Gregorio Hernández Peñalver
ETSI Informáticos, UPM

MATEMÁTICA DISCRETA II (MI)
TRABAJOS EN GRUPO

REPRESENTACIÓN DE ENTEROS COMO SUMA DE CUADRADOS

¿Qué enteros se pueden escribir como suma de dos cuadrados? Esta pregunta es tan antigua como la teoría de números y su respuesta es uno de los teoremas más bellos de la aritmética.

Diofanto en el siglo III dio la primera respuesta: "El producto de dos sumas de dos cuadrados se puede representar como suma de dos cuadrados" Por ejemplo, como $5 = 4 + 1$ y $13 = 9 + 4$ son suma de cuadrados también $5 \cdot 13 = 65$ es suma de cuadrados, $65 = 8^2 + 1^2$

En la Navidad de 1640, Fermat escribió una carta a Mersenne anunciándole el siguiente resultado:

"Todo primo congruente con 1 módulo 4 es suma de dos cuadrados"

que a veces se conoce como Teorema de Navidad de Fermat. Naturalmente Fermat no dio ninguna demostración, hubo que esperar a Euler quien presentó una primera demostración en 1749 utilizando su técnica de "descenso infinito". Posteriormente Lagrange, Gauss y Dedekind publicaron nuevas demostraciones.

Comprobemos el resultado con primos de la forma $4k + 1$
$13 = 2^2 + 3^2$, $41 = 4^2 + 5^2$, $61 = 5^2 + 6^2$, …
Este teorema es el ingrediente principal del siguiente teorema que responde a la pregunta inicial.

Teorema

Un número natural n se puede representar como suma de dos cuadrados si y solo si todos los factores primos de la forma p = 4k + 3 aparecen con exponente par en la factorización de n

Los números menores que 200 que se pueden representar como suma de dos cuadrados son:
5, 10, 13, 17, 20, 25, 26, 29, 34, 37, 40, 41, 45, 50, 52, 53, 58, 61, 65, 68, 73, 74, 80, 82, 85, 89, 90, 97, 100, 101, 104, 106, 109, 113, 116, 117, 122, 125, 130, 136, 137, 145, 146, 148, 149, 153, 157, 160, 164, 169, 170, 173, 178, 180, 181, 185, 193, 194, 197, ..
según podéis comprobar en la sucesión A004431 de The On-Line Encyclopedia of Integer Sequences®

Objetivos del trabajo:

- Presentar dos demostraciones elegantes del Teorema de Fermat: la primera de Thue que utiliza la estructura algebraica del conjunto Z_p y otra elemental de Heath-Brown. Ninguna de ellas es constructiva.
- Demostrar el teorema que responde a la pregunta inicial.
- Averiguar si la pregunta: *¿De cuántas formas se puede representar un número como suma de cuadrados?* tiene respuesta.
  Un ejemplo: $53461 = 231^2 + 10^2 = 206^2 + 105^2$
- ¿Qué resultados hay si permitimos 3 cuadrados, 4 cuadrados, ….?

Referencias

M. Aigner, G. Ziegler: "Proofs from THE BOOK", (cap. 4, 4th edition), Springer, 2010.
T. Koshy, "Elementary Number Theory with applications", Academic Press, 2002
S. Wagon: *Editor's corner*: "The Euclidean algorithm strikes again", Amer. Math. Monthly 97 (1990), 125-129
D. Zagier: "A one-sentence proof that every prime p≡1 (mod 4) is a sum of squares". *Amer. Math. Monthly*, 97, (1990), 144.