Una prueba elemental del último teorema de Fermat

Moreno Borrallo, Juan

September 20, 2018

e-mail: juan.morenoborrallo@gmail.com

"Entia non sunt multiplicanda praeter necessitatem" (Ockam, W.)

Abstract

En este artículo se prueba el último Teorema de Fermat, utilizando únicamente métodos elementales.

Keywords. *Último Teorema de Fermat, teorema del Binomio, elemental*

1 Introducción

El último Teorema de Fermat puede enunciarse del siguiente modo:

Último Teorema de Fermat. *La ecuación*

$$A^n + B^n = C^n$$

Donde A, B, C, n son enteros positivos, tiene solución si y solo si $n \leq 2$.

En este artículo se establece una prueba mediante el siguiente procedimiento:

- Suponemos que el último Teorema de Fermat es falso, y que la ecuación $A^n + B^n = C^n$ tiene soluciones si $n > 2$ y n es un número primo. Denominamos a esta suposición Hipótesis Nula.
- Se establecen determinadas condiciones necesarias que tienen que darse para que pueda ser verdadera la Hipótesis Nula.

- Se prueba por contradicción que dichas condiciones necesarias no pueden darse.

- Al probarse que la Hipótesis Nula es falsa, queda probado inmediatamente el último Teorema de Fermat para todos los exponentes primos mayores que 2, y por extensión para todos los demás casos.

2 Desarrollo de la prueba

Lema 1. *La Hipótesis Nula es verdadera si y solo si* $A + B \neq C$*.*

Demostración.

Si $A + B = C$, entonces $C^n = (A + B)^n$. Como por el teorema del Binomio $(A + B)^n > A^n + B^n$, queda probado el Lema 1.

Lema 2. *La Hipótesis Nula es verdadera si y solo si* $C < A + B < 2C$*.*

Demostración.

Si $A \geq C$ o $B \geq C$, entonces $A^n \geq C^n$ o $B^n \geq C^n$, lo que implicaría que $A^n + B^n > C^n$; por tanto, tiene que cumplirse que $A < C$ y $B < C$, y en consecuencia $A + B < 2C$.

Por otro lado, conforme al Lema 1, la Hipótesis Nula es verdadera si y solo si $A + B \neq C$. Si $A + B \neq C$, tiene que cumplirse que $A + B > C$*;* en caso contrario, $C^n = (A + B + (C - (A + B)))^n$, que por el teorema del Binomio sería mayor que $A^n + B^n$.

En conclusión, la Hipótesis Nula es verdadera si y solo si $C < A + B < 2C$.

Lema 3. $A + B \mid A^{2n+1} + B^{2n+1}$*; por tanto, la Hipótesis Nula es verdadera si y solo si* $A + B \mid C^n$*.*

Demostración.

Para demostrar que $A + B \mid A^{2n+1} + B^{2n+1}$, aplicaremos una demostración por inducción.

Para $n = 1$,

$$A^{2n+1} + B^{2n+1} = A^3 + B^3$$

$$A^3 + B^3 = (A + B)(AB + (B - A)^2)$$

$$A + B \mid A^3 + B^3$$

Asumimos que $A + B \mid A^{2n+1} + B^{2n+1}$, y comprobamos para el caso $n + 1$.

Para $n+1$,

$$A^{2(n+1)+1}+B^{2(n+1)+1}=A^2(A^{2n+1})+B^2(B^{2n+1})=$$

$$=A^2(A^{2n+1})+(B^2+A^2-A^2)(B^{2n+1})=$$

$$=A^2(A^{2n+1}+B^{2n+1})+(B^2-A^2)(B^{2n+1})=$$

$$=A^2(A^{2n+1}+B^{2n+1})+(B-A)(B+A)(B^{2n+1})$$

El sumando $A^2(A^{2n+1}+B^{2n+1})$ es divisible por $A+B$ si asumimos que $A+B \mid A^{2n+1}+B^{2n+1}$, y el segundo sumando es un producto de factores entre los cuales se encuentra $A+B$, por lo que también es divisible por $A+B$.

Por tanto, la expresión es divisible por $A+B$, y queda probado que $A+B \mid A^{2n+1}+B^{2n+1}$para el caso $n+1$ se cumple si es cierto para el caso n. Como es cierto para el caso $n=1$, queda probado para todos los números naturales.

Como la Hipótesis Nula considera que el exponente n es un número primo mayor que 2, y dado que todo número primo mayor que 2 es de la forma $2n+1$, la Hipótesis Nula es verdadera si y solo si $A+B \mid A^n+B^n$, y por equivalencia, si y solo si $A+B \mid C^n$.

Contradicción de los Lemas 2 y 3.

Conforme al Lema 2, la Hipótesis Nula es verdadera si y solo si $C < A+B < 2C$. Esta inecuación implica que $A+B \nmid C$, y por tanto $A+B \nmid C^n$.

Conforme al Lema 3, y dado que todo número primo mayor que 2 es de la forma $2n+1$, la Hipótesis Nula es verdadera si y solo si $A+B \mid C^n$, lo que entra en contradicción con el Lema 2.

Así pues, hemos llegado a una contradicción, por lo que la Hipótesis Nula no puede ser verdadera.

Conclusión

Por extensión, es fácil demostrar que el Teorema es cierto para el resto de números, ya que si el exponente n es un número compuesto $m=n_1n_2...n_t$, la igualdad se puede reexpresar con otra igualdad equivalente en la que el exponente sea cualquier número primo que componga dicho exponente, como sigue:

$$A^m+B^m=C^m=$$

$$= A^{n_1 n_2 \dots n_t} + B^{n_1 n_2 \dots n_t} = C^{n_1 n_2 \dots n_t} =$$

$$= (A^{n_2 \dots n_t})^{n_1} + (B^{n_2 \dots n_t})^{n_1} = (C^{n_2 \dots n_t})^{n_1} =$$

$$= (A^{n_1 \dots n_t})^{n_2} + (B^{n_1 \dots n_t})^{n_2} = (C^{n_1 \dots n_t})^{n_2} = \dots$$

$$= (A^{n_1 n_2 \dots})^{n_t} + (B^{n_1 n_2 \dots})^{n_t} = (C^{n_1 n_2 \dots})^{n_t}$$

Por tanto, queda demostrado el último Teorema de Fermat por métodos elementales, c.q.d.