UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

Ecuaciones Diofantinas III: Sumas de Cuadrados

Alan Reyes-Figueroa

Teoría de Números

(Aula 30) 18.octubre.2024

Sumas de dos Cuadrados

Caracterizamos los números que son sumas de dos cuadrados.

Teorema

Los únicos números que pueden expresarse como suma de dos cuadrados son los de la forma $n = 2^s d^2 \ell$, donde $s \in \mathbb{N}$ y ℓ es libre de cuadrados tales que su factores primos son de la forma $4k + 1$.

Prueba: Comenzamos observando que si p es un primo de la forma $4k + 3$ que divide a $n = a^2 + b^2$, entonces $p \mid a$ y $p \mid b$.
De hecho, si esto no ocurriese, b sería invertible módulo p. Luego, de $a^2 \equiv -b^2 \pmod{p}$, tendríamos que $(ab^{-1})^2 \equiv a^2 b^{-2} \equiv -1 \pmod{p}$ y -1 sería un residuo cuadrático módulo p, lo cual es imposible pues $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k+2}{2}} = (-1)^{2k+1} = -1$.

Luego, $p^2 \mid a^2$, $p^2 \mid b^2 \Rightarrow p^2 \mid n$. Repitiendo el proceso son $\frac{n}{p^2} = (\frac{a}{p})^2 + (\frac{b}{p})^2$ en lugar de n, se concluye que todo primo de la forma $4k + 3$ aparece con exponente par en la factoración de n.

Sumas de dos Cuadrados

Ahora, todo natural n puede expresarse como $n = k^2 m$, donde $k, m \in \mathbb{Z}^+$ y m es libre de cuadrados.
Si $m = a^2 + b^2$, es suma de cuadrados, entonces lo mismo ocurre para $n = (ka)^2 + (kb)^2$.
Además, si $m = a^2 + b^2$ y $n^2 = c^2 + d^2$, entonces

$$\begin{aligned} mn &= (a^2 + b^2)(c^2 + d^2) = |a + bi|^2 \cdot |c + di|^2 = |(a + bi)(c + di)|^2 \\ &= |(ac - db) + (ad + bc)i|^2 = (ac - bd)^2 + (ad + bc)^2. \end{aligned}$$

y el producto también es suma de dos cuadrados. Así, para mostrar que todo natural n de la forma descrita en el teorema es suma de dos cuadrados, basta mostrar que 2 y que todo primo impar de la forma $4k + 1$ es suma de dos cuadrados. Para el caso $p = 2$, tenemos que $2 = 1^2 + 1^2$. En el otro caso, precisamos del siguiente resultado.

Lema (Lema de Thue)

Si $m > 1$ es un número natural, y $a \in \mathbb{Z}$ es tal que $(a, m) = 1$, entonces existen naturales $x, y \in \mathbb{N}$, con $0 < x, y \leq \sqrt{m}$, tales que alguno de los números $ax \pm y$ es múltiplo de m.

Sumas de dos Cuadrados

Prueba: Sea $q = \lfloor \sqrt{m} \rfloor$. Entonces $q + 1 > \sqrt{m}$ y portanto $(q+1)^2 > m$. Consideramos todos los $(q+1)^2$ números de la forma $ax - y$, donde x y y toman valores $0, 1, \ldots, q$. Como sólo existen m residuos al dividir entre m, por el Principio de Dirichlet, existen al menos dos de los números anteriores, digamos $ax_1 - y_1$ y $ax_2 - y_2$ son congruentes módulo m.

Luego, la diferencia $m \mid a(x_1 - x_2) + (y_1 - y_2) = (ax_1 - y_1) - (ax_2 - y_2)$. Tenemos además, $0 \leq x_i, y_i \leq \sqrt{m} \Rightarrow |x_1 - x_2|, |y_1 - y_2| \leq \sqrt{m}$. Así,

- $x_1 = x_2 \Rightarrow x_1 - x_2 = 0$, entonces $m \mid y_1 - y_2$, lo que implica $y_1 = y_2$, un absurdo, pues los pares (x_1, y_1), (x_2, y_2) son distintos.
- $y_1 = y_2 \Rightarrow y_1 - y_2 = 0$, entonces $m \mid a(x_1 - x_2)$. Como $(a, m) = 1$, entonces $m \nmid a$ y se tiene que $m \mid x_1 - x_2$, lo que implica $x_1 = x_2$, de nuevo un absurdo, pues los pares (x_1, y_1), (x_2, y_2) son distintos.

Por lo tanto, los números $x = |x_1 - x_2|$ y $y = |y_1 - y_2|$ cumplen con la condición requerida.

□

Sumas de dos Cuadrados

Retomando el teorema inicial, si p es un primo de la forma $4k+1$, entonces $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k}{2}} = (-1)^{2k} = 1$, Luego, existe $a \in \mathbb{Z}$ tal que $a^2 \equiv -1 \pmod{p}$, de modo que $p \mid a^2+1$.

Aplicando el Lema de Thue, existen enteros $0 < x, y \leq \sqrt{p}$ tales que alguno de los números $ax \pm y$ es divisible entre p. De ahí que $p \mid (ax-y)(ax+y) = a^2x^2 - y^2$,

$$\implies \quad p \mid x^2(a^2+1) - (a^2x^2 - y^2) = x^2 + a^2x^2 - a^2x^2 + y^2 = x^2 + y^2.$$

Como $0 < x, y < \sqrt{p}$, entonces $0 < x^2 + y^2 < 2p$, de modo que $p = x^2 + y^2$. Esto encierra la prueba del teorema. $\square$

Comentarios: Existen otras demostraciones del Lema de Thue. Veremos una de estas cuando hablemos de teoría algebraica de números.

Sumas de dos Cuadrados

El método anterior puede aplicarse para obtener otras representaciones de números primos.

Ejemplo: Sean $d \in \{1, 2, 3, 7\}$ y p un número primo impar tal que $(\frac{-d}{p}) = 1$. Entonces, existen $e, f \in \mathbb{N}$ tales que $p^2 = e^2 + df^2$.

Solución: Sea $a \in \mathbb{N}$ tal que $a^2 \equiv -d \pmod{p}$. Por el Lema de Thue, existen enteros $x, y \in \mathbb{Z}$ tales que $(x + ay)(x - ay) \equiv 0 \pmod{p} \iff p \mid x^2 + dy^2$. Como $0 << x^2 + dy^2 < (d + 1)p$, entonces tenemos

$$x^2 + dy^2 = kp, \qquad \text{con } k \in \{1, 2, \ldots, d\}.$$

Sumas de cuatro Cuadrados

Una pregunta natural es la siguiente: ¿cuántos cuadrados son necesarios sumar para representar cualquier entero positivo n?. Bachet conjeturó que todo natural $n \in \mathbb{N}$ puede representarse como suma de a lo sumo cuatro cuadrados. Esta conjetura fue provada por Fertmat, usando su método del descenso. Veremos a continuación una prueba debido a Lagrange en 1770, usando una identidad de Euler.

Lema (Identidad de Euler)

Para todo $a, b, c, d, w, x, y, z \in \mathbb{Z}$, se tiene que

$$\begin{aligned}(a^2+b^2+c^2+d^2)(w^2+x^2+y^2+z^2) &= (aw+bx+cy+dz)^2+(ax-bw-cz+dy)^2+\\ &\quad +(ay+bz-cw-dx)^2+(az-by+cx-dw)^2.\end{aligned}$$

Prueba: Consideramos la siguiente identidad entre matrices complejas en $\mathbb{C}^{2\times 2}$:

$$\begin{pmatrix}\alpha & \beta\\ -\bar{\beta} & \bar{\alpha}\end{pmatrix}\begin{pmatrix}\gamma & \delta\\ -\bar{\delta} & \bar{\gamma}\end{pmatrix}=\begin{pmatrix}\alpha\gamma-\beta\bar{\delta} & \alpha\delta+\beta\bar{\gamma}\\ -\overline{\alpha\delta+\beta\bar{\gamma}} & \overline{\alpha\gamma-\beta\bar{\delta}}\end{pmatrix}.$$

Sumas de cuatro Cuadrados

Calculando los determinantes, obtenemos

$$(|\alpha|^2 + |\beta|^2)(|\gamma|^2 + |\delta|^2) = |\alpha\gamma - \beta\bar{\delta}|^2 + |\alpha\delta + \beta\bar{\gamma}|^2.$$

Haciendo $\alpha = a - bi$, $\beta = -c - di$, $\gamma = w + xi$, $\delta = y + zi$. Se obtiene la identidad. $\square$

Esta identidad se entiende de forma más natural si utilizamos *cuaterniones*. Recordemos que el conjunto de los cuaterniones es $\mathbb{R}^4$, con la suma usual y la norma euclideana, donde escribimos $(a, b, c, d) = a + bi + cj + dk$, y definimos el producto

$$i^2 = j^2 = k^2 = -1, \qquad ij = -ji = k, \qquad jk = -kj = i, \qquad ki = -ik = j.$$

En este caso, la identidad de Euler se traduce como $|zw| = |z| \cdot |w|$, con z, w cuaterniones.

Más aún, si identificamos el cuaternio $a + bi + cj + dk$ con la matriz

$$\begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}$$

obtenemos una identificación entre cuaterniones y las matrices usadas en la prueba.

Lema

Si $2m$ es suma de dos cuadrados, entonces m es suma de dos cuadrados.

Prueba: Como $2m = x^2 + y^2$, entonces x, y tienen la misma paridad. Luego

$$m = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2. \ \square$$

Lema

Si p es un primo impar, entonces existen $a, b, k \in \mathbb{Z}$ tales que $a^2 + b^2 + 1 = kp$.

Prueba: Considere los conjuntos

$$A = \{a^2 \in \mathbb{Z}/p\mathbb{Z} : \ 0 \leq a \leq \tfrac{p-1}{2}\}, \qquad B = \{-b^2 - 1 \in \mathbb{Z}/p\mathbb{Z} : \ 0 \leq b \leq \tfrac{p-1}{2}\}.$$

Cada conjunto posee $\frac{p+1}{2}$ elementos de $\mathbb{Z}/p\mathbb{Z}$, de modo que $A \cap B \neq 0$, esto es, existen a, b tales que $a^2 + b^2 + 1 \equiv 0 \pmod{p}$. $\square$

Teorema (Prueba de Lagrange)

Todo entero positivo n puede escribirse como suma de cuatro cuadrados.

Prueba: De la identidad de Euler, basta mostrar el resultado para los números primos.

Observe que $2 = 1^2 + 1^2 = 1^2 + 1^2 + 0^2 + 0^2$ es suma de cuatro cuadrados. Nos limitamos al caso p primo impar. Ahora, por el lema anterior, sabemos que existen $a, b, c, d, m \in \mathbb{Z}$, con $m > 0$, tales que $mp = a^2 + b^2 + c^2 + d^2$ (aquí se toma $c = 1$ y $d = 0$).

Para completar la prueba, basta mostrar que si $m > 1$, entonces existe $0 < n < m$ tal que np se puede escribir como suma de cuatro cuadrados.

- Si m es par, entonces ninguno, dos o cuatro de los números a, b, c, d son pares. Aplicando el primer lema, basta tomar $n = \frac{m}{2}$, pues

$$np = \frac{m}{2}p = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2$$

(basta agrupar términos del mismo signo).

Sumas de cuatro Cuadrados

- Si m es impar, $m > 1$, sean w, x, y, z enteros tales que

$$w \equiv a \pmod{m}, \qquad x \equiv b \pmod{m}, \qquad y \equiv c \pmod{m}, \qquad z \equiv d \pmod{m},$$

donde $w, x, y, z \in (-\frac{m}{2}, \frac{m}{2})$. Luego,

$$w^2 + x^2 + y^2 + z^2 < 4 \cdot \frac{m^2}{4} = m^2 \qquad \text{y} \qquad w^2 + x^2 + y^2 + z^2 \equiv 0 \pmod{m}.$$

Portanto, $w^2 + x^2 + y^2 + z^2 = nm$, con $0 < n < m$. Debido a la elección de w, x, y, z, tenemos que los números $ax - bw - cz + dy$, $ay + bz - cw - dx$ y $az - by + cx - dw$ son divisibles entre m, y $aw + bx + cy + dz \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m}$. Aplicando el primer lema,

$$\begin{aligned} np &= \frac{1}{m^2}(mp)(nm) = \frac{1}{m^2}(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) \\ &= \left(\tfrac{aw+bx+cy+dz}{m}\right)^2 + \left(\tfrac{ax-bw-cz+dy}{m}\right)^2 + \left(\tfrac{ay+bz-cw-dx}{m}\right)^2 + \left(\tfrac{az-by+cx-dw}{m}\right)^2 \end{aligned}$$

es suma de cuatro cuadrados. □

El Problema de Waring

En general, para $n \in \mathbb{N}$, podemos preguntarnos si existe un enter positivo $s = s(n)$, que depende de n, tal que cualquier número natural se escribe como suma de a lo sumo s n-ésimas potencias. Este problema se conoce como el **problema de** Waring, y fue respondido afirmativamente por Hilbert en 1909.

Denotemos por $g(n)$ el menor de estos números s. El teorema anterior muestra que $g(2) \leq 4$, de hecho, $g(2) = 4$ pues se puede mostrar que ningún número de la forma $4^k(8t + 7)$ se puede escribir como suma de tres cuadrados.

Se conocen algunos otros valores para $g(n)$:

- $g(2) = 4$ (Fermat, Lagrange, Gauss).
- $g(3) = 9$ (Wieferich, Kempner).
- $g(4) = 19$ (Balasubramanian, Dress, Deshoulliers).
- $g(5) = 37$ (Jungrun).
- $g(6) = 73$ (Pillai).

El Problema de Waring

En general, se tiene la siguiente

Conjetura (Euler)

Para todo $n \geq 2$, vale

$$g(n) = 2^n + \left\lfloor \left(\frac{3}{2}\right)^n \right\rfloor - 2.$$

Se puede demostrar que

Teorema (Euler)

Para todo $n \geq 2$, vale

$$g(n) \geq 2^n + \left\lfloor \left(\frac{3}{2}\right)^n \right\rfloor - 2.$$

Prueba: Consideremos el número $m = 2^n \left\lfloor (\frac{3}{2})^n \right\rfloor - 1$, y escribámoslo como suma de n-ésimas potencias. Como $m < 3^n$, en esta suma sólo pueden aparecer potencias de 1 ó 2.

El Problema de Waring

Sea k el número de potencias de 2 en esta suma. Tenemos que $m - 2^n k$ términos son iguales a 1, de modo que hay $(m - 2^n k) + k = m - (2^n - 1)k$ términos en total.

Por otro lado, como $k \leq \left\lfloor (\frac{3}{2})^n \right\rfloor - 1$, se tiene

$$\begin{aligned} m - (2^n - 1)k &\geq \left(2^n \left\lfloor \left(\frac{3}{2}\right)^n \right\rfloor - 1\right) - (2^n - 1)\left(\left\lfloor \left(\frac{3}{2}\right)^n \right\rfloor - 1\right) \\ &\geq 2^n + \left\lfloor \left(\frac{3}{2}\right)^n \right\rfloor - 2. \quad \square \end{aligned}$$

Sumas de tres Cuadrados

El siguiente teorema, demostrado por GAUSS, muestra cuándo un número es suma de tres cuadrados.

Teorema (Teorema de los 3 Cuadrados de Gauss)

Un entero $n \geq 0$ es suma de tres cuadrados si, y sólo si, n no es de la forma $4^a(8b+7)$, con $a, b \in \mathbb{N}$.

Prueba: () Observe inicialmente que $k^2 \equiv 0, 1, 4 \pmod 8$, para todo $k \in \mathbb{Z}$. En consecuencia, una suma de tres cuadrados no puede ser congruente a $7 \pmod 8$.

Además, si $x, y, z \in \mathbb{Z}$ son tales que $x^2 + y^2 + z^2 \equiv 0 \pmod 4$, entonces x, y, z deben ser pares.
Luego, si $x^2 + y^2 + z^2 = 4^a(8b+7)$, tenemos que $x = 2\bar{x}$, $y = 2\bar{y}$, $z = 2\bar{z}$, y
$4(\bar{x}^2+\bar{y}^2+\bar{z}^2) = (2\bar{x})^2+(2\bar{y})^2+(2\bar{z})^2 = x^2+y^2+z^2 = 4^a(8b+7) \quad \Rightarrow \quad \bar{x}^2+\bar{y}^2+\bar{z}^2 = 4^{a-1}(8b+7)$.

y usando esto repetidamente, entonces $2^a \mid (x, y, z)$; y luego
$\left(\frac{x}{2^a}\right)^2 + \left(\frac{y}{2^a}\right)^2 + \left(\frac{z}{2^a}\right)^2 = 8b + 7 \equiv 7 \pmod 8$, lo que es un absurdo.

($\Leftarrow$) Para mostrar la suficiencia, primero demostramos el siguiente

Lema

Si $n \in \mathbb{N}$ es supa de tres cuadrados de números racionales, entonces n es suma de tres cuadrados enteros.

Prueba: Sea $n = x_1^2 + x_2^2 + x_3^2$, con $x_1, x_2, x_3 \in \mathbb{Q}$. Sean $x_1 = \frac{p_1}{q}, x_2 = \frac{p_2}{q}, x_3 = \frac{p_3}{q}$, con q un denominador común para x_1, x_2, x_3, entonces $q^2 n = p_1^2 + p_2^2 + p_3^2$.

Sea $d > 0$ el menor entero positivo para el cual existen $y_1, y_2, y_3 \in \mathbb{N}$ con

$$d^2 n = y_1^2 + y_2^2 + y_3^2.$$

Queremos mostrar que $d = 1$. Supongamos, por absurdo, que $d > 1$. Escribiendo $y_1 = dy_1' + z_1$, $y_2 = dy_2' + z_2$, $y_3 = dy_3' + z_3$, con $y_i', z_i \in \mathbb{Z}$, $|z_i| \leq \frac{d}{2}$ para $i = 1, 2, 3$, definimos

$$a = y_1'^2 + y_2'^2 + y_3'^2 - n, \qquad b = 2(nd - y_1 y_1' - y_2 y_2' - y_3 y_3'), \qquad d' = ad + b, \qquad y_i'' = a y_i + b y_i'.$$

Sumas de tres Cuadrados

Entonces

$$\begin{aligned}\sum_{1\le i\le 3}(y_i'')^2 &= a^2\sum_{1\le i\le 3}y_i^2 + 2ab\sum_{1\le i\le 3}y_iy_i' + b^2\sum_{1\le i\le 3}y_i^2\\ &= a^2d^2n + ab(nd-b) + b^2(a+n) \;=\; (ad+b)^2n = (d')^2n.\end{aligned}$$

y

$$\begin{aligned}dd' &= ad^2+bd \;=\; d^2\Big(\sum_{1\le i\le 3}(y_i'')^2 - n\Big) + 2d\Big(nd - \sum_{1\le i\le 3}y_iy_i'\Big)\\ &= \sum_{1\le i\le 3}y_i^2 - 2d\sum_{1\le i\le 3}y_iy_i' + d^2\sum_{1\le i\le 3}(y_i'')^2 \;=\; \sum_{1\le i\le 3}(y_i-dy_i')^2 \;=\; \sum_{1\le i\le 3}z_i^2 \;\le\; \tfrac{3}{4}d^2.\end{aligned}$$

Luego, $0 < d' \le \frac{3}{4}d < d$, lo que contradice la minimalidad de d. Note que si $d' = 0$, entonces $\sum_{1\le i\le 3}z_i^2 = dd' = 0$, de donde $z_1 = z_2 = z_3 = 0$, y tendríamos que $(y_1')^2 + (y_2')^2 + (y_3')^2 = n$, un absurdo. $\square$