DEMOSTRACION DEL TEOREMA DE FERMAT

El teorema de Fermat nos indica que no es posible obtener ternas de números enteros positivos **x, a, b**, tales que cumplan la ecuación

$$x^n - a^n = b^n \qquad (1)$$

n=número entero positivo; n>2

Factorizando la ecuación anterior:

$$(x^{n/2} + a^{n/2})\,(x^{n/2} - a^{n/2}) = b^n$$

Si b es entero y se pretende encontrar valores de x,a enteros que cumplan la igualdad anterior, sepuede expresar:

$$(x^{n/2} + a^{n/2})\,(x^{n/2} - a^{n/2}) = b^n \cdot 1^*$$

$$x^{n/2} + a^{n/2} = b^n \quad (2)$$

$$x^{n/2} - a^{n/2} = 1 \qquad (3)$$

de forma que los valores de x,a enteros que cumplan la ecuación (1), deberán cumplir las ecuaciones (2) y (3).

Fijándonos en la ecuación (3), se comprueba que no pueden existir valores enteros de x, a, que cumplan la ecuación (3), ya que la diferencia de dos potencias de bases x,a (enteros) con x>a, y exponente n/2, con n>2 es siempre mayor que la unidad, por lo que para valores de b enteros no es posible encontrar valores enteros a,x, que cumplan la ecuación (1).

Queda demostrado el Teorema de Fermat. ***

*Existen otras combinaciones de enteros cuyo producto es b^n ;

$$b^n = \alpha \cdot \beta$$

$$\alpha, \beta = \text{enteros}, \ \alpha > \beta$$

Si $\beta=1$; $b^n= b^n\cdot 1$ En este caso se puede afirmar que no es posible encontrar ningún valor de b entero que genere valores enteros de x,a en la ecuación (1)

Por lo que si no es posible encontrar ningún valor de b entero que genere valores enteros de x,a en la ecuación (1), no pueden existir pares de valores enteros α, β, que generen valores enteros de a,x en la ecuación (1), ya que $b^n=\alpha\cdot\beta$

** Se adjunta una demostración.

Generalizando, b^n se puede expresar como el producto de dos enteros α,β:

$$b^n=\alpha\cdot\beta$$

$$\alpha>\beta$$

y las ecuaciones anteriores se pueden expresar:

$$(x^{n/2}+a^{n/2})(x^{n/2}-a^{n/2})=\alpha\cdot\beta$$

$$x^{n/2}+a^{n/2}=\alpha(2')$$

$$x^{n/2}-a^{n/2}=\beta\quad(3')$$

sin embargo, si no es posible encontrar valores de x,a enteros que cumplan las ecuaciones (2) y (3), para valores de $\beta=1$, no será posible encontrar valores de x,a enteros que cumplan las ecuaciones (2') y (3') para valores enteros de $\beta>1$, siendo β divisor de a^n

Se puede comprobar, sumando las ecuaciones (2) y (3).

$$2x^{n/2}=\alpha+\beta;$$

$$\alpha+\beta-2x^{n/2}=0\qquad(4)$$

Para resolver la ecuación anterior en términos enteros, podemos utilizar la expresión:

$$(\alpha^{1/2}-\beta^{1/2})^2=\alpha+\beta-2\alpha^{1/2}\beta^{1/2}$$

De tal forma que si se iguala a 0 se obtiene:

$$\alpha+\beta-2\alpha^{1/2}\beta^{1/2}=0\quad(5)$$

Si se igualan las ecuaciones 4 y 5:

$$-2x^{n/2}=-2\alpha^{1/2}\beta^{1/2}$$

Resultando:

$$x^n=\alpha\beta$$

$$x^n=b^n$$

$$x=b$$

Como:

$$(\alpha^{1/2}-\beta^{1/2})^2=0$$

Resulta:

$$\alpha=\beta$$

$$\alpha=b^{n/2}$$

$$\beta=b^{n/2}$$

Obteniéndose la solución cuasitrivial :

$$x=b$$

$$a=0$$

Quedando demostrado que si no es posible encontrar valores enteros de x,a para el producto

$b^n=b^n\cdot 1$, en la ecuación siguiente:

$$(x^{n/2}+a^{n/2})\ (x^{n/2}-a^{n/2})=b^n\cdot 1$$

tampoco pueden encontrarse valores enteros de x,a para el producto $b^n=\alpha\beta$, en la ecuación:

$$(x^{n/2}+a^{n/2})\ (x^{n/2}-a^{n/2})=\alpha\cdot\beta$$

*** Si se parte de la ecuación:

$$x^n-b^n=a^n$$

cuando **a** es entero y se pretende encontrar valores de **x,b** enteros, ya que

$$(x^{n/2}+b^{n/2})\ (x^{n/2}-b^{n/2})=a^n\cdot 1^*$$

$$x^{n/2}+b^{n/2}=a^n \quad (2")$$

$$x^{n/2}-b^{n/2}=1 \qquad (3")$$

Se comprueba que no pueden existir valores enteros de **x, b**, que cumplan las ecuaciones (2”), (3”)anteriores, para valores enteros de **a**, ya que la diferencia de dos potencias de bases **x,b** (enteros) con **x>b**, y exponente n/2, con n>2 es siempre mayor que la unidad, por lo que para valores de **a** enteros no es posible encontrar valores enteros **b,x,** que cumplan la ecuación: $x^n-b^n=a^n$

Queda demostrado el Teorema de Fermat.

Definición original del Teorema de Fermat

Es imposible descomponer un cubo en dos cubos, un bicuadrado en dos bicuadrados, y en general, una potencia cualquiera, aparte del cuadrado, en dos potencias del mismo exponente

Esta definición se corresponde con la expresión:

$$x^n=a^n+b^n$$

n=número entero positivo; n>2

Como se ha demostrado:

- si **a** es entero es imposible encontrar pares de valores **x,b**enteros que cumplan la expresión anterior.

-Si **b** es entero es imposible encontrar pares de valores **x,a** enteros, que cumplan la expresión anterior.

Y como consecuencia, en la expresión anterior si **x** es entero, es imposible encontrar pares de valores **a,b** enteros que cumplan la expresión anterior (descomponer un cubo en dos cubos…..)

OTRA DEMOSTRACION DEL TEOREMA DE FERMAT

El teorema de Fermat nos indica que no es posible obtener ternas de números enteros positivos **x, a, b**, tales que cumplan la ecuación

$$x^n - a^n = b^n (1)$$

n=número entero positivo; n>2

1.- Obtención de ternas pitagóricas para la ecuación anterior

Si **r,p** son números enteros positivos con **r>p,** las ternas pitagóricas ($x^{n/2}$, $a^{n/2}$, $b^{n/2}$), en función de r,pse pueden expresar:

$$x^{n/2} = r^2 + p^2$$

$$a^{n/2} = r^2 - p^2$$

$$b^{n/2} = 2rp$$

Dando valores a r,p se obtienen todas las ternas (primitivas y no primitivas)

Si de forma conjunta se pudieran encontrar valores enteros de x,a,b , NO SE CUMPLIRIA EL TEOREMA DE FERMAT, ya que la ecuación (1) se cumpliría para valores enteros de x,a,b con n>2

Demostraremos que no es posible encontrar, de forma conjunta, valores enteros de x,a,b, para valores de r,p enteros positivos. Con ello quedará demostrado el T. **Fermat**

*$x^{n/2}$, $a^{n/2}$, $b^{n/2}$, son los elementos de una terna que elevados al cuadrado satisface la ecuación:

$$x^n - a^n = b^n \quad (1)$$

ya que

$$(x^{n/2})^2 - (a^{n/2})^2 = (b^{n/2})^2$$

$$(r^2 + p^2)^2 - (r^2 - p^2)^2 = (2rp)^2$$

*Las ternas primitivas se obtienen si:

1) r=par; p=impar

2) r=impar; p=par

siempre que r no sea múltiplo de p

2.-Demostracion del Teorema

Para valores enteros de r, p, en el sistema de ecuaciones:

$$x^{n/2} = r^2 + p^2$$

$$a^{n/2} = r^2 - p^2$$

$$b^{n/2} = 2rp$$

se presentan tres posibilidades:

a).-es posible encontrar valores enteros de r,p, con n>2 que generan valores enteros de **a,** en la ecuación:

$$a^{n/2} = r^2 - p^2$$

pero esos valores de r,p,n no generan valores enteros de **x**o de **b** en las otras dos ecuaciones.

b).-es posible encontrar valores enteros de r,p, con n>2 que generan valores enteros de **b,** en la ecuación:

$$b^{n/2} = 2rp$$

pero esos valores de r,p,n no generan valores enteros de **x** o de **a** en las otras dos ecuaciones.

c).-es posible encontrar valores enteros de r,p, con n>2 que generan valores enteros de **x,** en la ecuación:

$$x^{n/2} = r^2 + p^2$$

pero esos valores de r,p,n no generan valores enteros de **a** o de **b** en las otras dos ecuaciones.

Para la constatar la veracidad del teorema bastara con demostrar que se cumple cualquiera de las afirmaciones anteriores.

<u>Demostración para el supuesto a).</u>

factorizando la ecuación:

$$r^2 - p^2 = a^{n/2}$$

$$(r+p)(r-p) = (a^{n/2}) \cdot 1$$

Igualando:

$$r+p = a^{n/2}$$

$$r-p = 1$$

Se obtiene:

$$r = (a^{n/2}+1)/2$$

$$p = (a^{n/2}-1)/2$$

Sustituyendo en:

$$x^{n/2} = r^2 + p^2$$

$$b^{n/2} = 2rp$$

se obtiene:

$$x^{n/2} = (a^n+1)/2$$

$$b^{n/2} = (a^n-1)/2$$

restando las ecuaciones anteriores:

$$x^{n/2} - b^{n/2} = 1 \qquad (2)$$

resultando que, para valores enteros de a, con:

r,p=enteros

r>p

n>2

no es posible encontrar en la expresión (2) valores enteros de x o de b, que satisfagan dicha ecuación, porque la diferencia de dos potencias de bases x,b (con x,b enteros , n>2, y exponente n/2) es siempre mayor que la unidad.

Por tanto, queda demostrado el teorema de Fermat.

<u>Demostración para el supuesto b).</u>

$$2rp= b^{n/2}$$

$$rp=(b^{n/2})/2\cdot 1$$

Igualando:

$$r= (b^{n/2})/2$$

$$p=1$$

Sustituyendo en:

$$x^{n/2}= r^2 + p^2$$

$$a^{n/2}=r^2- p^2$$

se obtiene:

$$x^{n/2}=(b^n/4)+1$$

$$a^{n/2}=(b^n/4)- 1$$

restando las ecuaciones anteriores:

$$x^{n/2}-a^{n/2} =2 \qquad (2)$$

resultando que, para valores enteros de a, con:

r,p=enteros

$r>p$

$n>2$

no es posible encontrar en la expresión (2) valores enteros de x o de a, que satisfagan dicha ecuación, porque la diferencia de dos potencias de bases x,a (con x,b enteros , n>2, y exponente n/2) es siempre mayor que dos.*

Por tanto, queda demostrado el teorema de Fermat.

<u>Otra Demostración para el supuesto b).</u>

Es posible encontrar en función de r,p, valores enteros de b, para cualquier n>2, en la ecuación

$$b^{n/2}=2rp$$

pero para los anteriores valores de r,p,n, no es posible encontrar valores enteros de x a, en las ecuaciones:

$$x^{n/2}= r^2 + p^2$$

$$a^{n/2}= r^2 - p^2$$

A su vez $b^{n/2}$ se puede expresar:

$$b^{n/2}=2(2^{(n/2)-1})\alpha^{n/2}$$

$$\alpha=1,2,3,4,\ldots\ldots$$

Igualando:

$$2rp=2(2^{(n/2)-1})\alpha^{n/2}$$

Se obtiene:

$$r=\alpha^{n/2}$$

$$p=2^{(n/2)-1}$$

que sustituyendo en las ecuaciones:

$$x^{n/2}= r^2 + p^2$$

$$a^{n/2}= r^2 - p^2$$

resulta:

$$x^{n/2}= \alpha^n +2^{n-2}$$

$$\alpha^n =a^{n/2} + 2^{n-2}$$

sumando las ecuaciones anteriores:

$$x^{n/2} - a^{n/2} = 2^{n-1} \qquad (3)$$

resultando que, para valores enteros de b, con:

r,p=enteros

r>p

n>2

no es posible encontrar en la expresión (3) valores enteros de x o de a, que satisfagan dicha ecuación, porque la diferencia de dos potencias de bases x,a (con x,a enteros, n>2, y exponente n/2) es siempre mayor que 2^{n-1}.

Por tanto, queda demostrado el teorema de Fermat.

Demostración para el supuesto c).

La ecuación:

$$x^{n/2} - b^{n/2} = 1$$

establece la relación entre **x** y **b** para valores enteros de **a**.

De esta ecuación se deduce que para valores enteros de **a** y de **x**, no pueden encontrarse valores enteros de **b**

La ecuación

$$x^{n/2} - a^{n/2} = 2$$

establece la relación entre **x** y **a** para valores enteros de **b**.

De esta ecuación se deduce que para valores enteros de **b** y de **x**, no pueden encontrarse valores enteros de **a**

Por tanto; para valores enteros de **x** en la ecuación:

$$x^{n/2} = r^2 + p^2$$

no es posible encontrar valores enteros de **a** o de **b**en las ecuaciones:

$$a^{n/2} = r^2 - p^2$$

$$b^{n/2} = 2rp$$

Queda demostrado el teorema de Fermat, yaque no es posible encontrar de forma conjunta valores enteros de x,a,b, que cumplan la ecuación (1)

$$x^n - a^n = b^n \quad (1)$$

n=número entero positivo; n>2

Julio 2024