Miniaturas matemáticas de La Gaceta de la RSME
Vol. 24 (2021), Núm. 1, Pág. 146

Un resultado de Kubilyus y Linnik

Fijado $b \in \mathbb{Z}^+$, por ejemplo $b = 1$, es un problema abierto probar que la ecuación $p_1p_2 = n^2 + b^2$ admite infinitas soluciones con p_1, p_2 primos y $n \in \mathbb{Z}^+$. En analogía con otros problemas abiertos, como la conjetura de Goldbach, esto parece sugerir que tampoco hay muchas esperanzas de probarlo si hacemos b variable buscando soluciones p_1, p_2, n y b tales que b sea menor que una potencia pequeña de p_1p_2. Sin embargo, I. P. Kubilyus y Yu. V. Linnik (*Uspehi Mat. Nauk (N.S.)* **11** (1956), no. 2(68), 191–192) mostraron, con un bello argumento, que el problema para b acotado por algo del orden de $\log(p_1p_2)$ es «fácil». Usando su razonamiento aquí se prueba la siguiente versión explícita:

Teorema. *Sea* $\mathcal{C} = \{p \in [N, 2N) \text{ primo} : 4 \mid (p-1)\}$. *Para* N *mayor que cierta constante, la ecuación* $p_1p_2 = n^2 + b^2$ *admite una solución con* $p_1, p_2 \in \mathcal{C}$ *y* $n, b \in \mathbb{Z}^+$ *que satisface* $b < 2\log(p_1p_2)$.

Tomando N igual a potencias sucesivas de 2 se tiene la infinitud de soluciones con la restricción $b < 2\log(p_1p_2)$. En la demostración se usan dos hechos conocidos, el primero es debido a Fermat y el segundo es una consecuencia débil del teorema de los números primos en progresiones aritméticas:

(1) Los elementos de $\mathcal{C}$ se escriben como suma de dos cuadrados de forma única salvo el orden de los sumandos.

(2) Para N mayor que cierta constante, $\operatorname{card}(\mathcal{C}) > \frac{2N}{5\log N} + 1$.

Demostración del teorema. Por (1), para cada $p \in \mathcal{C}$ existen $a, b \in \mathbb{Z}^+$, $a > b$, con $p = |a + bi|^2$. Así p queda asociado a un número complejo de argumento $\varphi \in (0, \pi/4)$. Por (2) y el principio del palomar existen $z_1 = a_1 + ib_1$, $z_2 = a_2 + ib_2$ distintos con argumentos φ_1, φ_2 tales que $0 \le \varphi_1 - \varphi_2 < \frac{5\pi \log N}{8N} < \frac{2\log N}{N}$. Sean $p_1 = |z_1|^2$ y $p_2 = |z_2|^2$; claramente $p_1p_2 = |z_1\bar{z}_2|^2 = n^2 + b^2$ con $n = \left|\operatorname{Re}(z_1\bar{z}_2)\right|$ y $b = \left|\operatorname{Im}(z_1\bar{z}_2)\right|$. Con esto y la desigualdad $|\operatorname{sen}(x)| \le |x|$, tenemos

$$b = \left|\operatorname{Im}\left(\sqrt{p_1}e^{i\varphi_1}\sqrt{p_2}e^{-i\varphi_2}\right)\right| = \sqrt{p_1p_2}\left|\operatorname{sen}(\varphi_1 - \varphi_2)\right| < 4\log N \le 2\log(p_1p_2).$$

El caso $b = 0$ está excluido porque p_1 y p_2 son distintos. □

A pesar de que el problema mencionado al principio está abierto, hay un teorema que implica que, para b fijado, $n^2 + b^2$ tiene a lo más dos factores primos para infinitos $n \in \mathbb{Z}^+$. Este resultado es difícil, uno de los pináculos de la llamada «criba combinatoria» (H. Iwaniec, Almost-primes represented by quadratic polynomials, *Invent. Math.* **47** (1978), 171–188). El obstáculo teórico para separar los casos con exactamente dos factores primos se conoce como «fenómeno de la paridad».

Fernando Chamizo, Universidad Autónoma de Madrid e ICMAT
Correo electrónico: fernando.chamizo@uam.es
Página web: http://matematicas.uam.es/~fernando.chamizo/