sobre todo, su amistad, pero también las conversaciones frecuentes, alrededor de un café, en las que sus ojos brillaban contándonos la nueva observación sobre los números que acababa de hacer y que tanto le alegraba. Aparte de su talento matemático, especialmente dotado para la matemática discreta, teoría de números, grafos y combinatoria, Javier poseía el don de la música. No solo tocaba bien la guitarra, sino que era capaz de reconstruir enseguida las notas de una partitura después de haber escuchado su interpretación.

Javier pertenecía a la promoción de la UAM que inició sus estudios de licenciatura allá por 1979, que fue precisamente el año en el que yo tomé posesión, como solía decirse entonces, de la cátedra de Análisis Matemático. Por exigencias del guion, según una frase que se hizo popular en aquellos tiempos de la movida, enseguida me convertí en una especie de profesor orquesta que impartía clases de álgebra, geometría diferencial, probabilidad, teoría de números e, incluso, de análisis matemático. Le tuve pues de alumno en diversas asignaturas y recuerdo muy bien que cuando el asunto iba de modelos de la física o de la geometría, el interés y las calificaciones de Javier palidecían un poco, pero en cuanto se trataba de temas aritméticos o combinatorios ahí aparecía siempre con soluciones muy originales, de Matrícula de Honor.

A finales del verano de 1983, un año antes de licenciarse, se matriculó en un curso de Teoría de Números que impartí en Jarandilla de la Vera, dentro del programa organizado por Miguel de Guzmán y Carlos Benítez. Creo que ese curso fue para él una especie de epifanía, de manera que, a la vuelta del año sabático que disfruté entonces en la Universidad de Chicago, me pidió ser su director de tesis doctoral en torno a esos problemas aritméticos que tanto le habían interesado en mi curso.

Por orden cronológico es el sexto de mis alumnos de doctorado en Madrid. Su tesis fue, sin embargo, la primera que dirigí en Teoría de Números, pero sobre cuestiones que provenían mayormente de mi experiencia con las series e integrales de Fourier. En los años de mi doctorado en Chicago, y bajo la influencia de A. Zygmund, conocí la obra aritmética de Hardy, Littlewood y Ramanujan (el método del círculo y la importancia de las sumas trigonométricas en la teoría de los números), que me inspiró muchos problemas interesantes para investigar. Así es que a Javier le sugerí estudiar a fondo las monografías de H. Davenport (*Multiplicative number theory*) y H. Halberstam y K. Roth (*Sequences*), y redactar una tesina sobre el problema de estimar los puntos del retículo dentro de círculos, a partir de los artículos pioneros de Hardy y Littlewood, y de las ideas que yo había introducido en el tratamiento de los operadores llamados de sumación esférica de series de Fourier dobles. El resultado fue un interesante documento que no solo mostraba el dominio de esas técnicas, sino que también presentaba varias mejoras sobre las fórmulas aproximadas del llamado término de error, obtenidas por Hardy y Littlewood. Esa tesina, escrita a mano con una letra muy clara, es también una muestra fehaciente del enorme progreso que la escritura de las Matemáticas ha experimentado en las últimas décadas.

Javier era, creo yo, bastante inmune a los achaques del ego. A lo largo de mi carrera universitaria he tenido que soportar muchas situaciones tediosas, protagonizadas por personajes que creen haber sido ungidos por los dioses y alcanzado una notoriedad que tiene que ser constantemente reconocida por los demás. Ese trajín con el nombre que afecta a quienes gastan sus energías en hacerse notar. Si he podido salir incólume, o al menos no sufrir demasiados estragos, ha sido gracias al apoyo de un grupo de buenos amigos, entre los cuales el de Javier fue para mí especialmente importante, y ahora lo echaré mucho de menos. Aunque no me resulta nada fácil hacerlo sin que se me quiebre la escritura, a continuación, y de acuerdo con lo que me han pedido los directores de La Gaceta, voy a comentar brevemente algunos resultados que publicó en los temas desarrollados bajo mi influencia, con la pretensión, quizás exagerada, de ayudar a comprender su trayectoria matemática.

1. Contando puntos del retículo

Contar los puntos de coordenadas enteras dentro de un conjunto, o de una familia de conjuntos, es un asunto que aparece con frecuencia en muchas teorías interesantes. Un ejemplo es la función $r_2(n)$, que cuenta el número de representaciones del entero n como suma de dos cuadrados; es decir, el cardinal del conjunto de puntos del retículo unidad que están en la circunferencia de radio igual a la raíz cuadrada de n y centrada en el origen de coordenadas. Enseguida se ve que va tomando valores de forma poco regular: $r_2(1) = r_2(2) = r_2(4) = 4$, $r_2(3) = r_2(6) = r_2(7) = 0$, $r(5) = 8, \ldots$

No obstante, a partir de la descomposición en factores primos de n podemos calcular el valor de $r_2(n)$ con una fórmula explícita, que encuentra su explicación más transparente dentro de la teoría de divisibilidad del anillo $\mathbb{Z}[i]$ de los enteros de Gauss. Dice así: si

$$n = 2^\alpha \prod_{p_j \equiv 1\,(4)} p_j^{\beta_j} \prod_{q_i \equiv 3\,(4)} q_i^{\gamma_i},$$

entonces

$$r_2(n) = \begin{cases} 4\prod_j (1+\beta_j) & \text{si } \gamma_i \text{ es par para todo } i, \\ 0 & \text{en caso contrario.} \end{cases}$$

De esta fórmula resulta fácil deducir las siguientes consecuencias:

$$r_2(n) = O(n^\varepsilon) \quad \text{para todo } \varepsilon > 0,$$

$$\limsup_{n\to\infty} \frac{r_2(n)}{(\log(n))^p} = \infty \quad \text{para todo } p.$$

Es decir, asintóticamente, el número de puntos del retículo en la circunferencia $x^2 + y^2 = n$ es menor que cualquier potencia positiva del radio, pero puede ser mayor que cualquier potencia de su logaritmo.

Cabe también preguntarse acerca de la distribución de los puntos reticulares en arcos de esas circunferencias centradas en el origen: ¿cuántos puntos de coordenadas enteras puede contener un arco de longitud R^α, con $0 < \alpha < 1$? Javier dio una interesante respuesta en uno de sus primeros trabajos ([6]):

Teorema 1. *Para todo $\alpha < 1/2$ existe una constante C_α tal que un arco de longitud R^α contiene, a los más, C_α puntos del retículo.*

Este resultado y sus extensiones al caso de elipses e hipérbolas aparecen de forma recurrente en diversas publicaciones de Javier ([6], [4], [10]), y constituye una parte importante de esa primera etapa de su producción científica. Un ejemplo es el siguiente.

Sea $S(n)$ el área del polígono cuyos vértices son los puntos del retículo en el círculo $x^2 + y^2 = n$ (cuando $r_2(n) \neq 0$), y consideremos la cantidad $S(n)/(\pi n)$. Claramente esos puntos estarán mejor distribuidos cuando $S(n)/(\pi n)$ se encuentre muy próximo a la unidad:

TEOREMA 2. *El conjunto* $\{S(n)/(\pi n) : r(n) \neq 0\}$ *es denso en el intervalo* $(2/\pi, 1)$.

TEOREMA 3. *Existe una infinidad de valores* n *tales que*[1]

$$\Big|\frac{S(n)}{\pi n} - 1\Big| \lesssim \Big[\frac{\log\log n}{\log n}\Big]^2.$$

La estimación anterior está cerca de lo óptimo, ya que es fácil demostrar que, en la dirección opuesta, tenemos la desigualdad

$$\Big|\frac{S(n)}{\pi n} - 1\Big| \gtrsim \frac{1}{r_2^2(n)}.$$

El precioso artículo [2] que F. Chamizo ha escrito para este mismo número de LA GACETA contiene una demostración del Teorema 1 obtenida por Javier y G. Tennenbaum algunos años después, y distinta de la primera. Fernando describe también el origen del problema y su relación con la teoría de las series trigonométricas dobles: el teorema de Cooke–Zygmund y las propiedades de restricción de las series e integrales de Fourier. Y hace alusión al interés que estos resultados han adquirido recientemente en los trabajos de J. Bourgain y Z. Rudnick sobre las regiones nodales de las autofunciones de operadores de Laplace–Beltrami, a lo que hay que añadir su relevancia en ciertos modelos mecano-estadísticos.

Creo que a Javier le agradaba mucho saber de esas consecuencias y aplicaciones del teorema, pero tenía tantos proyectos aritméticos sobre los que trabajar que no lograba encontrar un hueco para conocerlas en profundidad. En cuanto al exponente 1/2, me consta que estaba bastante convencido de su irrelevancia y que el teorema, según él, tendría que ser cierto para todo $\alpha < 1$. Sin embargo, yo no estoy tan seguro de ello, y por el contrario tiendo a pensar que 1/2 puede ser relevante, basándome en la analogía con el teorema de restricción de la transformada de Fourier bidimensional. En cualquier caso, saber lo que ocurre más allá de 1/2 ha demostrado ser una cuestión tan interesante como difícil.

2. SERIES TRIGONOMÉTRICAS ESPECIALES: CONJUNTOS DE SIDON

Las series trigonométricas llamadas lacunares tienen frecuencias que crecen geométricamente ($n_{k+1}/n_k > \rho > 1$), y poseen propiedades muy particulares. Por ejemplo: si $\sum_k a_k \exp(2\pi i n_k x)$ es la serie de Fourier de una función f en el espacio $L^2(0,1)$, entonces, necesariamente, f pertenece a $L^p(0,1)$ para todo $p < \infty$.

[1] Usaremos la notación estándar: i) $A(z) \simeq B(z)$ cuando existen constantes $0 < C_1 < C_2 < \infty$ tales que $C_1 A(z) \leq B(z) \leq C_2 A(z)$ para todo z; ii) $A(z) \lesssim B(z)$ si existe una constante finita C tal que $A(z) \leq C\, B(z)$ siempre).

Se trata de un resultado bien conocido del análisis armónico que tiene una interpretación dentro del espacio BMO (acrónimo en inglés de las funciones de oscilación media acotada): el multiplicador de Fourier $\widehat{Tf}(j) = m(j) \cdot \widehat{f}(j)$, donde $m(j) = 1$ si j está entre los n_k, y es igual a 0 en caso contrario, es un operador acotado de L^2 a BMO y, por tanto, a L^p para todo $p < \infty$. Pero admite también otras interpretaciones de carácter probabilístico y aritmético: por un lado, las funciones $\{\exp(2\pi i n_k x)\}$ se comportan como si fuesen variables aleatorias independientes, y por otro, dado s, el número de representaciones de un entero arbitrario como suma de s términos n_k está uniformemente acotado. Creo poder afirmar que a Javier no le interesaba demasiado la primera de ellas, pero sí, y mucho, las otras dos.

¿Habrá una teoría similar cuando las frecuencias crezcan de forma polinomial? Se trata de una pregunta natural que tiene consecuencias aritméticas muy interesantes. Supongamos que la sucesión creciente de enteros positivos $n_1 < n_2 < n_3 < \cdots$ tiene la propiedad llamada $B_2(g)$: el número de representaciones de un entero arbitrario como suma de dos términos de la sucesión es menor que g. Resulta entonces fácil comprobar que el multiplicador asociado de Fourier está acotado del espacio $L^2(0,1)$ al $L^4(0,1)$. En otras palabras: la serie $f(x) = \sum_k a_k \exp(2\pi i n_k x)$ está en $L^4(0,1)$ si y solo si $\sum_k |a_k|^2 < +\infty$.

La sucesión de los cuadrados $n_k = k^2$ no satisface esta hipótesis pero, en cierto sentido, no queda muy lejos de hacerlo, siendo una conjetura famosa del área (también llamada problema de Rudin) la que asegura que la estimación

$$\Big\| \sum_k a_k \exp(2\pi i k^2 x) \Big\|_p \leq C_p \Big(\sum_k |a_k|^2 \Big)^{1/2}$$

es cierta para todo p, $1 \leq p < 4$.

Aunque su enunciado sea «muy analítico», la conjetura tiene un fuerte contenido aritmético, y en ella las sumas de Gauss

$$G_N(x) = \sum_{n=0}^{N-1} \exp(2\pi i n^2 x)$$

desempeñan un papel relevante.

Definamos $T_N f = G_N * f$. La conjetura de Rudin es equivalente a la acotación uniforme $L^2 \to L^p$, $p < 4$, de estos operadores, lo que, por dualidad, resulta ser equivalente a su acotación uniforme entre L^q y L^2, para $q > 4/3$.

Cuando Javier empezó a trabajar conmigo escuchaba estas disquisiciones con atención, seguramente por deferencia a su director de tesis, pero creo que sin mostrar demasiado entusiasmo. Sin embargo, este se despertaba en cuanto aparecían las implicaciones aritméticas.

Consideremos una progresión aritmética de enteros positivos

$$A = \{a, a + r, a + 2r, \dots\}$$

y preguntémonos: ¿cuántos cuadrados podemos encontrar entre sus N primeros términos?

Naturalmente, de lo que se trata es de dar buenas estimaciones cuando N tiende a infinito manteniéndose a y r fijos.

Sea

$$f(x) = \sum_{k=0}^{N-1} \exp(2\pi i(a+kr)\,x)$$

y sea $\widehat{Tf}(j) = m(j)\widehat{f}(j)$ el multiplicador de la serie de Fourier dado por la función indicadora de los cuadrados: $m(j) = 1$ si j es un cuadrado perfecto, y $m(j) = 0$ en caso contrario. Tenemos que:

$$\|T(f)\|_2^2 = \text{número de cuadrados en la sucesión } \{a, a+r, \dots, a+(N-1)r\}.$$

Si la conjetura de Rudin fuese cierta tendríamos que $\|T(f)\|_2 \le C_p\,\|f\|_p \le C'_p\,N^{(p-1)/p}$ para todo $p > 4/3$, lo que da lugar a la estimación

$$\#\big\{\{a, a+r, \dots, a+(N-1)r\} \cap \{1^2, 2^2, 3^2, \dots\}\big\} \le C_\varepsilon\,N^{1/2-\varepsilon},$$

esto es, el número de cuadrados entre los primeros N términos de la sucesión es $\lesssim N^{1/2-\varepsilon}$ para todo $\varepsilon > 0$. El mejor resultado conocido ([1]) dista mucho de esta estimación óptima.

Ocurre que los núcleos de Gauss son muy distintos de los de las integrales singulares de la teoría de Calderón–Zygmund que sabemos tratar en el análisis armónico. Estos últimos tienen sus singularidades en el origen y en el infinito, mientras que en las sumas de Gauss las singularidades se encuentran entre los racionales de denominador pequeño respecto de N. Y aunque siguiendo el método del círculo de Hardy–Littlewood–Ramanujan conocemos muy bien los valores de G_N en los llamados arcos mayores, sin embargo, la cancelación intrínseca a las convoluciones $G_N * f$ con una función genérica de L^2 se escapa, por ahora, a los métodos conocidos del análisis. A Henryk Iwaniec le oí en una ocasión un acertado comentario sobre este asunto:

> [...] en el análisis armónico se consideran núcleos de convolución «sencillos» que se aplican a funciones «complicadas», mientras que en la teoría de los números consideramos núcleos «muy complicados» que actúan sobre funciones «sencillas».

De manera que cabe, siguiendo a Iwaniec, resolver los problemas aritméticos sin entrar en laberintos analíticos del tipo de la conjetura de Rudin, ¿o no?

Le debo a Antoni Zygmund (mi bisabuelo en matemáticas) haber despertado mi interés por este tipo de cuestiones ubicadas en la frontera del análisis armónico y la teoría de los números, que luego logré transmitir a Javier. A continuación voy a describir un resultado del año 1992, que seguramente no estará entre los más destacados de nuestra producción, pero que creo representativo de la acción en esa frontera de las dos áreas antes mencionadas donde se ha desarrollado gran parte de nuestros proyectos conjuntos.

Una manera conocida de regularizar los valores de la función $r_2(n)$ es considerar sus promedios o, lo que es equivalente, la sucesión de sus sumas parciales

$$\sum_{n\leq x} r_2(n),$$

que representa el número de puntos reticulares dentro del círculo de radio $\sqrt{x}$ centrado en el origen, siendo de sobra conocida la estimación asintótica

$$\sum_{n\leq x} r_2(n) = \pi\, x + O(x^{1/2})\,, \quad x\to\infty.$$

La «irregularidad» de los valores de la función $r_2(n)$ viene expresada en el hecho de que el orden de magnitud de $\sum_{n\leq x} r_2^2(n)$ sea estrictamente mayor que el de $\sum_{n\leq x} r_2(n)$:

$$\frac{\sum_{n\leq x} r_2^2(n)}{\sum_{n\leq x} r_2(n)} \gtrsim \log(x).$$

La siguiente definición trata de captar este fenómeno.

Definición 4. Diremos que una sucesión de enteros positivos $\{n_k\}$ tiene la propiedad $B_2(\infty)$ si

$$\limsup_{x\to\infty} \frac{\sum_{n\leq x} r^2(n)}{\sum_{n\leq x} r(n)} < \infty,$$

donde, ahora,

$$r(n) = \#\{(n_k, n_j)\ :\ n = n_k + n_j\}.$$

El resultado que vamos a comentar dice así:

Teorema 5. *Existen sucesiones infinitas de cuadrados $a_1^2 < a_2^2 < a_3^2 < \cdots$ satisfaciendo la propiedad $B_2(\infty)$ y tales que $a_k^2 < k^2\log(k)$.*

En [7] se construye explícitamente una tal sucesión de la manera siguiente. Sean $I_j = \{n : 2^j < 2n < 2^j(1+1/j)\}$, donde $j = 1, 2, 3, \ldots$, y consideremos $I = \cup_j I_j$; la sucesión buscada consiste en los cuadrados de los elementos de I.

La estimación $a_k^2 < k^2\log(k)$ es inmediata, y tenemos también la desigualdad

$$\sum_{n\leq x} r(n) = \sum_{\substack{a_k^2+a_j^2\leq x\\ a_k<a_j}} 1 \geq \frac{1}{2}\Big(\sum_{a_k^2\leq x/4} 1\Big) \gtrsim \frac{x}{(\log x)^2}.$$

Por lo tanto es suficiente con demostrar que

$$\sum_{n\leq x} r^2(n) \lesssim \frac{x}{(\log x)^2}.$$

Consideremos, para cada j, la función $r_j(n)$ que cuenta el número de representaciones de n como suma de dos elementos de I_j. (La notación $r_j(n)$ introducida ahora hace referencia a la sucesión I_j y no debe confundirse, en el caso $j = 2$, con la función que cuenta el número de representaciones como suma de cuadrados que hemos considerado antes). Tenemos que

$$\sum_{n\le x} r^2(n) \lesssim \Big[\sum_{j\le\lfloor \log_4(x)\rfloor} \Big(\sum_n r_j^2(n)\Big)^{1/2}\Big]^2,$$

que es una consecuencia de la teoría de Littlewood–Paley del análisis armónico, junto con la interpretación de las sumas $\sum_{n\le x} r^2(n)$ en términos de normas L^4 de unos polinomios trigonométricos apropiados:

$$\begin{aligned}\sum_{n\le x} r^2(n) &\simeq \Big\| \sum_{j\le(\log_2 x)/2} \sum_{n\in I_j} \exp(2\pi i n^2 x)\Big\|_4^4\\ &\simeq \Big\|\Big(\sum_{j\le(\log_2 x)/2} \Big|\sum_{n\in I_j} \exp(2\pi i n^2 x)\Big|^2\Big)^{1/2}\Big\|_4^4\\ &\lesssim \Big(\sum_{j\le(\log_2 x)/2} \Big\|\sum_{n\in I_j} \exp(2\pi i n^2 x)\Big\|_4^2\Big)^2 \simeq \Big(\sum_{j\le(\log_2 x)/2} \Big(\sum_n r_j^2(n)\Big)^{1/2}\Big)^2.\end{aligned}$$

La demostración se consigue a partir de la acotación

$$\sum_n r_j^2(n) \lesssim \Big(\frac{2^j}{j}\Big)^2, \tag{$\star$}$$

ya que

$$\sum_{n\le x} r^2(n) \lesssim \Big(\sum_{j\le(\log_2 x)/2} \frac{2^j}{j}\Big)^2 \lesssim \frac{x}{(\log x)^2}.$$

La estimación $(\star)$ anterior es una consecuencia del siguiente lema:

LEMA 6. *Si $r_j(n) \ge 2$, entonces $r_j^2(n) \le F(n)$, donde $F(n)$ cuenta el número de soluciones enteras (a_1, b_1, a_2, b_2) del sistema de desigualdades*

$$0 < \Big|\frac{a_1}{b_1}\Big| < \frac{1}{j}, \qquad 0 < \Big|\frac{a_2}{b_2} - 1\Big| < \frac{1}{j}, \qquad n = a_1^2 + b_1^2 = a_2^2 + b_2^2.$$

Suponiéndolo cierto, la propiedad $(\star)$ buscada se demuestra así:

$$\sum_n r_j^2(n) = \sum_{r_j(n)=1} r_j(n) + \sum_{r_j(n)\ge 2} r_j^2(n),$$

y como

$$\sum_{r_j(n)=1} r_j(n) \le \Big(\frac{2^j}{j}\Big)^2,$$

basta pues con estimar el segundo sumando.

Pero el lema 6 nos dice que está acotado por el número de soluciones (a_1, b_1, a_2, b_2) del sistema

$$2\,(2^j)^2 \le (a_1^2 + b_1^2)\,(a_2^2 + b_2^2) \le 2\,(2^{j+1}/j)^2$$
$$0 < \Big|\frac{a_1}{b_1}\Big| < \frac{1}{j}, \qquad 0 < \Big|\frac{a_2}{b_2} - 1\Big| < \frac{1}{j}.$$

Con (a_1, b_1) fijado, estimaremos cuántos (a_2, b_2) verifican

$$\sqrt{2}\,\frac{2^j}{\sqrt{a_1^2 + b_1^2}} \le \sqrt{a_2^2 + b_2^2} \le \sqrt{2}\,\frac{2^j + 2^j/j}{\sqrt{a_1^2 + b_1^2}},$$

es decir, el número de puntos del retículo en una región simétrica respecto a la bisectriz del primer cuadrante, contenida entre los radios

$$r_1 = \sqrt{2}\,\frac{2^j}{\sqrt{a_1^2 + b_1^2}} \quad \text{y} \quad r_2 = \sqrt{2}\,\frac{2^j + 2^j/j}{\sqrt{a_1^2 + b_1^2}},$$

y cuya longitud en la dirección angular es también

$$\sqrt{2}\,\frac{2^j/j}{\sqrt{a_1^2 + b_1^2}}\,.$$

Ahora bien, la condición $0 < |a_2/b_2 - 1| < 1/j$ implica que $b_2 > j$, y un sencillo cálculo muestra que las dimensiones, radial y angular, de esa región son lo suficientemente grandes como para que el número de puntos reticulares contenidos en ella pueda ser estimado por su área, lo que nos permite escribir

$$\sum_{r_j(n)\ge 2} r_j(n)^2 \lesssim \sum_{\substack{a_1, b_1 \\ 0<|a_1/b_1|<1/j}} \frac{4^j}{(a_1^2 + b_1^2)\,j^2} \lesssim \sum_{b_1 \le 2^j} \frac{4^j}{b_1\,j^3} \le \frac{4^j}{j^2}\,,$$

y, por tanto,

$$\sum_{n\le x} r^2(n) \lesssim \frac{x}{(\log x)^2}\,.$$

Demostración del Lema 6. Empezamos observando que si $n \equiv 0 \pmod 4$ admite dos representaciones distintas como suma de dos cuadrados, $n = a^2 + b^2 = c^2 + d^2$, entonces existen enteros a_1, b_1, a_2, b_2 tales que

$$\frac{a_1}{b_1} = \tan\Big(\frac{\arctan(a/b) + \arctan(c/d)}{2}\Big),$$
$$\frac{a_2}{b_2} = \tan\Big(\frac{\arctan(a/b) - \arctan(c/d)}{2}\Big).$$

Sea pues $n = a_r^2 + b_r^2 = a_s^2 + b_s^2$ un entero con dos representaciones distintas como suma de dos cuadrados tales que

$$2^j \le a_r \le a_s \le b_s \le b_r \le 2^j + 2^j/j, \qquad a_r \equiv b_r \equiv a_s \equiv b_s \pmod 2.$$

Por la observación anterior, existen enteros a_1, b_1, a_2, b_2 de manera que

$$\begin{aligned} n &= (a_1^2 + b_1^2) \cdot (a_2^2 + b_2^2), \\ \frac{a_1}{b_1} &= \tan\Big(\frac{\arctan(a_r/b_r) + \arctan(a_s/b_s)}{2}\Big), \\ \frac{a_2}{b_2} &= \tan\Big(\frac{\arctan(a_r/b_r) - \arctan(a_s/b_s)}{2}\Big). \end{aligned}$$

Las condiciones impuestas sobre a_1, b_1, a_2, b_2 implican que $|a_1/b_1| < 1/j$ y $|a_2/b_2 - 1| < 1/j$. Pero ambas cantidades tienen que ser también estrictamente mayores que 0, porque hemos partido de dos representaciones distintas de n como suma de cuadrados. Cada pareja de tales representaciones origina ángulos diferentes y, por consiguiente, enteros distintos a_1, b_1, a_2, b_2. Podemos concluir que el número de tales parejas, $r_j(n)(r_j(n)-1)/2$, está acotado por arriba por el número de soluciones del sistema

$$\begin{aligned} n &= (a_1^2 + b_1^2) \cdot (a_2^2 + b_2^2)\,, \\ 0 &< \Big|\frac{a_1}{b_1}\Big| < \frac{1}{j}\,, \\ 0 &< \Big|\frac{a_2}{b_2} - 1\Big| < \frac{1}{j}\,. \end{aligned}$$

La demostración se concluye observando que si $r_j(n) \geq 2$, entonces

$$r_j^2(n) \leq 4(r_j(n)(r_j(n)-1)/2). \qquad \square$$

El teorema exhibe una fusión de métodos del análisis armónico (multiplicadores de Fourier, teoría de Littlewood–Paley) y de elementales, pero ingeniosas, maneras de contar puntos del retículo, en las que puede apreciarse el inconfundible marchamo de Javier, quien siguió interesado en este tipo de cuestiones pero con una clara deriva hacia su parte más combinatoria.

Parece ser que Simon Sidon preguntó a Pál Erdős sobre las sucesiones de enteros de menor crecimiento que tuvieran esa propiedad de producir el teorema $L^2(0,1) \to L^4(0,1)$ para las correspondientes series de Fourier. En manos de Erdős, Rényi y la espléndida escuela húngara de matemática discreta, el problema se transformó en desafío y objeto del deseo, aunque modificaron un poco el enunciado: «un conjunto de enteros positivos es llamado de Sidon si las sumas de dos cualesquiera de ellos son siempre distintas». Surge el problema: construir, o probar la existencia, de sucesiones de Sidon de manera que la función $A(x)$ que cuenta el número de puntos de A entre 1 y x sea lo mayor posible.

Una primera aproximación se obtiene con el llamado «algoritmo avaricioso»: empezando con $a = 1$, definimos a_{n+1} como el menor entero positivo que podemos añadir al conjunto $\{a_1, \ldots, a_n\}$ de manera que se conserve la propiedad de Sidon. Obtenemos así la sucesión

$$1, 2, 4, 8, 13, 21, 31, 45, 66, 81, 97, 123, \ldots$$

En cada paso, los elementos eliminados son todos aquellos de la forma $a_i+a_j-a_k$, donde tanto i como j y k son menores que n. Como, a lo más, hay n^3 de ellos, podemos concluir que $a_{n+1} \leq n^3+1$, lo que implica que $A(x) \gtrsim x^{1/3}$.

Resulta relativamente fácil comprobar que la estimación $A(x) \gtrsim x^{1/2}$ es falsa, por lo que la verdad se encuentra en un exponente intermedio entre 1/3 y 1/2.

Conjetura 7 (Atribuida a Erdős). *Para cada $\varepsilon > 0$, existe un conjunto de Sidon tal que $A(x) \gtrsim x^{1/2-\varepsilon}$.*

La conjetura ha resistido los ataques de los miembros más conspicuos del área (Erdős, Szemeredi, Rusza, Cilleruelo, etc.), quienes, no obstante, han logrado interesantes resultados parciales. Hasta hace poco, el mejor de ellos se debía a I. Rusza quien, usando métodos probabilísticos, logró probar la existencia de un conjunto de Sidon cuya función contadora satisface

$$A(x) = x^{\sqrt{2}-1+o(1)}.$$

Pero el método de Rusza no es constructivo y restaba dar un ejemplo explícito de una tal sucesión. Eso lo llevó a cabo Javier en la que, seguramente, es una de sus mejores publicaciones ([5]).

Teorema 8. *Existe una sucesión explícita de Sidon cuya función contadora satisface la estimación asintótica $A(x) = x^{\sqrt{2}-1+o(1)}$, $x \to \infty$.*

La construcción, aunque basada en métodos elementales, no es nada fácil, y contiene muchos regates ingeniosos: a partir de la sucesión de los logaritmos de los números primos, que por el teorema fundamental de la Aritmética forman un conjunto de Sidon de números reales, se obtiene una sucesión con la propiedad de Sidon y densidad grande… Y aquí no cabe ya otro comentario sino recomendar la lectura de [5].

Con gran agrado por mi parte, he sido testigo de cómo Javier fue conectando con los expertos reconocidos del área, quienes han venido a Madrid para trabajar y colaborar en sus proyectos; al tiempo que él ha sido un participante habitual en todos los congresos y *workshops* importantes, organizados en los centros del mundo donde se cultiva el arte combinatoria y la teoría aditiva de números. Y aunque esa espléndida actividad lo alejara un tanto de los problemas de las series trigonométricas que estuvieron en sus comienzos conmigo, me he sentido muy orgulloso de sus logros y de su trayectoria.

Referencias

[1] E. Bombieri y U. Zannier, A note on squares in arithmetic progressions. II. *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl.* **13** (2002), no. 2, 69–75.

[2] F. Chamizo, Un teorema de Javier Cilleruelo (en este mismo número de *La Gaceta*). [Hay que poner la referencia precisa cuando compongamos la revista]

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

[4] J. CILLERUELO, The distribution of the lattice points on circles, *J. Number Theory* **43** (1993), no. 2, 198–202.

[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, $B_2[\infty]$-sequences of square numbers, *Acta Arith.* **61** (1992), no. 3, 265–270.

[8] J. CILLERUELO Y A. CÓRDOBA, Lattice points on ellipses, *Duke Math. J.* **76** (1994), no. 3, 741–750.

[9] J. CILLERUELO Y J. L. FERNÁNDEZ, P. FERNÁNDEZ, Visible lattice points in random walks. Prepublicación, arXiv: 1512.04722 (2016).

[10] J. CILLERUELO Y J. JIMÉNEZ-URROZ, Lattice points on hyperbolas. *J. Number Theory* **63** (1997), no. 2, 267–274.

[11] J. CILLERUELO Y F. LUCA, Every positive integer is a sum of three palindromes. Prepublicación, arXiv: 1602.06208 (2016).

[12] J. CILLERUELO, I. RUSZA Y C. VINUESA, Generalized Sidon sets, *Adv. Math.* **225** (2010), no. 5, 2786–2807.

ANTONIO CÓRDOBA, ICMAT Y DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD AUTÓNOMA DE MADRID, CAMPUS DE CANTOBLANCO, 28049 MADRID

Correo electrónico: antonio.cordoba@uam.es