El Teorema de Lagrange

Enzo R. Gentile[1]

Este célebre teorema establece que todo entero no negativo es suma de 4 cuadrados enteros. Este teorema fue conjeturado por P. de Fermat y su primer demostración se debe a Lagrange.

El objetivo de esta nota es dar una demostración elemental de este resultado.

Primeramente probaremos una identidad algebraica, también llamada identidad de Lagrange que expresa que el producto de sumas de 4 cuadrados es suma de cuatro cuadrados.

Para el caso de suma de 2 cuadrados, hay una identidad similar que es consecuencia de una propiedad de la norma de números complejos. Mostremos esto. Sea $Z = a + bi$ un número complejo y sea $\bar{Z} = 9 - bi$ su conjugado se define la norma de Z al valor $N(Z) = Z.\bar{Z} = a^2$ y b^2.

Es un hecho elemental que N es una función multiplicativa:

$$N(Z_1 Z_1) = N(Z_1).N(Z_2)$$

que se traduce en la siguiente identidad:

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

Si en cambio multiplicamos $Z_1.\bar{Z}_2$ resulta la identidad

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

con un sumando de la forma particular $(x_1 y_1 + x_2 y_2)^2$.

[1] Nota de la redacción: Este artículo es una nota póstuma de nuestro gran maestro, el Dr. Gentile. Si bien hay detalles a completar nos pareció prudente transcribir textualmente su manuscrito ya que así no tergiversamos su exposición.

Se trata de generalizar toda esta situación para el caso de 4 cuadrados. Para esto haremos una traducción de lo anterior a matrices.

Escribiendo los números complejos como matrices reales de 2x2 se tiene la correspondencia

$$x + iy \rightarrow \begin{bmatrix} x & -y \\ y & x \end{bmatrix}.$$

y además la norma de $x + iy$ se transforma en el determinante de la matriz y la conjugación en la transpuesta de la misma. Por ejemplo

$$Z_1.\bar{Z}_2 = \begin{bmatrix} x_1 & -y_1 \\ y_1 & x_1 \end{bmatrix}.\begin{bmatrix} x_2 & -y_2 \\ -y_2 & x_2 \end{bmatrix}$$

$$\begin{bmatrix} x_1x_2 + y_1y_2 & x_1y_2 - x_2y_1 \\ y_1x_2 - x_1y_2 & x_1x_2 + y_1y_1 \end{bmatrix}$$

Tomando determinante obtenemos nuevamente la identidad anterior. Esta situación se generaliza a 4 dimensiones en los objetos llamados cuaterniones. Estos pueden interpretarse como matrices complejas de 2 x 2.

Dicho más precisamente, a toda cuaterna x_1, x_2, x_3, x_4 de números reales le asociamos la matriz Z compleja:

$$Z = \begin{bmatrix} x_1 + x_2i & -x_3 + x_4i \\ x_3 + x_4i & x_1 - x_2i \end{bmatrix}$$

Si llamamos $u = x_1 + x_2i, v = x_3 + x_4i$, se tiene

$$Z = \begin{bmatrix} u & -\bar{v} \\ v & \bar{u} \end{bmatrix}$$

Definimos "conjugado de Z" por

$$\bar{Z} = \begin{bmatrix} \bar{u} & -v \\ \bar{v} & u \end{bmatrix}$$

y la "norma de Z" por

$$Z.{}^t\bar{Z} = \begin{bmatrix} u\bar{u} + v\bar{v} & 0 \\ 0 & u\bar{u} + v\bar{v} \end{bmatrix}$$

que podemos identificar con el número real

$$u\bar{u} + v\bar{v} = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

La totalidad de cuaterniones forman un anillo.

Sean

$$x_1, x_2, x_3, x_4$$

$$y_1, y_2, y_3, y_4$$

dos cuaternas de números reales. Asociemos a las mismas los cuaterniones

$$Z_1 = \begin{bmatrix} x_1 + x_2 i & -x_3 + x_4 i \\ x_2 + x_4 i & x_1 - x_2 i \end{bmatrix}$$

$$Z_2 = \begin{bmatrix} y_1 + y_2 i & -y_3 + y_4 i \\ y_3 + y_4 i & y_1 - y_2 i \end{bmatrix}$$

Hallemos el producto

$$(1) \qquad Z_1.{}^t\bar{Z}_2 = \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix}$$

con

$$c_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$$

$$c_2 = x_2y_1 - x_1y_2 - x_4y_3 + x_3y_4$$

$$c_3 = x_3y_1 + x_4y_2 - x_1y_3 - x_2y_4$$

$$c_4 = x_4y_1 - x_3y_2 + x_2y_3 - x_1y_4$$

Observemos que tomando determinante en (1) resulta la identidad buscada

$$(2) \qquad (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4) = (c_1^2 + c_2^2 + c_3^2 + c_4^2)$$

Es importante notar que los valores c_1, c_2, c_3, c_4 son funciones "bilineales" de $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4$.

El haber tomado $Z_1.{}^t\bar{Z}_2$ en lugar de $Z_1.Z_2$ nos permitió obtener uno de los c_i de forma particular:

$$x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4,$$

análogo al caso de 2 dimensiones.

Se sigue de la identidad de Lagrange y del teorema fundamental de la Aritmética que para probar el teorema será suficiente probar que todo primo > 0 es suma de 4 cuadrados.

Veamos el siguiente lema auxiliar.

Lema: Sea p primo, entonces existen enteros x_1, x_2, x_3, no todos divisibles por p, tales que

$$p | x_1^2 + x_2^2 + x_3^2$$

(Se sigue en particular que todo primo divide a una suma de 4 cuadrados).

Demostración: Trabajamos en el cuerpo de restos $\mathbf{Z}_p$. Sea la forma cuadrática $x^2 + ay^2 + cz^2$, con $a, c \in \mathbf{Z}_p$.

Afirmamos que existe $(x_1, y_1, z_1) \in \mathbf{Z}^3$ no nula tal que

$$x_1^2 + ay_1^2 + cz_1^2 \equiv 0 (\text{mod p})$$

Nota: el resultado es trivial si $p = 2$. Sea $p > 2$.

Sean

$$M_1 = \{1 + ay^2 | y \in \mathbf{Z}_p\}$$

$$M_2 = \{-cz^2 | z \in \mathbf{Z}_p\}$$

de M_1 y M_2 son subconjuntos de $\mathbf{Z}_p$. Como hay $\frac{p-1}{2}$ cuadrados no nulos en $\mathbf{Z_p}$, se sigue que

$$|M_1| = \frac{p-1}{2} + 1 = \frac{p+1}{2}$$

(puesto que hemos agregado $1 + a.0^2$).
Análogamente $|M_2| = \frac{p+1}{2}$. Como $\frac{p+1}{2} + \frac{p+1}{2} = p + 1$,
Concluimos que $M_1 \cap M_2 \neq \phi$.

Por lo tanto existen $y_1, z_1 \in \mathbf{Z}_p$ tales que

$$1 + ay_1^2 = -cz_1^2$$

o sea

$$1^2 + ay_1^2 + cz_1^2 = 0$$

y la terna $(1, y_1, z_1)$ es un cero no trivial de la forma cuadrática.
El Lema queda demostrado.

Demostración del Teorema.

Sea $p.m_0 = x_1^2 + x_2^2 + x_3^2 + x_4^2$ y no ha sido elegido de manera tal que $p.m_0$ es el múltiplo mas pequeño de p que es suma de 4 cuadrados. Si $m_0 = 1$ nada habrá que probar. Si $m_0 > 1$.

Supongamos $2|m_0$. Entonces x_1, x_2, x_3, x_4 son todos impares o hay 2 pares y dos impares. Sean x_1, x_2 pares y x_3, x_4 impares. Dado que la identidad

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

contradice la hipótesis de minimalidad de m_0. Se tiene que m_0 es impar, podemos suponer que $m_0 > 2$, o sea $m_0 \geq 3$.

Escribamos según el algoritmo de división

$$x_i = m_0 q_i + v_i \qquad |v_i| < \frac{m_0}{2} \qquad i = 1, 2, 3, 4.$$

Como $m_0 | \sum x_i^2$, entonces para algún m

$$m.m_0 = v_1^2 + v_2^2 + v_3^2 + v_4^2$$

y es claro que $m < m_0$.

Se tiene

$$v_1^2 + v_2^2 + v_3^2 + v_4^2 = 0 \qquad (\text{mod } m_0)$$

Además

$$p.m_0^2.m = (\sum x_i^2)(\sum v_i^2).$$

Escribamos

$$(\sum x_i^2)(\sum v_i^2) = (\sum x_i v_i)^2 + \ldots$$

Ahora

$$\sum x_i v_i \equiv \sum v_i^2 \equiv 0 (\text{mod } m_0)$$

Por lo tanto

$$m_0^2 | (\sum x_i v_i)^2$$

Con el mismo razonamiento probamos que m_0 divide a todos los términos del desarrollo (2) de $(\sum x_i^2)(\sum v_i^2)$ obtenido anteriormente. Se sigue que pm es

suma de cuadrados, con $m < m_0$. Como también $1 < m$, pues hemos supuesto que p no es suma de 4 cuadrados, se llega a una contradicción, esto prueba el teorema.

Nota 1: Observar que no hemos utilizado el hecho que p es primo. Las mismas ideas permiten demostrar que si $m|x_1^2 + x_2^2 + x_3^2 + x_4^2$ entonces m es suma de 4 cuadrados. Dejamos a cargo del lector esta verificación.

Nota 2: Las mismas ideas prueban que si p es un primo de la forma $4m + 1$, entonces p es suma de 2 cuadrados. Hay que invocar el hecho que un tal primo p, divide a una suma de 2 cuadrados. Esto es consecuencia de que la ecuación $x^2 \equiv -1 \pmod{p}$ es resoluble en $\mathbf{Z}$.