EL ÚLTIMO TEOREMA. UN VIAJE DIFERENTE AL MISMO SITIO

PLANTEAMIENTO DEL PROBLEMA

Pierre de Fermat (1601?, 1665), al comentar el octavo problema del segundo libro de la Aritmética de Diofanto, referente a la solución en números racionales de la ecuación $\mathbf{x^2 + y^2 = a^2}$, hace el siguiente comentario:

> "Por el contrario, es imposible descomponer un cubo en dos cubos, una cuarta potencia en dos cuartas potencias, o, de un modo general, cualquier potencia superior a la segunda en dos potencias del mismo grado. Yo he descubierto una demostración maravillosamente exacta, pero este margen es demasiado estrecho para desarrollarlo" (*Fermat*, Oeuvres, III, pág. 241) (*)

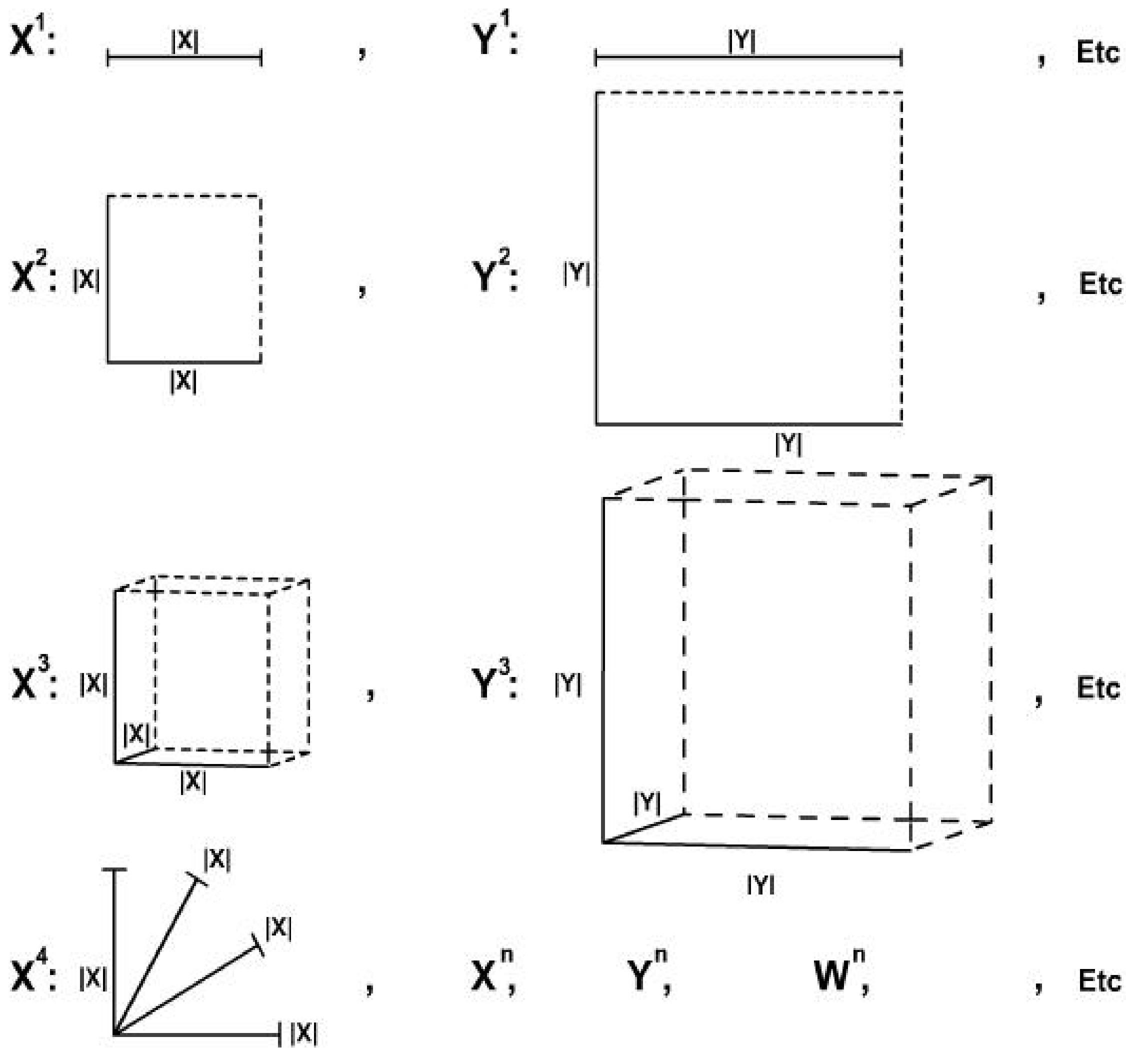
ET Bell. Los grandes matemáticos.
http://www.geocities.com/grandesmatematicos/cap04.html
(Abril 2005)

Es decir, la demostración de que, dados tres números racionales **x**, **y**, **z**, tales que $\mathbf{x^n + y^n = z^n}$, no existe solución para dicha ecuación cuando $\mathbf{n > 2}$. Esto es lo que, según *Fermat*, demostró él hacia el año 1637, pero cuyo texto nadie encontró.

Por fin, en 1995, el inglés *Andrew John Wiles* consiguió resolver con éxito este teorema demostrando la conjetura de *Shimura-Taniyama* que enlaza las ecuaciones modulares con las elípticas. Sin embargo, no pudo ser ésta aquella sencilla demostración a la que aludía *Fermat*, dada la complejidad y modernidad de los conceptos matemáticos empleados.

UNA SOLUCIÓN A ESTE PROBLEMA

Establezcamos una analogía entre la potencia natural (**n**) de un número racional cualquiera y su posible representación geométrica en forma de una figura cuadrada de **m** lados de la misma dimensión que el exponente y de tamaño igual al valor absoluto del número que tiene como base, de la siguiente forma:



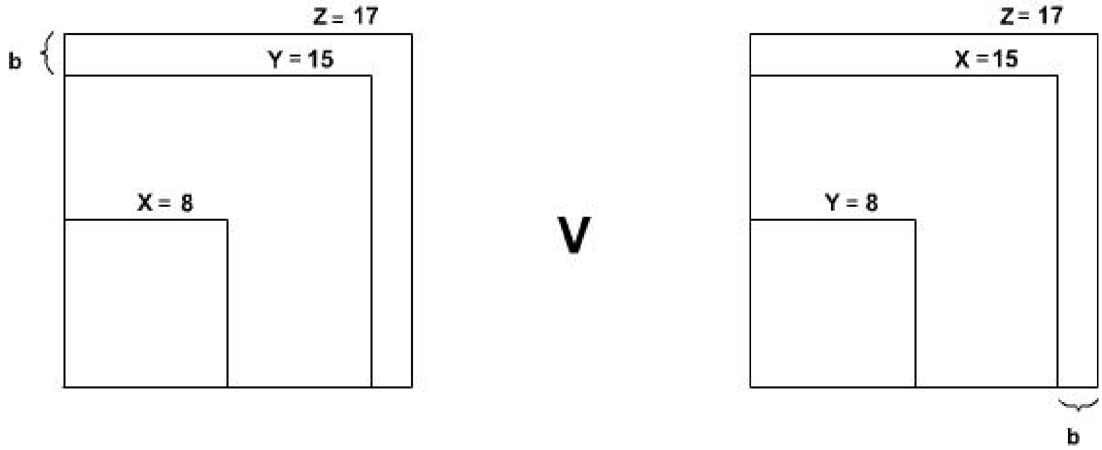
Así, una potencia de exponente de valor 1 de un número racional $\mathbf{x}$, será análogo a una figura cuadrada de un espacio de dimensión 1 (una recta) de tamaño (longitud): $|\,\mathbf{x}\,|$.

Y un exponente de valor 3 de un número $\mathbf{y}$, será análogo a una figura cuadrada de dimensión 3 (un cubo), cuyos lados rectos iguales serán exactamente de longitud $|\,\mathbf{y}\,|$, cada superficie formada por 4 de estos lados tendrá una magnitud de $|\,\mathbf{y}^2|$ y el volumen de la figura completa será de $|\,\mathbf{y}^3|$.

De la misma manera, un exponente de valor $\mathbf{n}$ de un número cualquiera $\mathbf{w}$, representará otra figura cuadrada proporcional a $|\,\mathbf{w}\,|$ y de dimensión $\mathbf{n}$.

Que los lados de estas u otras figuras rectas similares sean proporcionales a una figura cuadrada, esto es, que puedan ponerse en función uno respecto del otro y, por tanto, que lo sean también las distintas superficies, volúmenes y regiones que éstos generan entre sí, es una propiedad que de aquí en adelante llamaré: **“cuadrar”**. De esta manera, si una figura recta **n-**dimensional cualquiera (cuadrada o no) **“no cuadra”**, como veremos más adelante, diremos que no puede representar geométricamente la potencia natural de un número racional.

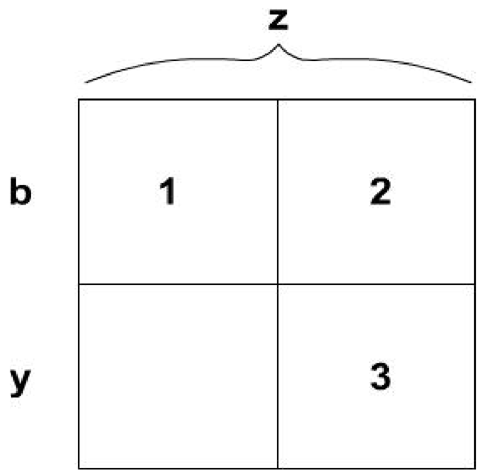
Si representamos ahora geométricamente la ecuación que nos ocupa de esta manera definida para **n = 2** , tendremos tres cuadrados de distintos tamaños, que puedo disponer en forma de dos cuadrados inscritos en un tercero. Así, para la terna de números (15, 8, 17), por ejemplo:



Para una terna de números como ésta, que satisface la ecuación $\mathbf{x^2 + y^2 = z^2}$ y basándonos en esta forma de representación donde se identifican los distintos cuadrados por los guarismos que determinan su área, se deducen 4 relaciones evidentes:

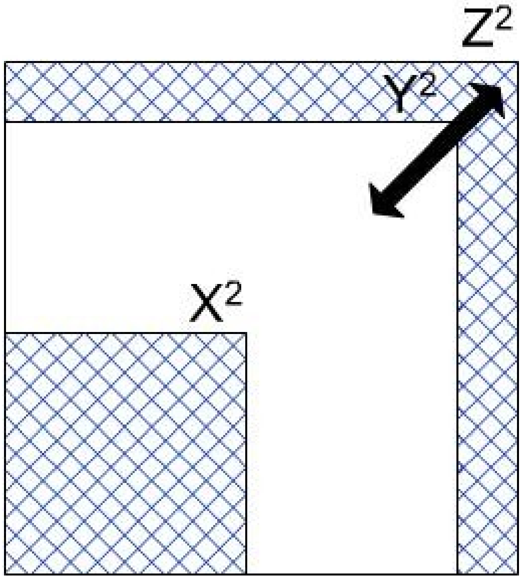
1. $\mathbf{x \neq y}$
2. $\mathbf{x \wedge y < z}$
3. $\mathbf{(b = z - y) \vee (b = z - x)}$ [A partir de ahora escribiré siempre $\mathbf{b = z - y}$ y representaré las figuras como $\mathbf{x < y}$]
4. $\mathbf{b < y}$ [En el supuesto anterior]

De estas 4 relaciones sólo la última es menos evidente y se demuestra de la siguiente manera: si **b** fuera igual a **y** , tendríamos:



Lo que implica que $\mathbf{z^2 = 4\, y^2}$. Y puesto que en este caso siempre $\mathbf{x^2 + y^2 < 4\, y^2}$, concluimos que $\mathbf{b \neq y}$ y por lo tanto, mucho menos que $\mathbf{b > y}$, por lo que nos queda que $\mathbf{b < y}$.

En base a esta representación, yo puedo hacer el siguiente planteamiento geométrico de lo que puede significar cualquier solución a la ecuación $\mathbf{x^2 + y^2 = z^2}$: que el área de la zona comprendida entre los cuadrados $\mathbf{z^2}$ y $\mathbf{y^2}$, sea igual al área del cuadrado $\mathbf{x^2}$. Algebraicamente: $\mathbf{x^2 = z^2 - y^2}$.



Como se ve en la figura, en principio, para un cuadrado $\mathbf{x^2}$ cualquiera, bastará con agrandar o achicar un cuadrado $\mathbf{y^2}$ como el representado de forma conveniente para que su diferencia con $\mathbf{z^2}$ sea igual al área del primero.

Para demostrar esto, partamos de esta forma de ecuación $\mathbf{x^2 = z^2 - y^2}$. Si aplicamos ahora la clásica regla de factorización a $\mathbf{z^2 - y^2}$, tendremos que $\mathbf{x^2 = (z - y) \cdot (z + y)}$. Esta relación debe cumplirla cualquier terna solución a la ecuación $\mathbf{x^2 + y^2 = z^2}$, sean éstas enteras o racionales como es fácil de comprobar.

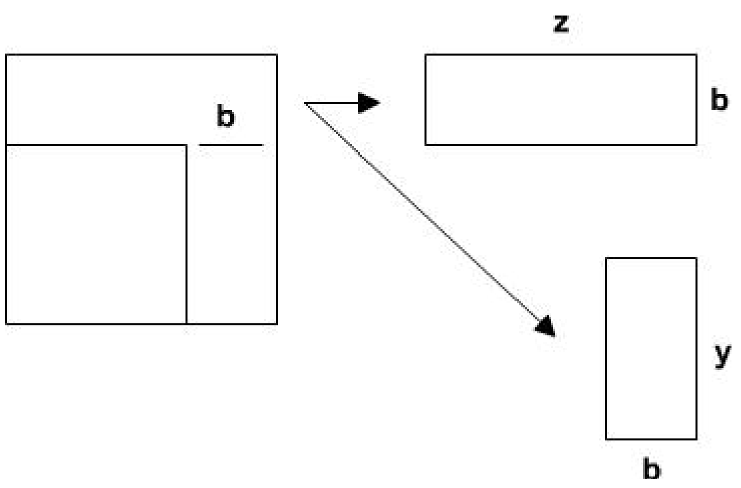
Veamos ahora cómo, siguiendo esta pista, puedo relacionar la ecuación que nos ocupa con la expresión más genérica $\mathbf{(x + y)^n}$:

Puesto que: $z = y + b$; entonces: $z^n = (y + b)^n$

Así, para $n = 2$:

$$z^2 = (y + b)^2 = y^2 + 2\ y\ b + b^2 \qquad ,\Rightarrow$$
$$z^2 - y^2 = 2\ y\ b + b^2 \qquad ,\Rightarrow$$
$$x^2 / b = 2\ y + b \quad (\wedge\ b = z - y) \qquad ,\Rightarrow$$
$$x^2 / b = 2\ y + (z - y) = y + z \qquad ,\Rightarrow$$
$$x^2 = y\ b + z\ b$$

Geométricamente:



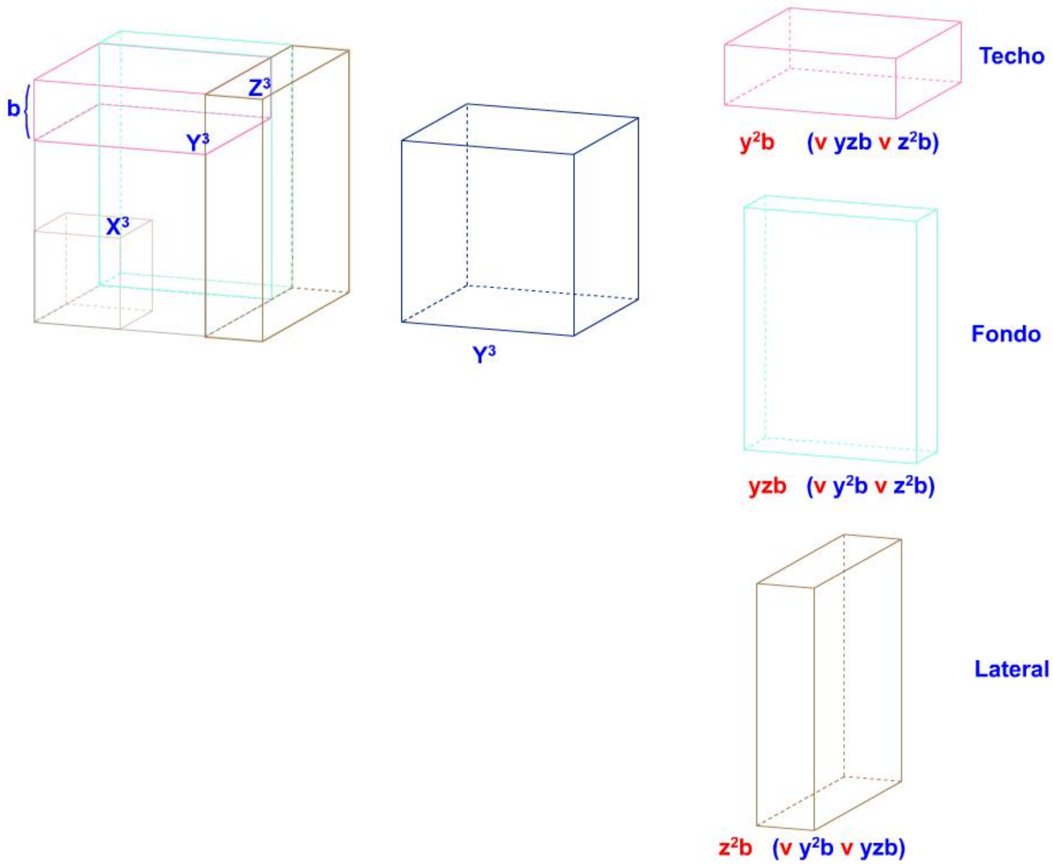
Veamos qué ocurre para $n = 3$:

$$z^3 = (y + b)^3 = y^3 + 3\ y^2 b + 3\ y\ b^2 + b^3 \quad ,\Rightarrow$$
$$z^3 - y^3 = 3\ y^2 b + 3\ y\ b^2 + b^3$$

Y puesto que generalizando por inducción matemática entendemos que existe un x^3 de volumen igual a la región comprendida entre z^3 y y^3, $\Rightarrow$

$$x^3 / b = 3\ y^2 + 3\ y\ b + b^2 \quad (\wedge\ b = z - y) \quad ,\Rightarrow$$
$$x^3 / b = 3\ y^2 + 3\ y\ (z - y) + (z - y)^2 = y^2 + y\ z + z^2 \ ,\Rightarrow$$
$$x^3 = y^2\ b + y\ z\ b + z^2\ b$$

Geométricamente:



Visto y probado este razonamiento para $\mathbf{n = k}$ y probado su posibilidad para $\mathbf{n = k + 1}$, antes de ver si existe o no ese $\mathbf{x^3}$, demos el salto para $\boldsymbol{n = n}$.

Partiendo del Teorema del binomio:

$$\mathbf{(x + y)^n = x^n + n\, x^{n-1} y +} \frac{n(n-1)}{2!} \mathbf{x^{n-2} y^2 +} \frac{n(n-1)(n-2)}{3!} \mathbf{x^{n-3} y^3}$$

$$+ \underline{\hspace{2cm}} + \frac{n(n-1)}{2!} \mathbf{x^2 y^{n-2} + n\, x\, y^{n-1} + y^n}$$

, sustituyendo por $\mathbf{(y + b)^n}$ y siguiendo el mismo razonamiento empleado para $\mathbf{n = 2}$ y $\mathbf{n = 3}$, se puede comprobar que llegamos a:

$$x^n = n\, y^{n-1} b + \frac{n(n-1)}{2!}\, y^{n-2} (z-y)\, b + \frac{n(n-1)(n-2)}{3!}\, y^{n-3} (z-y)^2 b$$

$$+ \_\_\_\_\_\_ + \frac{n(n-1)}{2!}\, y^2 (z-y)^{n-3} b + n\, y\, (z-y)^{n-2} b + (z-y)^{n-1} b$$

De esta manera:

$$x^2 = y\, b + z\, b$$
$$x^3 = y^2\, b + y\, z\, b + z^2 b$$
$$x^4 = y^3 b + y^2 z\, b + y\, z^2 b + z^3 b$$
$$x^5 = y^4 b + y^3 z\, b + y^2 z^2 b + y\, z^3 b + z^4 b$$

________ Etc.

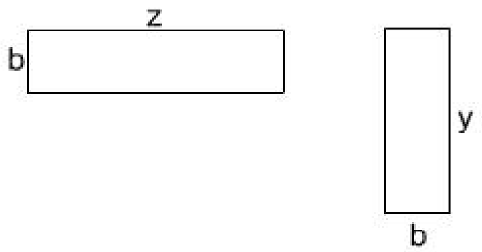
De donde se deduce a su vez:

$$x^n = y^{n-1} b + y^{n-2} z\, b + y^{n-3} z^2\, b + \_\_ + y^2 z^{n-3} b + y\, z^{n-2} b + z^{n-1} b$$

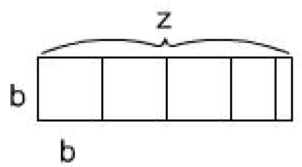
Dadas pues, unas figuras cuadradas **n-**dimensionales como las expuestas, descompuestas en una suma de figuras rectangulares descritas por el producto de sus **n** lados rectos que definen su región en el espacio, diremos lógicamente que esta suma es imposible cuando el resultado de sus sumandos sea un número raíz no entera de ningún otro.

Al principio de esta exposición hablé de lo que entendía por **"cuadrar"** una figura geométrica recta **n-**dimensional. En un primer momento puede parecer que esta propiedad sólo es aplicable a las figuras estrictamente cuadradas, pero no es así. Para cualquier figura de **m** lados rectos que conste de sólo 2 tipos de lados de diferente longitud también es aplicable dicha propiedad, en tanto que un lado puede 'razonarse' o ponerse 'en función' del otro. Esto significará que la figura como tal también podrá trocearse en figuras cuadradas más pequeñas, enteramente o racionalmente, que den cuenta de forma completa de toda la región que ocupa en el espacio.

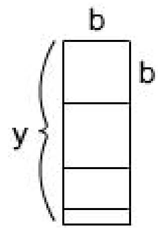
Así, en un sistema de 2 dimensiones, rectángulos como $\mathbf{y\ b}$ y $\mathbf{z\ b}$, para $\mathbf{(b, y, z, L, K)} \in \mathbb{Q} \wedge \mathbf{b < y < z}$:



, pueden dar lugar a:

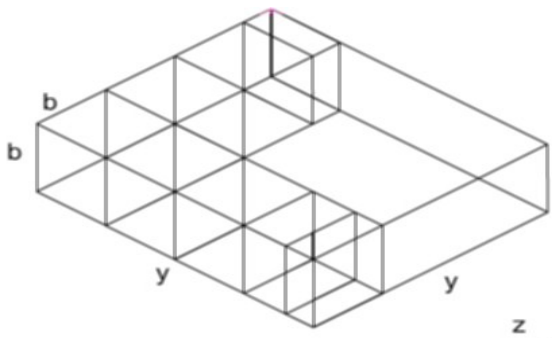


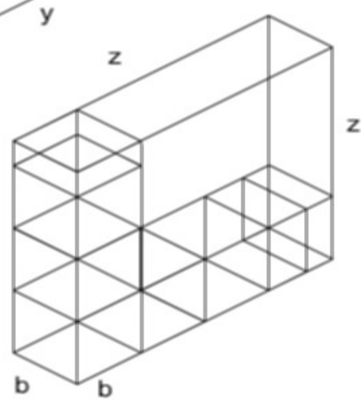
z/b= L figuras 'cuadradas' b^2



y/b= K figuras 'cuadradas' b^2

Y en un espacio de 3 dimensiones, de igual manera, para los ortoedros $\mathbf{y^2\ b}$ y $\mathbf{z^2\ b}$:





$(y/b)^2$= K^2 figuras 'cuadradas' b^3

$(z/b)^2$= L^2 figuras 'cuadradas' b^3

¿Qué ocurre en el caso de las figuras rectangulares **n**-dimensionales de la forma $\mathbf{y^p\, z^q\, b}$ $[(\mathbf{p, q}) \in \mathbf{N}]$? Pues sencillamente que **"no son cuadrables"**. Son imposibles de reducir a figuras cuadradas, sean del tipo $\mathbf{b^n}$ o cualquier otro y, por lo tanto, nunca podrán construir proporcionalmente de forma entera la región en el espacio definida por las formas del tipo $\mathbf{x^n}$ que estamos buscando.

No se puede 'razonar' matemática o lógicamente un lado en función de otros dos de diferente tamaño; o lo hago en función de uno, y entonces ya no es 'razón' del otro, o lo hago en función de ese otro, y entonces deja de ser 'razón' del primero. Dicho de otra manera: No existe la expresión:

$$\frac{a}{\frac{b}{c}} \;;\; \text{o es: } \frac{a/b}{c} = \frac{a}{bc} \;,\; \text{o es: } \frac{a}{b/c} = \frac{ac}{b} \;.$$

Veámoslo ahora desde un punto de vista más geométrico. Un cuadrado inscrito en otro dará lugar a 2 lados de diferente longitud respecto del que lo contiene (Ver **Fig.[A]**). 2 lados rectos de diferente longitud dan lugar a un rectángulo y la suma de 2 rectángulos construibles iguales del tamaño adecuado pueden dar lugar siempre a un tercer cuadrado menor que los otros 2.

Fig. [A]

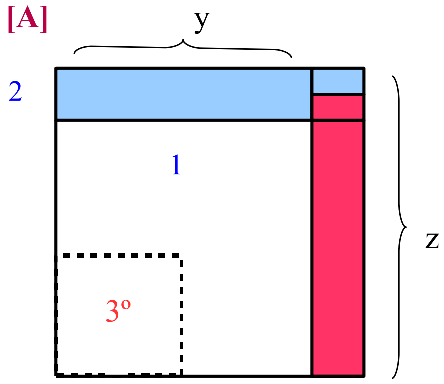
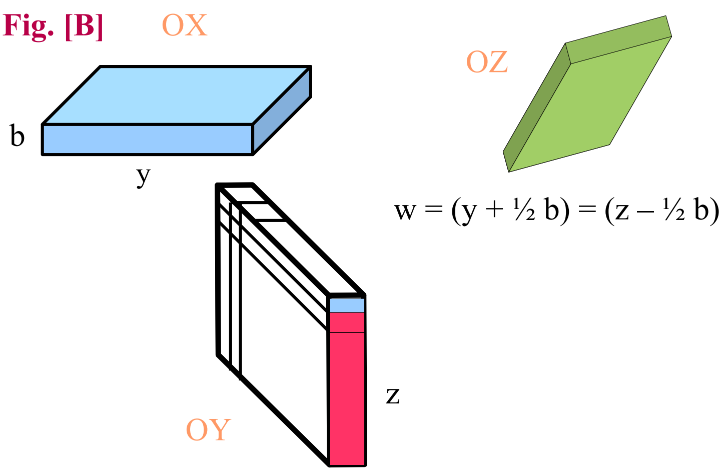


Fig. [B]



Un cubo, al igual que un cuadrado, es una figura de lados de una sola longitud. Estos lados, sin embargo, pueden ponerse también en función de otro lado de longitud distinta, en el sentido genérico en que a un número cualquiera puede corresponderle siempre funcionalmente el valor de sólo una imagen. Esto significará geométricamente que en 3 dimensiones sólo puedo obtener proporcionalmente un cubo de forma entera bien a partir de otras figuras de cubos más pequeños o bien a partir de ortoedros de sólo 2 lados de diferente longitud. Obviamente, dentro de un cubo puedo también respresentar una figura recta (ortoedro) de 3 lados diferentes; pero entonces no podría considerarla geométricamente proporcional al mismo, pues cúbicamente representará un espacio indeterminado sólo expresable mendiante números irracionales del tipo: $\mathbf{n^x}$ ó $\mathbf{x^n}$.

De esta manera, como un cubo inscrito en otro dará también lugar siempre a 2 lados de diferente longitud respecto de la longitud del lado del cubo que lo contiene. Con 2 lados rectos de diferente longitud podré construir, pues estamos en 3 dimensiones, un ortoedro y la suma de 3 ortoedros construibles iguales (en sentido OX, OY y OZ) de un tamaño adecuado, podrán dar lugar siempre también a un tercer cubo menor que los otros 2 (Ver **Fig.[B]**). Pero aquí es donde surge el problema (y la solución): no hay hueco entre el cubo inscrito y el que lo contiene para poder obtener 3 ortoedros iguales de 2 lados de diferente longitud, pues uno por fuerza deberá tener 3 lados diferentes. De este modo, jamás podré construir un tercer cubo de exponente perfecto proporcional a la perfección de los otros 2. Pues el único 'arreglo' que podría hacer para obtener otro cubo sin modificar la longitud del cubo matriz y obligarme a repetir los cálculos sin fin, es hacer no entero su exponente.

Un ejemplo. Si a las variables de la **Fig.[B]**: $\mathbf{y \wedge z}$, le doy los valores $\mathbf{3 \wedge 5}$, dado que parto que $\mathbf{y < z}$; entonces: $\mathbf{b = z - y = 2 \;\wedge\; yzb \neq w^2 b}$, pues: ó $\mathbf{3^{\,2,46 < x < 2,47}\; b = 30}$ ó $\mathbf{4^{\,1,95 < x < 1,96}\; b = 30}$ ó $\mathbf{(\sqrt{15})^2\; b = 30}$. Y en todos los casos tengo que utilizar un número irracional de infinitos decimales que no podrán representar nunca geométricamente una longitud concreta.

Más formalmente:

Para: $\mathbf{n \in \mathbb{N} \;\wedge\; x,y,z \in \mathbb{Q} \;\wedge\; (x < y < z) \;\wedge\; w = (y + ½\, b) = (z - ½\, b)}$

Como: $\mathbf{x^3 = y^2\, b + y\, z\, b + z^2\, b}$

Entonces debería cumplirse que: $\mathbf{y^2\, b + z^2\, b = 2\, yzb}$, pues partimos en la representación de: $\mathbf{2/3\; x^3 + 1/3\; x^3 = x^3}$

De esta forma: $\mathbf{2\, w^2\, b = 2\, yzb \;\wedge\; w^2 \neq yz}$

(De hecho ocurrirá siempre que: $\mathbf{y^2 + z^2 > 2yz}$)

Queda claro así porqué es imposible $\mathbf{x^3}$ en el caso visto antes, debido a la existencia de un ortoedro definido como $\mathbf{y\; z\; b}$ que hace imposible la suma en función de **figuras cuadrables** en las que se pueden descomponer los otros dos. Pero ahora hay que verlo para los casos $\mathbf{x^{n > 3}}$, donde se dan no sólo una, sino muchas de estas formas rectangulares **“no cuadrables”**. Para ello pretendo reducir la ecuación general $\mathbf{x^n}$ definida antes, a una suma, al modo del caso $\mathbf{x^3}$, de sólo 3 figuras geométricas rectangulares de regiones descritas por el producto de sus lados dimensionales:

Si:

$$x^n = y^{n-1}b + y^{n-2}z\,b + y^{n-3}z^2\,b + \_\_ + y^2z^{n-3}b + y\,z^{n-2}b + z^{n-1}b$$

Para: $K = y^{n-1}b \;\wedge\; L = z^{n-1}b \;\wedge\; M_n = b\sum_{i=1}^{n-2} y^{(n-1)-i}z^i$

Entonces: $x^n = K + M_n + L$

Y si:

$M_1 =$ **No está definido**

$M_2 =$ **No está definido**

$M_3 = y\,z\,b$

$M_4 = y^2z\,b + y\,z^2b = y\,z\,(y\,b + z\,b)$

$M_5 = y^3z\,b + y^2z^2b + y\,z^3b = y\,z\,(y^2\,b + y\,z\,b + z^2b)$

$M_6 = y^4z\,b + y^3z^2b + y^2\,z^3b + y\,z^4b$
$= y\,z\,(y^3b + y^2z\,b + y\,z^2b + z^3b)$

____________**Etc.**

Entonces: $M_n = y\,z\,x^{n-2}$

Y de esta forma: $x^n = y^{n-1}b + y\,z\,x^{n-2} + z^{n-1}\,b$

Entonces: Como comprobamos arriba, una figura cuadrada de 4 dimensiones inscrita en otra como ella que la contenga también dará lugar siempre a 2 lados de diferente longitud ($y \wedge b$) respecto de la longitud del lado de ésta y lo mismo pasará con una figura de 5 dimensiones inscrita en otra de 5 dimensiones, y con una de 6 en otra de 6... Así, siguiendo el razonamiento anterior:

$$y^{n-1}b + z^{n-1}\,b = 2\;\;y\,z\,x^{n-2} \quad \wedge$$

$$2\,w^{n-1}b = 2\;\;y\,z\,x^{n-2} \quad \wedge$$

$$w^{n-1}b = y\,z\,x^{n-2} \;\Rightarrow\; w = \sqrt[n-1]{\frac{yz}{b}}\cdot\sqrt[n-1]{x^{n-2}}$$

Por lo que **nunca**: $x^{\frac{n-2}{n-1}} = x^n$, **para** $x \in$ **Q** $\wedge$ **n > 2**

En definitiva: $\mathbf{M_n}$, frente a $\mathbf{K}$ y $\mathbf{L}$, representa una figura geométrica **"no cuadrable"**, pues está definida por el producto de 3 tipos de lados de diferente longitud; lo que hará imposible, como en el caso ya expuesto de $\mathbf{x^3}$, construir proporcionalmente de forma entera como resultado de esta suma, una figura como $\mathbf{x^n}$ de lados iguales. Y puesto que $\mathbf{M_n}$ se da siempre para $\mathbf{n > 2}$, queda así demostrado el problema planteado por Diofanto.

¿Era esta la solución que encontró Fermat?

En Sevilla, 28 de mayo de 2005

(Actualizado: 18 de julio de 2007)

Espero con gran interés vuestras noticias

solucionfermat@yahoo.es

Y en el foro:
http://www.rinconmatematico.com.ar/foros/index.php?topic=1547.0