Enteros como suma de dos y de cuatro cuadrados

Por Julio César Díaz Calderón

Nivel Avanzado[2]

Introducción

El propósito de este texto es introducir algunas técnicas de resolución de problemas en ecuaciones diofantinas desde el estudio de un ejemplo particular: el teorema de Fermat de la suma de dos cuadrados. Una ecuación diofantina es cualquier ecuación de la forma

$$f(x_1, x_2, \ldots, x_n) = 0, \tag{1}$$

donde f es una función polinomial en n variables con coeficientes racionales. El caso que nos interesa es cuando f es un polinomio con coeficientes enteros con $n \geq 2$ y la ecuación (1) en este caso se denomina ecuación diofantina algebraica. En este contexto, resolver una ecuación diofantina algebraica significa determinar cuáles son todas las configuraciones $(x_1, x_2, \ldots, x_n)$, donde $x_1, x_2, \ldots, x_n$ son números enteros que satisfacen (1).

El estudio de técnicas para resolver cierto tipo de ecuaciones diofantinas se vuelve muy importante a partir de la resolución del problema diez de Hilbert, el cual establece que no hay un método general para resolverlas. La lista de problemas de Hilbert es la más famosa en el ámbito matemático y consiste de 23 problemas que formuló el matemático David Hilbert en el Congreso Internacional de Matemáticas en París en 1900. Según Hilbert, dichos problemas era en los que valía la pena trabajar en el nuevo milenio.

[2]Este artículo está basado en una plática titulada *Técnicas de resolución de problemas en ecuaciones diofantinas* que se presentó el 25 de octubre de 2016 en la sesión especial por el treinta aniversario de la Olimpiada Mexicana de Matemáticas. Esta sesión tuvo lugar en el XLIX Congreso Nacional de la Sociedad Matemática Mexicana en Aguascalientes, Aguascalientes.

El problema diez de Hilbert consiste en determinar si es posible encontrar un proceso en el que en una cantifidad finita de operaciones se señale si una ecuación diofantina tiene una solución en los números racionales. En 1970, Yuri Matiyasevich demostró, con la ayuda del trabajo previo de Martin Davis, Hilary Putnam y Julia Robinson, que no es posible decidir la existencia de soluciones de una ecuación diofantina. Más aún, demostró que existe un polinomio explícito $F(x_0, x_1, x_2, \ldots, x_n)$ tal que no hay un algoritmo que, dado un entero a como entrada, pueda decidir en un número finito de pasos si la ecuación $F(a, x_1, x_2, \ldots, x_n) = 0$ tiene una solución en los enteros.
Como las técnicas de resolución de ecuaciones diofantinas son demasiadas, nos limitaremos a desarrollar las que surgen al trabajar con una ecuación diofantina particular:

$$n = a^2 + b^2. \tag{2}$$

Esta ecuación aparece de manera natural cuando se estudian las ecuaciones diofantinas en tres variables cuyo máximo exponente es 2. Una ecuación más sencilla que también sirve de motivación para (2), es la ecuación de las ternas pitagóricas:

$$c^2 = a^2 + b^2. \tag{3}$$

Se puede demostrar que las soluciones en los enteros positivos de (3) son de la forma $a = p^2 - q^2, b = 2pq, c = p^2 + q^2$, para cualesquiera dos enteros p y q tales que $p > q$. El problema 1 ayuda a demostrar este hecho.
Este artículo se divide en tres partes. En la primera se dará respuesta a la interrogante detrás del teorema de Fermat: ¿cuáles son los enteros que se pueden escribir como suma de dos cuadrados de enteros? Las siguientes dos secciones desarrollan dos preguntas de investigación relacionadas con el teorema principal. Se concluye con una lista de problemas para aplicar lo expuesto en el artículo.

El teorema de Fermat de la suma de dos cuadrados

Si se hacen los cálculos para los primeros enteros positivos, es posible determinar que 3 no se puede escribir como suma de dos cuadrados. Los siguientes: 6, 7, 11, 12, 14, 15, etc., no arrojan demasiada información respecto a cómo deben ser estos números. La clave en estas situaciones es restringir el problema a una familia de enteros, por ello, se resolverá primero la ecuación diofantina:

$$p = a^2 + b^2, \tag{4}$$

con p un primo. Para poder resolver (4) será necesario desarrollar una teoría llamada *aritmética modular*.

Definición 1 (Congruencias)**.** *Dos enteros a y b son congruentes módulo un entero n si n divide a $a - b$. Se escribirá $a \equiv b$ (mod n) para indicar que a es congruente a b módulo n.*

Bajo la definición anterior, todo entero es congruente a $0, 1, 2$ o 3, módulo 4. Además, el cuadrado de todo entero será congruente a 0 o 1 módulo 4. Así, $p = a^2 + b^2 \equiv 0, 1$ o 2 (mod 4). Esto elimina la posibilidad de que un primo de la forma $4k + 3$ se pueda

escribir como la suma de dos cuadrados. Un desarrollo introductorio de la aritmética modular se puede consultar en el libro *Teoría de números* de María Luisa Pérez Seguí. Todo número primo distinto de 2, es de la forma $4k+1$ o de la forma $4k+3$. Por la observación anterior, para que un primo sea suma de dos cuadrados, entonces p debe ser 2 o de la forma $4k+1$. Resulta que estos números sí se pueden escribir como suma de dos cuadrados. Para probarlo y eliminar algunos casos en la versión general del problema se demostrará el siguiente lema:

Lema de Lagrange: La ecuación $u^2+1 \equiv 0 \pmod{p}$ tiene solución si y solo si $p \equiv 1 \pmod{4}$ o $p=2$.

Demostración: Este lema utiliza dos teoremas clásicos de teoría de números, el teorema pequeño de Fermat y el teorema de Wilson.

Teorema pequeño de Fermat: Si p es un primo y a es un entero que no es múltiplo de p, entonces $a^{p-1} \equiv 1 \pmod{p}$.

Teorema de Wilson: Si p es un primo, entonces $(p-1)! \equiv -1 \pmod{p}$.

Las demostraciones de ambos teoremas, así como ejemplos y ejercicios, se pueden consultar en el libro *Teoría de números*. Supongamos que la ecuación $u^2+1 \equiv 0 \pmod{p}$ tiene solución y que $p = 4k+3$ con k un entero positivo. Como $u^2+1 \equiv 0 \pmod{p}$, entonces $\text{mcd}(u,p)=1$; así, por el teorema pequeño de Fermat, $u^{p-1} \equiv 1 \pmod{p}$. Entonces, $u^{4k+2} \equiv 1 \pmod{p}$. Sin embargo, $u^{4k+2} = (u^2)^{2k+1} \equiv (-1)^{2k+1} \equiv -1 \pmod{p}$. Por tanto, $1 \equiv -1 \pmod{p}$, es decir, $p=2$, lo cual es una contradicción. Entonces, $p \equiv 1 \pmod{4}$ o $p=2$.
Ahora, si $p = 4k+1$ para algún entero positivo k, el teorema de Wilson nos garantiza que:

$$\begin{aligned} 0 &\equiv (p-1)!+1 \\ &\equiv 1 \cdot 2 \cdots (2k-1) \cdot (2k) \cdot (2k+1) \cdot (2k+2) \cdots (4k-1) \cdot (4k) + 1 \\ &\equiv 1 \cdot 2 \cdots (2k-1) \cdot (2k) \cdot (-2k) \cdot (-(2k-1)) \cdots (-2) \cdot (-1) + 1 \\ &\equiv (-1)^{2k}((2k)!)^2 + 1 \\ &\equiv ((2k)!)^2 + 1 \pmod{p}. \end{aligned}$$

Así, $u = (2k)!$ es una solución de $u^2+1 \equiv 0 \pmod{p}$. Para el caso $p=2$, basta con verificar que $u=1$ cumple. Con lo que queda demostrado el lema de Lagrange.
Para concluir que todos los primos de la forma $p = 4k+1$ pueden escribirse como suma de dos cuadrados es necesario introducir una nueva herramienta: el principio de las casillas.

Principio de las casillas: El principio de las casillas establece que si se colocan $k+1$ objetos en k casillas, entonces se tendrán que colocar dos objetos en una misma casilla.

La dificultad de los problemas que se resuelven al aplicar un argumento que usa el principio de las casillas radica en identificar cuáles son los objetos y cuáles son las casillas. Para una discusión a profundidad de cómo utilizar el principio de las casillas, se recomienda consultar el libro *Principio de las casillas* de José Antonio Gómez Ortega, Rogelio Valdez Delgado y Rita Vázquez Padilla. Demostraremos el siguiente lema:

Lema 1: Los primos de la forma $4k + 1$ se pueden escribir como suma de dos cuadrados.

Demostración: En este caso las casillas serán los números $0, 1, 2, \ldots, p - 1$, estos cumplen que cada entero es congruente a uno de ellos módulo p. Los objetos corresponderán a los enteros de la forma $ux - y$, donde u es el entero que se obtuvo en el lema de Lagrange y $0 \leq x, y < \sqrt{p}$. El número de parejas (x, y), que cumplen las condiciones del problema es $(\lfloor\sqrt{p}\rfloor + 1)^2 > (\sqrt{p})^2 = p$. Por tanto, hay al menos $p + 1$ enteros de la forma $ux - y$ y p posibles congruencias módulo p, entonces el principio de las casillas nos garantiza que existen dos enteros $ux_1 - y_1$ y $ux_2 - y_2$ tales que $ux_1 - y_1 \equiv ux_2 - y_2 \pmod{p}$. Entonces, $u(x_1 - x_2) \equiv -(y_1 - y_2) \pmod{p}$, por tanto, $u^2(x_1 - x_2)^2 \equiv (y_1 - y_2)^2 \pmod{p}$. Pero, $u^2 \equiv -1 \pmod{p}$, entonces $-(x_1 - x_2)^2 \equiv (y_1 - y_2)^2 \pmod{p}$. Luego, $(x_1 - x_2)^2 + (y_1 - y_2)^2$ es un múltiplo de p. Sin embargo, $0 < (x_1 - x_2)^2 + (y_1 - y_2)^2 < (\sqrt{p})^2 + (\sqrt{p})^2 = 2p$. Por tanto, $(x_1 - x_2)^2 + (y_1 - y_2)^2 = p$, con lo que queda demostrado el lema. □

Para demostrar el teorema principal es necesario probar un lema que se obtiene por medio de una manipulación algebraica conocida como la identidad de Brahmagupta. Su demostración es inmediata al desarrollar ambos lados.

Identidad de Brahmagupta: Si a, b, c, d son números reales, entonces

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

Lema 2: Si n y m se pueden escribir como la suma de dos cuadrados, entonces nm también se puede escribir como la suma de dos cuadrados.

Demostración: Si $n = a^2 + b^2$ y $m = c^2 + d^2$, la identidad de Brahmagupta garantiza que $mn = (ac - bd)^2 + (ad + bc)^2$. Por tanto, mn se puede escribir como suma de dos cuadrados. □

Definición 2. *Un entero m es libre de cuadrados si todo primo p que divide a m es tal que p^2 no divide a m.*

Teorema de Fermat de la suma de dos cuadrados: Un entero positivo n es la suma de dos cuadrados si y solo si cada factor primo p de n tal que $p \equiv 3 \pmod{4}$ aparece con un exponente par en la factorización en primos de n.

Demostración: Sea n un entero, entonces lo podemos escribir como $n = r^2m$ donde m es un entero libre de cuadrados. Si $n = a^2 + b^2$, con $n, a, b \in \mathbb{Z}$, entonces $n = d^2(x^2 + y^2)$ donde $d = \text{mcd}(a, b)$, $a = dx$ y $b = dy$. Así, $\frac{n}{d^2} = \frac{r^2m}{d^2} = x^2 + y^2$. Como m es libre de cuadrados, entonces d^2 divide a r^2, por tanto, $x^2 + y^2 = tm$, para algún entero t. Sea p un primo divisor de m. Supongamos que $p = 4k + 3$, para un entero k. Se sabe que $x^2 + y^2 \equiv 0 \pmod p$ y que $\text{mcd}(x, y) = 1$, entonces $\text{mcd}(x, p) = \text{mcd}(y, p) = 1$. Además, $x^2 \equiv -y^2 \pmod p$, entonces $(x^2)^{2k+1} \equiv (-1)^{2k+1}(y^2)^{2k+1} \pmod p$, que equivale a $x^{p-1} \equiv -y^{p-1} \pmod p$. Pero, $\text{mcd}(x, p) = \text{mcd}(y, p) = 1$, entonces el teorema pequeño de Fermat asegura que $x^{p-1} \equiv y^{p-1} \equiv 1 \pmod p$, así $1 \equiv -1 \pmod p$. Por tanto, $p = 2$, lo cual es una contradicción. Entonces, todo divisor primo p de m cumple que $p \equiv 1 \pmod 4$ o $p = 2$.
Ahora, si todo factor primo p tal que $p \equiv 3 \pmod 4$ aparece con exponente par en la descomposición en factores primos de n, entonces m solo puede tener como factores primos a 2 y a primos p tales que $p \equiv 1 \pmod 4$. Dado que $2 = 1^2 + 1^2$ y el lema 1 es cierto, entonces todo factor primo de m se puede escribir como suma de dos cuadrados. Por tanto, el lema 2 garantiza que m se podrá escribir como suma de dos cuadrados, así $m = x^2 + y^2$, con x e y enteros. Entonces, $n = (rx)^2 + (ry)^2$. En conclusión, n se puede escribir como suma de dos cuadrados. □

La siguiente demostración de Dietmann y Elsholtz ilustra cómo utilizar el teorema anterior para resolver ecuaciones diofantinas. Se invita al lector a intentar resolver el problema antes de ver su solución.

Problema 1: Sea p un primo con $p \equiv 7 \pmod 8$. Demuestra que no hay enteros positivos x, y, z tales que $x^2 + y^2 + z^4 = p^2$.

Demostración: Si existiera una solución, entonces $x^2 + y^2 = (p - z^2)(p + z^2)$. Si z es par, entonces $p - z^2 \equiv 3 \pmod 4$. Si z es impar, entonces $p + z^2 \equiv 3 \pmod 4$. En ambos casos $p - z^2$ o $p + z^2$ contiene un primo divisor q tal que $q \equiv 3 \pmod 4$ y que es de multiplicidad impar. En efecto, si $n = p + z^2$ o $n = p + z^2$ y si

$$n = 2^\alpha \prod_{p \equiv 1 \pmod 4} p^{\beta_p} \prod_{q \equiv 3 \pmod 4} q^{\gamma_q}$$

donde p corre sobre todos los primos de n de la forma $4k + 1$ en el primer producto, q corre sobre todos los primos de n de la forma $4k + 3$ en el segundo producto y γ_q son todos pares, entonces

$$\begin{aligned} n &\equiv 2^\alpha \prod_{p \equiv 1 \pmod 4} 1^{\beta_p} \prod_{q \equiv 3 \pmod 4} (4k_q + 3)^{\gamma_q} \equiv 2^\alpha \prod_{q \equiv 3 \pmod 4} (16k_q^2 + 24k_q + 9)^{\frac{\gamma_q}{2}} \\ &\equiv 2^\alpha \pmod 4, \end{aligned}$$

que no puede ser congruente con 3 módulo 4. Por tanto, por el teorema de Fermat de la suma de dos cuadrados, tanto $p - z^2$ como $p + z^2$ son divisibles por q. Luego, la suma de ambos números, $2p$, y su diferencia, $-2z^2$, son divisibles entre q. Dado que p es un primo, entonces $p = q$; además como $z \neq 0$, entonces q divide a z. Lo anterior implica una contradicción pues $x^2 + y^2 + z^4 > q^4 > q^2 = p^2$.

Unicidad de las soluciones

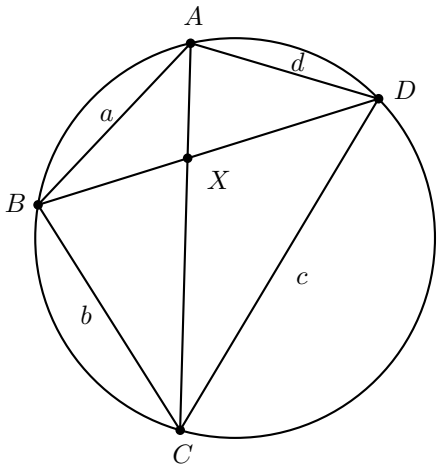
Una vez resuelto el problema inicial sobre qué enteros se pueden escribir como la suma de dos cuadrados, la pregunta que surge es: ¿dicha representación es única en los enteros positivos? Es decir, ¿puede ocurrir que $n = a^2+b^2 = c^2+d^2$ con $n, a, b, c, d \in \mathbb{Z}^+$ y $\{a, b\} \neq \{c, d\}$? La respuesta es afirmativa, por ejemplo: $65 = 1^2+8^2 = 4^2+7^2$. Sin embargo, conocer cuántas representaciones tiene un número como suma de dos cuadrados es complicado. En este apartado resolveremos el problema anterior para los primos.

Lema 3: Si hay dos pares no ordenados (x, y) de enteros positivos que satisfacen la ecuación

$$x^2 + y^2 = n,$$

entonces n es compuesto.

Demostración 1: Suponga que existe un primo $n = p$ tal que $x^2 + y^2 = n$ tiene dos soluciones enteras positivas (a, b) y (c, d). Sin pérdida de generalidad, $ac + bd \geq ad + bc$. Sea ω una circunferencia de diámetro $\sqrt{p}$. Por el teorema de Pitágoras es posible construir un cuadrilátero convexo $ABCD$ con vértices en ω tal que $AB = a$, $BC = b$, $CD = c$, $DA = d$ y $AC = \sqrt{p}$. Sea $BD = r$ y sea X la intersección de AC y BD. Como $ABCD$ es cíclico, el teorema de Ptolomeo[3] garantiza que $AC \cdot BD = AB \cdot CD + BC \cdot DA$, es decir, $r\sqrt{p} = ac + bd$. Denotemos por $u = BX$, $v = XD$ y $t = AX$.



La ley de senos en el $\triangle AXB$ dice que $\frac{u}{t} = \frac{BX}{AX} = \frac{\text{sen}(\angle BAC)}{\text{sen}(\angle ABD)}$. Pero, por la ley de senos en $\triangle ABD$ y $\triangle ABC$, se tiene que $\frac{b}{\text{sen}(\angle BAC)} = \frac{BC}{\text{sen}(\angle BAC)} = \sqrt{p} =$

[3] Ver en el apéndice el teorema 23.

$\frac{DA}{\operatorname{sen}(\angle ABD)} = \frac{d}{\operatorname{sen}(\angle ABD)}$; entonces, $\frac{b}{d} = \frac{\operatorname{sen}(\angle BAC)}{\operatorname{sen}(\angle ABD)}$. Por tanto, $\frac{u}{t} = \frac{b}{d}$, que equivale a $u = \frac{bt}{d}$. De manera análoga se demuestra que $v = \frac{ct}{a}$. Así, $r = u + v = t\left(\frac{ab+cd}{ad}\right)$. Ahora, por potencia de un punto desde X se tiene que $AX \cdot XC = BX \cdot XD$, es decir, $t(\sqrt{p} - t) = uv = t^2\left(\frac{bc}{ad}\right)$. Entonces, $t = \sqrt{p}\left(\frac{ad}{bc+ad}\right)$. Por tanto, $r = \sqrt{p}\left(\frac{ab+cd}{bc+ad}\right)$. Pero, $r\sqrt{p} = ac + bd$, entonces, $p = \frac{(ac+bd)(ad+bc)}{ab+cd}$. Así, p divide a $ac + bd$ o divide a $ad + bc$. Si p divide a $ac + bd$, entonces $p \leq ac + bd = r\sqrt{p}$, que equivale a $\sqrt{p} \leq r$. No obstante, se sabe que $BD = r$ es una cuerda y $AC = \sqrt{p}$ es un diámetro, entonces $ABCD$ es un rectángulo, que implica que $a = c$ y $b = d$, una contradicción. Ahora, si p divide a $ad + bc$, entonces $p \leq ad + bc \leq ac + bd = r\sqrt{p}$, que equivale a $\sqrt{p} \leq r$; la conclusión se sigue como en el caso anterior. Por tanto, n debe ser compuesto[4]. □

Demostración 2: Sean (a, b) y (c, d) dos soluciones de $x^2+y^2 = n$. Entonces, $a \neq c$ y $a \neq d$. Podemos asumir sin pérdida de generalidad que $a > c$. Entonces, $(a + c)(a - c) = (d + b)(d - b)$. Por tanto, existen enteros m, n, p, q tales que $\operatorname{mcd}(n, p) = 1$, $a + c = mn$, $a - c = pq$, $d + b = mp$, $d - b = nq$. Entonces, $a = \frac{1}{2}(mn + pq)$, $b = \frac{1}{2}(nq+mp)$ y $4n = 4(a^2+b^2) = (mn+pq)^2+(nq+mp)^2 = (m^2+q^2)(n^2+p^2)$. Asuma que n es primo. Entonces, sin pérdida de generalidad, $m^2+q^2 = 2$ o $m^2+q^2 = 4$. En el primer caso $m = q = 1$, lo que implica que $a = d$, que es una contradicción. El segundo es imposible para enteros positivos. Por tanto, n debe ser compuesto. □

El siguiente teorema resuelve el problema del número de representaciones de un entero positivo como suma de dos cuadrados, el lector interesado puede consultar su demostración en el punto 5.10 del libro *Introducción a la teoría de los números* de Ivan Niven y Herbert S. Zuckerman.

Teorema 2: Sea n un entero positivo y escribamos

$$n = 2^{\alpha} \prod_{p \equiv 1 \pmod 4} p^{\beta_p} \prod_{q \equiv 3 \pmod 4} q^{\gamma_q},$$

donde p corre sobre todos los primos de n de la forma $4k + 1$ en el primer producto y q corre sobre todos los primos de n de la forma $4k + 3$ en el segundo producto. Sea $N(n)$ el número de soluciones de $x^2 + y^2 = n$ y sea $Q(n)$ el número de parejas (x, y) de enteros tales que $(x, y) = 1$ y $x^2 + y^2 = n$. Si α es 0 o 1 y todos los γ_q son 0, entonces $Q(n) = 2^{t+2}$ donde t es el número de primos de la forma $4k + 1$ que dividen a n. En otro caso, $Q(n) = 0$. Si todos los γ_q son pares, entonces $N(n) = 4\prod_{p \equiv 1 \pmod 4}(\beta_p + 1)$. En otro caso, $N(n) = 0$.

[4]Esta demostración fue comentada al autor por Pablo Soberón Bravo. La identidad $p = \frac{(ac+bd)(ad+bc)}{ab+cd}$ es un caso particular del siguiente resultado: en un cuadrilátero cíclico $ABCD$, si a, b, c, d, x e y denotan las longitudes de los segmentos AB, BC, CD, DA, AC y BD, respectivamente, entonces $x^2 = \frac{(ac+bd)(ad+bc)}{ab+cd}$ e $y^2 = \frac{(ac+bd)(ab+cd)}{ad+bc}$, una demostración de este resultado se puede consultar en la página 25 del libro *Advanced Trigonometry* de C. V. Durell y A. Robson.

El problema de Waring

Alrededor de 1770, Waring afirmó que todo número natural se puede expresar como suma de 4 cuadrados, 9 cubos, 19 potencias cuartas y así en adelante. El problema que planteaba esa afirmación era que para cada entero positivo k existía un entero positivo s tal que todo número natural se puede expresar como suma de s enteros elevados a la k-ésima potencia. Esto quiere decir que todo número natural n tiene una expresión de la forma:

$$n = x_1^k + x_2^k + \cdots + x_s^k. \tag{5}$$

El siguiente lema demuestra que dado un entero positivo k, un s demasiado pequeño no funcionará.

Lema 4: Dado un entero positivo k, existe un entero que no se puede expresar como suma de $2^k + (\frac{3}{2})^k - 3$ enteros a la k-ésima potencia.

Demostración: Sea $q = (\frac{3}{2})^k$. Considera el número $n = 2^k q - 1 < 3^k$ que solo puede representarse con términos de la forma 1^k y 2^k. Dado que $n = (q-1)2^k + (2^k - 1)1^k$, entonces n requiere $2^k + q - 2$ sumandos a la k-ésima potencia. □

Hilbert probó en 1909 que para cada entero positivo k existía una s tal que la ecuación (5) tiene solución en los enteros para todo natural n. El problema de Waring consiste en encontrar para cada entero positivo k el menor entero s, que se denota como $g(k)$, para el cual la ecuación (5) tiene solución en los enteros para todo natural n. Dicho problema aún está abierto. Hardy se dio cuenta que solo unos números muy especiales necesitaban 9 cubos para poder escribirse como suma de cubos y que, en general, son pocos los números que necesitan $g(k)$ sumandos para escribirse como suma de enteros a la k-ésima potencia. A partir de dicha observación, Hardy planteó el problema de encontrar $G(k)$, el menor valor de s tal que todos los números suficientemente grandes, es decir, con un número finito de excepciones, pueden ser representados como la suma de s enteros elevados a la k-ésima potencia. En particular, $G(k) \leq g(k)$ para todo $k \in \mathbb{N}$. Los siguientes lemas y teoremas se usarán para demostrar que $G(2) = g(2) = 4$.

Lema 5: Sea $n \in \mathbb{N}$ tal que $n \equiv 7 \pmod 8$, entonces, n no se puede representar como suma de tres cuadrados.

Demostración: Con un simple cálculo de los diferentes casos se demuestra que todo cuadrado de un entero módulo 8 es congruente a 0, 1 o 4. Así, si $x, y, z \in \mathbb{Z}$, entonces $x^2 + y^2 + z^2 \equiv 0, 1, 2, 3, 4, 5$ o $6 \pmod 8$. En ningún caso $x^2 + y^2 + z^2 \equiv 7 \pmod 8$. □

Lema 6: Si p es un primo impar, entonces existen enteros x, y y m con $0 < m < p$, tales que $1 + x^2 + y^2 = mp$.

Demostración: Si x_1, x_2 son dos enteros positivos tales que $x_1^2 \equiv x_2^2 \pmod{p}$, entonces $(x_1 - x_2)(x_1 + x_2) \equiv 0 \pmod{p}$, por tanto $x_1 \equiv \pm x_2 \pmod{p}$. Así, para $x = 0, 1, \ldots, \frac{p-1}{2}$, los números x^2 serán todos diferentes módulo p. De la misma manera, para $y = 0, 1, \ldots, \frac{p-1}{2}$, los números $-1 - y^2$ serán todos diferentes módulo p. Dado que hay $p + 1$ números entre los elementos de ambos conjuntos y solo p congruencias distintas módulo p, debe existir un entero $x \in \{0, 1, \ldots, \frac{p-1}{2}\}$ y un entero $y \in \{0, 1, \ldots, \frac{p-1}{2}\}$ tales que $x^2 \equiv -1 - y^2 \pmod{p}$, entonces $x^2 + 1 + y^2 = mp$, para algún entero positivo m. Sin embargo, $x^2 < \left(\frac{p}{2}\right)^2$ y $y^2 < \left(\frac{p}{2}\right)^2$, entonces $mp = x^2 + 1 + y^2 < 1 + 2 \cdot \left(\frac{p}{2}\right)^2 < p^2$; por tanto, $m < p$. □

Para probar el siguiente lema es necesario introducir una técnica clásica para la resolución de ecuaciones diofantinas: el método de descenso infinito de Fermat. También será necesario introducir la identidad de Euler.

Método de descenso infinito de Fermat: Sea k un entero que no es negativo. Sea P una propiedad sobre los enteros no negativos y sea $(P(n))_{n \geq 1}$ la secuencia de proposiciones dada por: $P(n) =$ "n satisface la propiedad P". Suponga que siempre que $P(m)$ es verdadero para un entero $m > k$, entonces existe un entero j, con $m > j > k$, para el cual $P(j)$ es verdadero. Entonces, $P(n)$ es falso para todo $n > k$. Se llama descenso infinito porque si $P(n)$ fuera cierto para $n > k$, entonces sería posible construir una secuencia $n > n_1 > n_2 > \cdots$ de enteros tales que todos son mayores que k. Sin embargo, esa clase de secuencias infinitas decrecientes no existen en los enteros que no son negativos.

Identidad de Euler Si $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \in \mathbb{R}$, entonces

$$\begin{aligned}&(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) + \\ &= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ &\quad + (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2.\end{aligned}$$

Lema 7: Si p es un primo impar, entonces existen enteros x, y, z, w tales que $p = x^2 + y^2 + z^2 + w^2$.

Demostración: Por el lema 6, para todo primo impar p, debe existir un entero m tal que $0 < m < p$ y que $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Se debe probar que el menor entero m que cumple las propiedades anteriores es $m = 1$. Sea m_0 el menor entero que cumple las dos propiedades anteriores. Suponga que $1 < m_0 < p$. Si m_0 es par, entonces por paridad todos tienen la misma paridad o dos son pares y dos son impares. Sin pérdida de generalidad, x_1 y x_2 tienen la misma paridad, entonces los cuatro números $x_1 \pm x_2$ y $x_3 \pm x_4$ son pares. Por tanto,

$$\frac{m_0}{2} \cdot p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2$$

lo que contradice que m_0 era mínimo. Así, m_0 es impar.
Dado que todo entero es congruente módulo m_0 a un elemento del conjunto:

$$\left\{-\frac{m_0-1}{2}, -\frac{m_0-3}{2}, \ldots, \frac{m_0-3}{2}, \frac{m_0-1}{2}\right\},$$

es posible escoger y_i, con $i \in \{1,2,3,4\}$, tal que $y_i \equiv x_i \pmod{m_0}$ y $\mid y_i \mid < \frac{m_0}{2}$. Ahora, si m_0 divide a todos los enteros x_i, entonces m_0^2 dividiría a $m_0 p$, lo que implicaría que m_0 dividiría a p, lo cual es una contradicción. Por tanto, $y_1^2+y_2^2+y_3^2+y_4^2 > 0$. Así, $y_1^2+y_2^2+y_3^2+y_4^2 < m_0^2$ y $y_1^2+y_2^2+y_3^2+y_4^2 \equiv 0 \pmod{m_0}$, lo que implica que $y_1^2+y_2^2+y_3^2+y_4^2 = m_0 m_1$ con $0 < m_1 < m_0$. Pero, $m_0 p = x_1^2+x_2^2+x_3^2+x_4^2$, entonces la identidad de Euler garantiza que existen enteros z_i, con $i \in \{1,2,3,4\}$, tales que

$$m_1 m_0^2 p = z_1^2+z_2^2+z_3^2+z_4^2. \tag{6}$$

Sin embargo, $z_1 = x_1y_1+x_2y_2+x_3y_3+x_4y_4 \equiv x_1^2+x_2^2+x_3^2+x_4^2 \equiv 0 \pmod{m_0}$. De manera análoga se demuestra que $z_i \equiv 0 \pmod{m_0}$, con $i \in \{2,3,4\}$. Por tanto, es posible escribir $z_i \equiv m_0 w_i$, con $i \in \{1,2,3,4\}$. Si se divide la ecuación (6) entre m_0^2, se tiene que $m_1 p = w_1^2+w_2^2+w_3^2+w_4^2$, lo que contradice que m_0 es mínimo. En conclusión, $m_0 = 1$.
El problema $2-b$) y el problema 7 permiten concluir que $G(2) = g(2) = 4$. □

Ejercicios

1) a) Observa que si $(x,y,z) = (x_0,y_0,z_0)$ es solución de la ecuación $z^2 = x^2+y^2$, entonces $(x,y,z) = (kx_0, ky_0, kz_0)$ también es solución para cualquier entero k. ¿Por qué basta con investigar las ternas en las que sus elementos son primos relativos por parejas para encontrar todas las soluciones de la ecuación?

   b) Una solución (x_0,y_0,z_0) de $z^2 = x^2+y^2$ se llama primitiva si x_0, y_0 y z_0 son primos relativos por parejas. Demuestra que $(x_0 = m^2-n^2, y_0 = 2mn, z_0 = m^2+n^2)$, con m y n enteros positivos tales que $m > n$ y $m+n$ impar, es una solución primitiva de $z^2 = x^2+y^2$.

   c) Demuestra que toda solución primitiva de $z^2 = x^2+y^2$ cumple, sin pérdida de generalidad, que $y = 2a$, $z+x = 2b$ y $z-x = 2c$, con a, b y c enteros.

   d) Demuestra que todas las soluciones primitivas de $z^2 = x^2+y^2$ son como en el inciso b).

2) a) Demuestra que hay una infinidad de primos de la forma $4k+3$. Concluye que hay una infinidad de enteros positivos que no se pueden escribir como suma de dos cuadrados.

   b) Demuestra que hay una infinidad de enteros positivos que no se pueden escribir como suma de tres cuadrados.

3) Demuestra que todas las soluciones de la ecuación $x^2+y^2+z^2 = t^2$, donde x, y, z y t son enteros positivos y y y z son pares, están dadas por

$$x^2 = \frac{l^2+m^2-n^2}{n}, \quad y = 2l, \quad z = 2m, \quad t = \frac{l^2+m^2+n^2}{n},$$

para l y m enteros positivos arbitrarios y n cualquier divisor de $l^2 + m^2$ menor que $\sqrt{l^2 + m^2}$. Además, demuestra que cada solución aparece exactamente una vez por la forma en que se describió.

4) (F. Smarandache). Resuelve en los enteros positivos la ecuación

$$(x!)^2 + (y!)^2 = (z!)^2.$$

5) Demuestra que si $x \neq 0, y \neq 0, z \neq 0$, entonces la ecuación $x^4 + y^4 = z^2$ no tiene soluciones en los enteros.

6) (Bulgaria 1999/6). Demuestra que la ecuación $x^3 + y^3 + z^3 + t^3 = 1999$ tiene infinitas soluciones en los enteros.

7) (Teorema de Lagrange). Demuestra que todo entero positivo se puede escribir como suma de cuatro cuadrados.

8) Se tardó mucho en descubrir que la ecuación $x^3 + y^3 + z^3 = 30$ tiene soluciones. La solución más pequeña es $(-283059965, -2218888517, 2220422932)$ y fue descubierta en 1999 por E. Pine, K. Yarbrough, W. Tarrant y M. Beck al seguir una sugerencia de N. Elkies. Decidir si la ecuación $x^3 + y^3 + z^3 = 33$ tiene soluciones es un problema abierto. Pese a la dificultad de estos problemas, es posible descartar fácilmente algunos valores de x, y, z. Demuestra que la ecuación $x^3 + y^3 + z^3 = 30$ no tiene soluciones si:

   a) $x, y, z > 0$.

   b) $x < 0, y > 0$ y $z > 0$.

9) (IMO 2001/6). Sean a, b, c, d enteros con $a > b > c > d$. Supón que

$$ac + bd = (b + d + a - c)(b + d - a + c).$$

   Demuestra que $ab + cd$ no es primo.

10) El propósito de este problema es demostrar el caso $n = 3$ del famoso teorema de Fermat. Dicho teorema establece que la ecuación $x^n + y^n = z^n$ no tiene soluciones en los enteros positivos si $n > 2$. Fue demostrado en su versión general por Andrew Wiles en 1995 con la ayuda de Richard Taylor.

    a) Reduce el problema mediante un cambio de variables a demostrar que $w^3 = 2u(u^2 + 3v^2)$ no tiene soluciones en los enteros positivos.

    b) Demuestra que si mcd$(a, b) = 1$, entonces cada factor de $a^2 + 3b^2$ es de la forma $d^2 + 3c^2$.

    c) ¿Cuánto puede valer mcd$(2u, 3v^2)$?

    d) Resuelve los dos casos posibles con descenso infinito.

Bibliografía

1) Andreescu T., Andrica D., Cucurezeanu I. *An Introduction to Diophantine Equations: A Problem-Based Approach*, Birkhäuser, 2010.

2) Bhaskar J. *Sum of Two Squares*, 2008.

3) Clark P. L. *Thue-Vinogradov and Integers of the Form* $x^2 + Dy^2$, 2011.

4) Dietmann R., Elsholtz C. *Sums of Two Squares and One Biquadrate*.

5) Durell C. V., Robson A. *Advanced Trigonometry*, Dover Publications, 2003.

6) Gómez Ortega J. A., Valdez Delgado R., Vázquez Padilla R. *Principio de las casillas*. Cuadernos de Olimpiadas de Matemáticas. Instituto de Matemáticas de la UNAM, 2014.

7) Hardy G. H., Wright E. M. *An Introduction to the Theory of Numbers*. Oxford University Press, 1975.

8) Lalín M. N. *Every Positive Integer is the Sum of Four Squares! (and other exciting problems)*, 2002.

9) Niven I., Zuckerman H. S. *Introducción a la teoría de los números*. Editorial Limusa, 1969.

10) Niven I., Zuckerman H. S., Montgomery H. L. *An Introduction to the Theory of Numbers*. John Wiley & Sons, 1991.

11) Pérez Seguí M. L. *Teoría de números*. Cuadernos de Olimpiadas de Matemáticas. Instituto de Matemáticas de la UNAM, 2011.

12) Sandor J. *Selected Chapters of Geometry, Analysis and Number Theory: Classical Topics in New Perspectives*, LAP Lambert Academic Publishing, 2009.

13) Santos D. A. *Number Theory for Mathematical Contests*, 2005.