Ecuaciones Diofánticas - Suma de Cuadrados

Pablo S. Herrera

Universidad del Valle de Guatemala

24 de octubre de 2025

Suma de cuadrados I

Teorema 1. *Un número n no puede escribirse como suma de dos cuadrados si y sólo si, en su factorización en primos, aparece al menos un primo congruente con 3 módulo 4 elevado a una potencia impar.*

Demostración. Supongamos que p es un primo tal que $p \equiv 3 \pmod 4$ y que aparece en la factorización de n con exponente impar. Es decir, existe $e \geq 0$ tal que

$$p^{2e+1} \mid n \quad \text{y} \quad p^{2e+2} \nmid n. \tag{1}$$

Supongamos, por contradicción, que $n = x^2 + y^2$ para algunos enteros x, y.
Sea $d = (x, y)$ y definamos:

$$x_1 = \frac{x}{d}, \qquad y_1 = \frac{y}{d}, \qquad n_1 = \frac{n}{d^2}. \tag{2}$$

Entonces

$$x_1^2 + y_1^2 = n_1, \qquad (x_1, y_1) = 1. \tag{3}$$

Suma de cuadrados II

Si p^f es la mayor potencia de p que divide a d, entonces n_1 es divisible por $p^{2e-2f+1}$. Este exponente es impar y al menos 1, así que $p \mid n_1$.
Si $p \mid x_1$, de (3) se deduce $p \mid y_1$, lo cual contradice $(x_1, y_1) = 1$. Por tanto, $p \nmid x_1$, y existe un número u tal que

$$x_1 u \equiv y_1 \pmod{p}. \tag{4}$$

Reemplazando en (3):

$$0 = x_1^2 + y_1^2 \equiv x_1^2 + (x_1 u)^2 = x_1^2(1 + u^2) \pmod{p}. \tag{5}$$

Como $(x_1, p) = 1$, se cancela x_1^2 y queda

$$1 + u^2 \equiv 0 \pmod{p}. \tag{6}$$

Esto implica que -1 es un residuo cuadrático módulo p, lo cual es imposible pues $p \equiv 3 \pmod 4$. Por tanto, $n = x^2 + y^2$ es imposible. ■

Suma de cuadrados III

Esta parte demuestra una dirección del teorema. Para completar la doble implicación, presentaremos ahora cuatro lemas esenciales.

Lema 1.

$$(x^2 + y^2)(w^2 + z^2) = (xw + yz)^2 + (xz - yw)^2, \quad \forall x, y, w, z \in \mathbb{Z}. \tag{7}$$

Este lema muestra que si dos números pueden escribirse como suma de dos cuadrados, entonces también su producto puede representarse de la misma forma.

Lema 2. *Si n se puede expresar como suma de dos cuadrados, entonces lo mismo ocurre con $k^2 n$, para todo $k \in \mathbb{Z}$.*

Demostración. Si $n = x^2 + y^2$, entonces

$$k^2 n = (kx)^2 + (ky)^2. \tag{8}$$

■

Suma de cuadrados IV

Lema 3. *Todo número entero positivo n puede escribirse como*

$$n = k^2 \prod_{i=1}^{r} p_i, \tag{9}$$

donde k es un entero y los p_i son primos distintos.

Lema 4. *Todo primo congruente con 1 módulo 4 puede escribirse como la suma de dos cuadrados.*

Si $p \equiv 1 \pmod 4$, existen enteros x, y tales que

$$x^2 + y^2 = kp, \tag{10}$$

para algún $k \geq 1$. Si $k = 1$, la prueba está completa. Si $k > 1$, construiremos nuevos x_1, y_1 tales que

$$x_1^2 + y_1^2 = k_1 p, \quad \text{con } k_1 < k. \tag{11}$$

Suma de cuadrados V

Demostración. Como $p \equiv 1 \pmod 4$, -1 es un residuo cuadrático módulo p. Por tanto, existe u tal que

$$u^2 \equiv -1 \pmod p. \tag{12}$$

De esto se sigue que

$$u^2 + 1 = kp. \tag{13}$$

Definamos s, t tales que:

$$s \equiv x \pmod k, \quad t \equiv y \pmod k, \quad s, t \in \left(-\tfrac{k}{2}, \tfrac{k}{2}\right). \tag{14}$$

Entonces

$$s^2 + t^2 \equiv x^2 + y^2 \equiv 0 \pmod k, \tag{15}$$

de modo que $s^2 + t^2 = k_1 k$ para algún k_1 entero. Usando el **Lema 1**, se cumple:

$$(s^2 + t^2)(x^2 + y^2) = (sx + ty)^2 + (sy - tx)^2 = k_1 k^2 p. \tag{16}$$

Suma de cuadrados VI

Como k divide a ambos términos, definimos:

$$x_1 = \frac{sx + ty}{k}, \quad y_1 = \frac{sy - tx}{k}, \tag{17}$$

y obtenemos la ecuación (11).
Además, $s^2 + t^2 \leq \frac{k^2}{2}$, lo que implica $k_1 < k$. Así, por descenso, se obtiene $k = 1$ y el resultado se cumple. ■

Demostración. [Final del Teorema] Por el **Lema 3**, todo n puede escribirse como

$$n = k^2 \cdot 2^{\alpha} \cdot \prod_{q \equiv 1 (\mathrm{mod}\ 4)} q^{\beta_q}, \tag{18}$$

donde $\alpha, \beta_q \in \{0, 1\}$.
Por el **Lema 4**, cada primo $q \equiv 1 \pmod 4$ puede expresarse como suma de dos cuadrados, y $2 = 1^2 + 1^2$ también cumple esa propiedad.

Suma de cuadrados VII

Por el **Lema 1**, el producto de números con esa propiedad vuelve a tenerla. Finalmente, por el **Lema 2**, multiplicar por k^2 no altera la forma de suma de cuadrados.
Por lo tanto, n puede escribirse como suma de dos cuadrados. Esto completa la contrapuesta y, por tanto, el teorema. ■

Introducción al Teorema de Lagrange

De lo anterior surge la pregunta. Si hay ciertos números que puedo representar como suma de dos cuadrados ¿Podría representar más números como sumas de más cuadrados?

Introducción al Teorema de Lagrange

De lo anterior surge la pregunta. Si hay ciertos números que puedo representar como suma de dos cuadrados ¿Podría representar más números como sumas de más cuadrados?

La respuesta es sí y el teorema de Lagrange es el teorema que no solo nos afirma la representación de enteros como sumas de cuadrados, pero también nos indica que son específicamente 4 cuadrados los necesarios para representar a cualquier número entero.

Suma de cuatro cuadrados I

Formalmente el teorema de Lagrange dice lo siguiente:

Teorema Cuatro cuadrados de Lagrange.
Para un número entero positivo n cualquiera, n puede expresarse como la suma de cuatro cuadrados.

Ejemplos

$$3 = 1^2 + 1^2 + 1^2 + 0^2$$

$$5 = 2^2 + 1^2 + 0^2 + 0^2$$

$$23 = 1^2 + 2^2 + 3^2 + 3^2$$

Para demostrar este teorema es necesario algunos lemas previos para facilitar la demostración.

Suma de cuatro cuadrados II

Como Primer lema para la suma de cuatro cuadrados, se tiene la siguiente identidad. Tal identidad fue descubierta por Euler y nos dice que la representación en cuatro cuadrados se mantiene si multiplicamos dos números con representación en cuatro cuadrados.

Lema Identidad de Euler.

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

Demostración. Se puede verificar el resultado multiplicando simplemente ambos términos o bien, hay una demostración más directa utilizando matrices complejas.

Suma de cuatro cuadrados III

Consideremos la siguiente identidad de matrices complejas.

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

al calcular el determinante de la matriz resultante se obtiene

$$|\alpha\gamma - \beta\bar{\delta}|^2 + |\alpha\delta + \beta\bar{\gamma}|$$

al hacer $\alpha = x_1 - ix_2$, $\beta = -x_3 - ix_4$, $\gamma = y_1 + iy_2$, $\delta = y_3 + iy_4$ se obtiene la identidad. ■

Suma de cuatro cuadrados IV

Lema 5. *Si $2m$ es una suma de dos cuadrados entonces m también es suma de dos cuadrados.*

Demostración. En primer lugar, notese que si $2m = x^2 + y^2$ entonces x, y tienen la misma paridad. Ahora vea lo siguiente:

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

■

Lema 6. *Si p es un primo impar entonces existen a, b, k tales que $a^2 + b^2 + 1 = kp$*

Demostración. Considere los conjuntos

$$A = \{a^2 \in \mathbb{Z}/p\mathbb{Z} \ni 0 \leq a \leq \frac{p-1}{2}\}$$

Suma de cuatro cuadrados V

$$B = \{-b^2 - 1 \in \mathbb{Z}/p\mathbb{Z} \ni 0 \leq b \leq \frac{p-1}{2}\}$$

Cada conjunto posee $\frac{p+1}{2}$ elementos de módulo p, de modo que $A \cap B \neq \emptyset$. Por lo que habrá $a^2 \equiv -b^2 - 1 \bmod p$. Lo que es equivalente a decir que $a^2 + b^2 + 1 \equiv 0 \bmod p$. ■

Veamos un ejemplo, tomemos $p = 13$, entonces $\frac{p-1}{2} = \frac{13-1}{2} = 6$. Entonces aqui $0 \leq a, b \leq 6$.

a	a^2	a^2 mód 13
0	0	0
1	1	1
2	4	4
3	9	9
4	16	3
5	25	12
6	36	10

$$\Rightarrow \quad A = \{0, 1, 3, 4, 9, 10, 12\}.$$

Suma de cuatro cuadrados VI

b	b^2	$-b^2-1$	$(-b^2-1)$ mód 13
0	0	-1	12
1	1	-2	11
2	4	-5	8
3	9	-10	3
4	16	-17	9
5	25	-26	0
6	36	-37	2

$\Rightarrow \quad B = \{0, 2, 3, 8, 9, 11, 12\}.$

$$A = \{0, 1, 3, 4, 9, 10, 12\}, \quad B = \{0, 2, 3, 8, 9, 11, 12\}.$$

Del ejemplo se puede ver que habrán elementos que se intersecten y se puede asegurar la existencia de $a^2 + b^2 + 1 \equiv 0 \bmod p$.

Demostración Teorema de Lagrange I

Ahora que tenemos los lemas necesarios, procedemos a la demostración del teorema de cuatro cuadrados de Lagrange. El enunciado fue mostrado anteriormente en la presentación.

Demostración. Consideremos p un número **primo impar**. Por el lema 6, algún múltiplo de p es suma de dos cuadrados y uno. Es decir $kp = a^2 + b^2 + 1$, para k algún entero mayor o igual que 1.

Definamos $c = 1$ y $d = 0$. Entonces la ecuación anterior se puede reescribir de la siguiente manera:

$$kp = a^2 + b^2 + c^2 + d^2$$

- Si $k = 1$, se trivializa y ya se tiene que p es suma de cuatro cuadrados.
- Veamos el caso en el que $k > 1$

Demostración Teorema de Lagrange II

Caso k es un número par: Si k es par entonces $k = 2n$ para algún entero n. Entonces se tiene lo siguiente:

$$kp = (a+b)^2 + (a-b)^2 + (c+d)^2 + (c-d)^2$$

si sustituimos k se tiene que

$$2np = (a+b)^2 + (a-b)^2 + (c+d)^2 + (c-d)^2$$

Por el lema 5, se tiene que np también será una suma de cuatro cuadrados. Particularmente

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

Demostración Teorema de Lagrange III

Este proceso se repite hasta que el coeficiente que acompañe a p sea un dos, para que al la mitad finalmente se tenga 1 como el coeficiente que acompaña a p y finalmente se tiene que p es la suma de cuatro cuadrados.

Caso k es un número impar: Para este caso consideremos w, x, y, z enteros tales que

$$w \equiv a \ (mod \ k), x \equiv b \ (mod \ k), y \equiv c \ (mod \ k), z \equiv d \ (mod \ k)$$

de tal forma que las nuevos valores estén entre $\left(-\frac{k}{2}, \frac{k}{2}\right)$.

Debido al intervalo donde están las nuevas variables, se cumple que

$$w^2 + x^2 + y^2 + z^2 < 4\left(\frac{k}{2}\right)^2 = k^2$$

y por como definimos las variables

Demostración Teorema de Lagrange IV

$$w^2 + x^2 + y^2 + z^2 \equiv 0 \ (mod \ k)$$

Por lo tanto se tiene que

$$w^2 + x^2 + y^2 + z^2 = nk$$

para algun n entero menor que k. Nuevamente, por la forma en la que definimos las variables se tiene que

$$ax - bw - cz + dy$$

$$ay + bz - cw - dx$$

$$az - by + cx - dw$$

son enteros divisibles entre k. Finalmente como

$$aw + bx + cy + dz \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \ (\text{mod } p)$$

Demostración Teorema de Lagrange V

, por el primer lema, se tiene lo siguiente:

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

■

Notas adicionales

Probablemente se preguntarán ¿Qué pasa en el caso que $p = 2$?
Es sencillo, solamente nótese que

$$2 = 1^2 + 1^2 + 0^2 + 0^2$$

Ejemplos: Representaciones como suma de cuatro cuadrados

Notas adicionales

Probablemente se preguntarán ¿Qué pasa en el caso que $p = 2$?
Es sencillo, solamente nótese que

$$2 = 1^2 + 1^2 + 0^2 + 0^2$$

Ejemplos: Representaciones como suma de cuatro cuadrados

$$7 = 2^2 + 1^2 + 1^2 + 1^2$$

Notas adicionales

Probablemente se preguntarán ¿Qué pasa en el caso que $p = 2$?
Es sencillo, solamente nótese que

$$2 = 1^2 + 1^2 + 0^2 + 0^2$$

Ejemplos: Representaciones como suma de cuatro cuadrados

$$7 = 2^2 + 1^2 + 1^2 + 1^2$$

$$15 = 3 \cdot 5 = (1^2 + 1^2 + 1^2 + 0^2)(2^2 + 1^2 + 0^2 + 0^2) = 3^2 + 1^2 + 2^2 + 1^2$$

Notas adicionales

Probablemente se preguntarán ¿Qué pasa en el caso que $p = 2$?
Es sencillo, solamente nótese que

$$2 = 1^2 + 1^2 + 0^2 + 0^2$$

Ejemplos: Representaciones como suma de cuatro cuadrados

$$7 = 2^2 + 1^2 + 1^2 + 1^2$$

$$15 = 3 \cdot 5 = (1^2 + 1^2 + 1^2 + 0^2)(2^2 + 1^2 + 0^2 + 0^2) = 3^2 + 1^2 + 2^2 + 1^2$$

$$18 = 2 \cdot 3^2 = (1^2 + 1^2 + 0^2 + 0^2)(3^2 + 0^2 + 0^2 + 0^2) = 3^2 + (-3)^2 + 0^2 + 0^2$$

Así, cualquier número compuesto puede representarse también como suma de cuatro cuadrados.

Más alla de las sumas de cuadrados I

Con este gran descubrimiento, la representación de números no quedo solamente en lo que acabamos de ver respecto de cuadrados, pero busco ir mucho más alla.

La motivación de esta investigación era hallar la cantidad mínima posible para representar números como sumas de cuadrados. Gauss en su momento propuso un teorema que hablabla de una caracterización para hallar los números podían representarse como suma de tres cuadrados.

Teorema Sumas de tres Cuadrados de Gauss. *Un entero* $n \geq 0$ *es suma de tres cuadrados sí y sólo sí* n *no es de la forma* $4(8b + 7)$ *para cualesquiera* $a, b \in \mathbb{N}$.

Más alla de las sumas de cuadrados II

La generalización de tal problema fue propuesta por Waring. El enunció que *En general, para cualquier $n \in \mathbb{N}$ ¿Existe un entero positivo $S = S(n)$ tal que cualquier número natural se puede escribir como suma de hasta s n-ésimas potencias?*

El problema conocido popularmente como **El problema de Waring** fue respondido de forma afirmativa por Hilbert en 1909.

Sea $g(n)$ el mínimo de estos números s, es decir, **el mínimo número de potencias necesarias para reescribir cualquier número natural**. Algunos valores para $g(n)$ son:

$$g(2) = 4$$
$$g(3) = 9$$
$$g(4) = 19$$
$$g(5) = 37$$
$$g(6) = 73$$