Suma de cuadrados

Joshua Chicoj

Universidad del Valle de Guatemala

2023

Agenda

1. Suma de dos cuadrados
2. Suma de tres cuadrados
3. Suma de cuatro cuadrados

Agenda

1. Suma de dos cuadrados
2. Suma de tres cuadrados
3. Suma de cuatro cuadrados

Representación primitiva

Sean $n, x, y \in \mathbb{Z}$. Se dice que $n = x^2 + y^2$ es una representación primitiva si $(x, y) = 1$

Lema 1

Sea $n \in \mathbb{Z}, p$ un primo de la forma $4m + 3$. Si $p \mid n \implies n$ no tiene representación primitiva.

Demostración Lema 1

Demostración.

Supongamos que $n = x^2 + y^2 \ni (x, y) = 1$ y sea p un factor primo de n, entonces $p | x^2 + y^2$, pero $(x, y) = 1 \implies p \nmid x \;\&\; p \nmid y$.

Demostración Lema 1

Demostración.

Supongamos que $n = x^2 + y^2 \ni (x, y) = 1$ y sea p un factor primo de n, entonces $p|x^2 + y^2$, pero $(x, y) = 1 \implies p \nmid x$ & $p \nmid y$. Puesto que $\mathbb{Z}/\mathbb{Z}_p$ es un campo, dividamos y^2 en la ecuación $x^2 + y^2 \equiv 0 \mod p \implies$

$$\left(\frac{x}{y}\right)^2 + \left(\frac{y}{y}\right)^2 \equiv 0 \mod p \implies \left(\frac{x}{y}\right)^2 \equiv -1 \mod p$$

Demostración Lema 1

Demostración.

Supongamos que $n = x^2 + y^2 \ni (x, y) = 1$ y sea p un factor primo de n, entonces $p|x^2 + y^2$, pero $(x, y) = 1 \implies p \nmid x$ & $p \nmid y$. Puesto que $\mathbb{Z}/\mathbb{Z}_p$ es un campo, dividamos y^2 en la ecuación $x^2 + y^2 \equiv 0 \mod p \implies$

$$\left(\frac{x}{y}\right)^2 + \left(\frac{y}{y}\right)^2 \equiv 0 \mod p \implies \left(\frac{x}{y}\right)^2 \equiv -1 \mod p$$

Esto implica que -1 es un residuo cuadrático $\mod p$, entonces

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = 1$$

Por lo tanto, $\frac{p-1}{2}$ debe ser par, entonces p es de la forma $4m + 1$ $\square$

Corolario 1

Si p_n/q_n es el n-esimo convergente del número irracional x, entonces

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_{n+1} q_n} \leqslant \frac{1}{q_n^2}$$

Lema 2

Si $x \in \mathbb{R}, n \in \mathbb{N}$ entonces hay una fracción $\frac{a}{b} \ni 0 < b \leqslant n$ y

$$x - \frac{a}{b} \leqslant \frac{1}{b(n+1)}$$

Demostración Lema 2

Demostración.

Considerese la fracción continua de x. Por el corolario 1, para cada m

$$\left| x - \frac{p_m}{q_m} \right| < \frac{1}{q_m \cdot q_{m+1}}$$

Puesto que $q_{m+1} \geqslant q_m + 1$ y $q_0 = 1 \implies \exists m \ni q_m \leqslant n < q_{m+1} \leqslant n + 1$, entonces

$$\left| x - \frac{p_m}{q_m} \right| < \frac{1}{q_m \cdot q_{m+1}} \leqslant \frac{1}{q_m \cdot (n+1)}$$

Por lo tanto, el m-esimo convergente de la fracción satisface el lema □

Teorema: Suma de dos cuadrados

Un entero positivo n es la suma de dos cuadrados si y solo si todos los factores primos $p|n$ de la forma $4m+3$ tienen exponente par en la factorización prima de n

Teorema: Suma de dos cuadrados

Un entero positivo n es la suma de dos cuadrados si y solo si todos los factores primos $p|n$ de la forma $4m+3$ tienen exponente par en la factorización prima de n

Demostración.

$(\implies)$ Supongamos por el absurdo que p, un primo de la forma $4m+3 \ni p^r|n$ & $p^{r+1} \nmid n$, para r impar y que $n = x^2 + y^2$.

Teorema: Suma de dos cuadrados

Un entero positivo n es la suma de dos cuadrados si y solo si todos los factores primos $p|n$ de la forma $4m+3$ tienen exponente par en la factorización prima de n

Demostración.

$(\implies)$ Supongamos por el absurdo que p, un primo de la forma $4m+3 \ni p^r|n$ & $p^{r+1} \nmid n$, para r impar y que $n = x^2 + y^2$. Hagamos $d = (x,y) \implies x = dx', y = dy' \implies n = d^2(x'^2 + y'^2) = d^2 n'$

Teorema: Suma de dos cuadrados

Un entero positivo n es la suma de dos cuadrados si y solo si todos los factores primos $p|n$ de la forma $4m+3$ tienen exponente par en la factorización prima de n

Demostración.

$(\implies)$ Supongamos por el absurdo que p, un primo de la forma $4m+3 \ni p^r|n$ & $p^{r+1} \nmid n$, para r impar y que $n = x^2 + y^2$. Hagamos $d = (x, y) \implies x = dx', y = dy' \implies n = d^2(x'^2 + y'^2) = d^2 n'$
Puesto que r es impar, $p|n'$, entonces por el lema 1 $(x', y') > 1 (\rightarrow\leftarrow)$ $\square$

Notemos que para la implicación de regreso podemos reducir el problema al caso en el que $n = n_1^2 n_2$, donde n_2 no tiene factores primos de la forma $4m + 3$. Puesto que

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1 x_2 - y_1 y_2)^2 + (x_1 y_2 + x_2 y_1)^2$$

entonces el producto de dos sumas de cuadrados es una suma de cuadrados. Y notemos que $2 = 1^2 + 1^2$, por lo tanto es suficiente mostrar que todo primo de la forma $4m + 1$ es una suma de dos cuadrados.

Suma de dos cuadrados

Demostración.

Recordemos que para p primo de la forma $4m+1$ tenemos que $(-1)^{(p-1)/2} = 1 \implies -1$ es un residuo cuadrado $\bmod p \therefore \exists r \in \mathbb{Z} \ni r^2 \equiv -1 \mod p$.

Suma de dos cuadrados

Demostración.

Recordemos que para p primo de la forma $4m+1$ tenemos que $(-1)^{(p-1)/2} = 1 \implies -1$ es un residuo cuadrado $\bmod p \therefore \exists r \in \mathbb{Z} \ni r^2 \equiv -1 \mod p$. Utilizando el resultado del lema 2 con $n = \lfloor \sqrt{p} \rfloor$ y $x = -\frac{r}{p}$, sabemos que $\exists a, b \in \mathbb{Z} \ni 0 < b < \sqrt{p}$ y

$$\left| -\frac{r}{p} - \frac{a}{b} \right| \leqslant \frac{1}{b(n+1)} < \frac{1}{b\sqrt{p}}$$

Suma de dos cuadrados

Demostración.

Recordemos que para p primo de la forma $4m+1$ tenemos que $(-1)^{(p-1)/2} = 1 \implies -1$ es un residuo cuadrado $\mod p \therefore \exists r \in \mathbb{Z} \ni r^2 \equiv -1 \mod p$. Utilizando el resultado del lema 2 con $n = \lfloor \sqrt{p} \rfloor$ y $x = -\frac{r}{p}$, sabemos que $\exists a, b \in \mathbb{Z} \ni 0 < b < \sqrt{p}$ y

$$\left| -\frac{r}{p} - \frac{a}{b} \right| \leqslant \frac{1}{b(n+1)} < \frac{1}{b\sqrt{p}}$$

Haciendo $c = rb + pa$ tenemos que

$$|c| < \frac{pb}{b\sqrt{p}} = \frac{pb}{b\sqrt{p}} = \frac{p}{\sqrt{p}} = \sqrt{p}$$

Entonces,

$$0 < b^2 + c^2 < 2p$$

$\square$

Suma de dos cuadrados

Demostración.

Pero, $c \equiv rb \mod p$, entonces

$$b^2 + c^2 \equiv b^2 + r^2 b^b \equiv b^2(1 + r^2) \equiv 0 \mod p$$

por lo tanto, $p = b^2 + c^2$ $\square$

Agenda

Lema

Lema 3

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

Demostración Lema 3

Demostración

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 $q^2 n = p_1^2 + p_2^2 + p_3^2$.

Demostración Lema 3

Demostración

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

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

Demostración Lema 3

Demostración

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

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

Ahora bien, supongamos por el absurdo, que $d > 1$. Si escribimos

$$y_1 = dy_1' + z_1, \quad y_2 = dy_2' + z_2, \quad y_3 = dy_3' + z_3,$$

con $y_i', z_i \in \mathbb{Z}$, $|z_i| \leqslant \frac{d^2}{2}$ para $i = 1, 2, 3$, definimos

$$a = {y'}_1^2 + {y'}_2^2 + {y'}_3^2 - n, \quad b = 2(nd - y_1 {y'}_1 - y_2 {y'}_2 - y_3 {y'}_3),$$

$$d' = ad + b, \quad {y''}_i = ay_i + by_i'.$$

Demostarción Lema 3

Demostración

Entonces

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

y

$$dd' = ad^2 + bd = d^2\left(\sum_{i=1}^{3}(y_i'')^2 - n\right) + 2d\left(nd - \sum_{i=1}^{3}y_iy_i'\right)$$
$$= \sum_{i=1}^{3}y_i^2 - 2d\sum_{i=1}^{3}y_iy_i' + d^2\sum_{i=1}^{3}(y_i'')^2$$
$$= \sum_{i=1}^{3}(yi - dy_i')^2 = \sum_{i=1}^{3}z_i^2 \leqslant \frac{3}{4}d^2.$$

Demostración.

Finalmente, $0 < d' \leqslant \frac{3}{4}d < d$, lo que contradice la minimalidad de d. Notemos que si $d' = 0$, entonces $\sum_{i=1}^{3} z_i^2 = dd' = 0$, de donde $z_1 = z_2 = z_3 = 0$, y tendríamos que $(y_1')^2 + (y_2')^2 + (y_3')^2 = n(\rightarrow\leftarrow)$.

Teorema: Suma de tres cuadrados

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

Demostración Teorema

Demostración

$(\implies)$Notemos que $k^2 \equiv 0, 1, 4 \pmod 8$, para todo $k \in \mathbb{Z}$. Por lo tanto, una suma de tres cuadrados no puede ser congruente a $7 \mod 8$. Además, si $x, y, z \in \mathbb{Z}$ son tales que $x^2 + y^2 + z^2 \equiv 0 \mod 4$, entonces x, y, z deben ser pares. Entonces, 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 $4(\bar{x}^2 + \bar{y}^2 + \bar{z}^2) = (2\bar{x})^2 + (2\bar{y})^2 + (2\bar{z})^2 = x^2 + y^2 + z^2 = 4^a(8b + 7) \Rightarrow \bar{x}^2 + \bar{y}^2 + \bar{z}^2 = 4^{a-1}(8b + 7)$.
De modo que $2^a|(x, y, z)$; entonces

$$x^2a^2 + y^2a^2 + z^2a^2 = 8b + 7 \equiv 7 \mod 8(\rightarrow\leftarrow)$$

$(\Leftarrow)$ Lema 3

Agenda

Identidad de Euler

Lema 4: Identidad de Euler

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

$$\left(a^2+b^2+c^2+d^2\right)\left(w^2+x^2+y^2+z^2\right)=$$
$$(aw+bx+cy+dz)^2+(ax-bw-cz+dy)^2+$$
$$+(ay+bz-cw-dx)^2+(az-by+cx-dw)^2$$

La demostración de la identidad puede ser consultada en la página 144 de Elements of Number Theory de Stillwell

Lema 5

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

Puesto que $2m = x^2 + y^2$, entonces x, y tienen la misma paridad, entonces

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

Suma de cuatro cuadrados

Lema 6

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

Considérense los conjuntos

$$A = \{a^2 \in \mathbb{Z}/\mathbb{Z}_p : 0 \leqslant a \leqslant \frac{p-1}{2}\}, B = \{-b^2 - 1 \in \mathbb{Z}/\mathbb{Z}_p : 0 \leqslant b \leqslant \frac{p-1}{2}\}$$

Cada conjunto posee $(p+1)/2$ elementos de $\mathbb{Z}/\mathbb{Z}_p$, por lo tanto $A \cap B \neq 0$, entonces $\exists a \in A, b \in B \ni a^2 + b^2 + 1 \equiv 0 \mod p$

Teorema: Suma de cuatro cuadrados

Todo entero positivo n puede escribirse como suma de cuatro cuadrados

Debido a la identidad de Euler, basta mostrar que el resultado para p un número primo. Notemos que $2 = 1^2 + 1^2 + 0^2 + 0^2$, por lo que nos enfocaremos al caso en el que p es impar. Del lema 6 tenemos que $\exists a, b, c, d, k \in \mathbb{Z} \ni mp = a^2 + b^2 + c^2 + d^2$ con $c = 1, d = 0$. Ahora consideremos los casos donde $m > 1$ es par y donde m es impar

- Si m es par, tomemos $n = m/2$, al aplicar el lema 5

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

Suma de cuatro cuadrados

- Si m es impar, sean w, x, y, z enteros tales que $w \equiv a \mod m, x \equiv b \mod m, y \equiv c \mod m, z \equiv d \mod m$ donde $w, x, y, z \in \left(-\frac{m}{2}, \frac{m}{2}\right)$. Por lo tanto,

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

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

Suma de cuatro cuadrados

Aplicando el lema 4,

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