

LA ECUACIÓN DE FERMAT

ALAN REYES-FIGUEROA
TEORÍA DE NÚMEROS

(AULA 32) 25.OCTUBRE.2024

Lema Técnico

Damos una prueba, basada en EULER, del último Teorema de Fermat, en el caso $n = 3$.

Lema

Todas las soluciones enteras positivas de

$$s^3 = a^2 + 3b^2, \text{ tales que } (a, b) = 1 \text{ y } s \text{ es impar,} \quad (1)$$

son

$$s = m^2 + 3n^2, \quad a = m^3 - 9mn^2, \quad b = 3m^2n - 3n^3, \quad (2)$$

con $m + n$ impar y $(m, 3n) = 1$.

Prueba: ($\Leftarrow$) Es relativamente fácil verificar que tales números s, a, b , producen una solución de la ecuación (1):

$$\begin{aligned} a^2 + 3b^2 &= (m^3 - 9mn^2)^2 + 3(3m^2n - 3n^3)^2 \\ &= m^6 - 18m^4n^2 + 81m^2n^4 + 27m^4n^2 - 54m^2n^4 + 27n^6 \\ &= m^6 + 9m^4n^2 + 27m^2n^4 + 27n^6 = (m^2 + 3n^2)^3 = s^3. \end{aligned}$$

Lema Técnico

Además, la hipótesis $m + n$ impar implica que m y n son de paridad distinta, de modo que $s = m^2 + 3n^2$ es impar. Además, $(m, 3n) = 1$ implica que $(m, n) = 1$ y

$$\begin{aligned}(a, b) &= (m(m^2 - 9n^2), 3n(m^2 - n^2)) = (m^2 - 9n^2, m^2 - n^2) = (8n^2, m^2 - n^2) \\ &= (8n^2, (m+n)(m-n)) = (n^2, m^2 - n^2) = (n^2, m^2) = (n, m)^2 = 1.\end{aligned}$$

($\Rightarrow$) Recíprocamente, sea (a, b, c) una solución positiva de la ecuación (1). Tome p un número primo impar, $p > 3$, tal que $p \mid s$. Como $(a, b) = 1$, y $s^3 = a^2 + 3b^2$, entonces $p \nmid a$ y $p \nmid b$. Entonces, $a^2 \equiv -3b^2 \pmod{p}$. Como b es invertible módulo p , entonces

$$-3 \equiv (ab^{-1})^2 \pmod{p}.$$

Por la ley de reciprocidad cuadrática, tenemos

$$\left(\frac{-3}{p}\right) = 1 \iff \left(\frac{p}{3}\right) = 1 \iff p \equiv 1 \pmod{6}.$$

Recordemos que la ecuación de Legendre ($ax^2 + by^2 + cz^2 = 0$) tiene solución $\Leftrightarrow -bc$ es cuadrado $\pmod{a}$, $-ca$ es cuadrado $\pmod{b}$, $-ab$ es cuadrado $\pmod{c}$.

Lema Técnico

De lo anterior, tenemos que

$$\left. \begin{array}{l} -3 \text{ es cuadrado } \pmod{p} \\ 3p \text{ es cuadrado } \pmod{1} \\ p \text{ es cuadrado } \pmod{3} \end{array} \right\} \implies -p + y^2 + 3z^2 = 0$$

tiene solución (con $x = 1$).

Así, existen enteros $m_1, n_1 \in \mathbb{Z}$ tales que $p = m_1^2 + 3n_1^2$, y se tiene que $p^3 = c^2 + 3d^2$,

donde $c = m_1^3 - 9m_1n_1^2$, y $d = 3m_1^2n_1 - 3n_1^3$.

En efecto,

$$p^3 = (m_1^2 + 3n_1^2)^3 = m_1^6 + 9m_1^4n_1^2 + 27m_1^2n_1^4 + 27n_1^6$$

y

$$\begin{aligned} c^2 + 3d^2 &= (m_1^3 - 9m_1n_1^2)^2 + (3m_1^2n_1 - 3n_1^3)^2 \\ &= m_1^6 - 18m_1^4n_1^2 + 81m_1^2n_1^4 + 27m_1^4n_1^2 - 54m_1^2n_1^4 + 27n_1^6 \\ &= m_1^6 + 9m_1^4n_1^2 + 27m_1^2n_1^4 + 27n_1^6. \end{aligned}$$

Lema Técnico

Observe que $(p, m_1) = (p, n_1) = 1$ y $p > 3$, y como $c = m_1^3 - 9m_1n_1^2$, $d = 3m_1^2n_1 - 3n_1^3$, entonces $(p, c) = (p, d) = 1$.

Procederemos a hallar la parametrización (2) por inducción sobre el número k de divisores primos de s .

- Si $k = 0$, entonces $s = 1$, y el resultado es inmediato, **pues en este caso, tenemos que $1^3 = 1^2 + 3 \cdot 0^2$, de modo que la única solución posible es $a = 1$ y $b = 0$.**
Haciendo $m = 1$ y $n = 0$, vale

$$\boxed{s = m^2 + 3n^2 = 1}, \quad \boxed{a = m^3 - 9mn^2 = 1}, \quad \boxed{b = 3m^2n - 3n^3 = 0},$$

con $m + n = 1 + 0 = 1$ impar y $(m, 3n) = (1, 0) = 1$.

- Si $k = 1$, entonces $s = p$ tiene un divisor primo es exactamente el resultado de la página anterior, en donde

$$\boxed{p = m_1^2 + 3n_1^2}, \quad \boxed{c = m_1^3 - 9m_1n_1^2}, \quad \boxed{d = 3m_1^2n_1 - 3n_1^3},$$

Lema Técnico

con $m_1 + n_1$ impar y $(m_1, 3n_1) = 1$.

Ahora, supongamos que el resultado vale para todo s impar que posee k factores primos (no necesariamente distintos). Si s tiene $k + 1$ factores primos, digamos $s = pt$, con p primo ($p > 3$), t impar, observemos que

$$t^3 p^6 = s^3 p^3 = (a^2 + 3b^2)(c^2 + 3d^2) = (ac \pm 3bd)^2 + 3(ad \mp bc)^2. \quad (3)$$

$$\begin{aligned}(ac \pm 3bd)^2 + 3(ad \mp bc)^2 &= (a^2 c^2 \pm 6abcd + 9b^2 d^2) + (3a^2 d^2 \mp 6abcd + 3b^2 c^2) \\ &= a^2(c^2 + 3d^2) + 3b^2(c^2 + 3d^2) = (a^2 + 3b^2)(c^2 + 3d^2).\end{aligned}$$

Además, como

$$(ad + bc)(ad - bc) = (ad)^2 - (bc)^2 = d^2(a^2 + 3b^2) - b^2(c^2 + 3d^2) = p^3(t^3 d^2 - b^2),$$

entonces $p^3 \mid (ad + bc)(ad - bc)$.

Afirmamos que p no puede dividir a ambos factores. Si p divide a los dos factores, tendríamos $p \mid ad$ y $p \mid bc$. Como $(p, c) = (p, d) = 1$, esto implica que $p \mid a$ y $p \mid b$, lo que

Lema Técnico

contradice la hipótesis $(a, b) = 1$. Así, p^3 divide exactamente a uno de los factores, y tomando adecuadamente el signo de este factor, se tiene

$$u = \frac{ac \pm 3bd}{p^3} \in \mathbb{Z}, \quad v = \frac{ad \mp bc}{p^3} \in \mathbb{Z}$$

son enteros tales que $t^3 = u^2 + 3v^2$, con t impar.

Son enteros, ya que de la ecuación (3) tenemos

$$\frac{1}{p^3} [(ac \pm 3bd)^2 + 3(ad \mp bc)^2] = \frac{1}{p^3} s^3 p^3 = s^3 \in \mathbb{Z},$$

y el segundo término v es entero debido a la divisibilidad por p^3 de arriba.

Asimismo,

$$u^2 + 3v^2 = \frac{1}{p^6} [(ac \pm 3bd)^2 + 3(ad \mp bc)^2] = \frac{1}{p^6} s^3 p^3 = \frac{1}{p^6} (tp)^3 p^3 = t^3.$$

Lema Técnico

Como t tiene k factores primos, se sigue de la hipótesis inductiva que

$$t = m_2^2 + 3n_2^2,$$

$$u = m_2^3 - 9m_2n_2^2,$$

$$v = 3m_2^2n_2 - 3n_2^3,$$

con $m_2 + n_2$ impar y $(m_2, 3n_2) = 1$.

Entonces

$$\begin{aligned}s &= pt = (m_1^2 + 3n_1^2)(m_2^2 + 3n_2^2) = m_1^2m_2^2 + 3m_1^2n_2^2 + 3m_2^2n_1^2 + 9n_1^2n_2^2 \\&= (m_1^2m_2^2 + 6m_1m_2n_1n_2 + 9n_1^2n_2^2) + (3m_1^2n_2^2 - 6m_1m_2n_1n_2 + 3m_2^2n_1^2) \\&= \underbrace{(m_1m_2 + 3n_1n_2)^2}_m + 3\underbrace{(m_1n_2 - m_2n_1)^2}_n,\end{aligned}$$

con m, n de paridad distinta (verifique!), y $(m, 3n) = 1$ (falta este detalle).

Lema Técnico

Ahora, como $a = uc + 3vd$ y $b = \pm(ud - vc)$, pues

$$\begin{aligned}uc + 3vd &= \frac{1}{p^3} [(ac \pm 3bd)c + 3(ad \mp bc)d] = \frac{1}{p^3} [ac^2 \pm 3bcd + 3ad^2 \mp 3bcd] \\&= \frac{1}{p^3} a(c^2 + 3d^2) = \frac{1}{p^3} ap^3 = a,\end{aligned}$$

y

$$\begin{aligned}\pm(ud - vc) &= \pm \frac{1}{p^3} [(ac \pm 3bd)d - (ad \mp bc)c] = \pm \frac{1}{p^3} [acd \pm 3bd^2 - acd \pm bc^2] \\&= \frac{1}{p^3} b(c^2 + 3d^2) = \frac{1}{p^3} bp^3 = b.\end{aligned}$$

Sustituyendo t, u, v, c, d en términos de m_i y n_i , para $i = 1, 2$, en s, a y b , resulta

$$\begin{aligned}a &= uc + 3vd = (m_1^3 - 9m_1n_1^2)(m_2^3 - 9m_2n_2^2) + 3(3m_1^2n_1 - 3n_1^3)(3m_2^2n_2 - 3n_2^3) \\&= (m_1^3m_2^3 - 9m_1n_1^2m_2^3 - 9m_1^3m_2n_2^2 + 81m_1m_2n_1^2n_2^2) + 27(m_1^2m_2^2n_1n_2 - m_1^2n_1n_2^3 - m_2^2n_2n_1^3 + n_1^3n_2^3) \\&= (m_1^3m_2^3 + 9m_1^2m_2^2n_1n_2 + 27m_1m_2n_1^2n_2^2 + 27n_1^3n_2^3) - 9(m_1^3m_2n_2^2 - 2m_1^2m_2^2n_1n_2 + m_1n_1^2m_2^3 + 3m_1^2n_1n_2^3 - 6m_1m_2n_1^2n_2^2 + 3m_2^2n_2n_1^3) \\&= (m_1m_2 + 3n_1n_2)^3 - 9(m_1m_2 + 3n_1n_2)(m_1n_2 - m_2n_1)^2 = m^3 - 9mn^2\end{aligned}$$

Lema Técnico

y

$$\begin{aligned} b &= -(ud - vc) = -[(3m_1^2n_1 - 3n_1^3)(m_2^3 - 9m_2n_2^2) - 3(m_1^3 - 9m_1n_1^2)(3m_2^2n_2 - 3n_2^3)] \\ &= -3[(m_1^2n_1m_2^3 - 9m_1^2m_2n_1n_2^2 - n_1^3m_2^3 + 9n_1^3m_2n_2^2) - (m_1^3m_2^2n_2 - 9m_1n_1^2m_2^2n_2 - m_1^3n_2^3 + 9m_1n_1^2n_2^3)] \\ &= 3[(m_1^3m_2^2n_2 - m_1^2n_1m_2^3 + 6m_1^2m_2n_1n_2^2 - 6m_1m_2^2n_1^2n_2 + 9m_1n_1^2n_2^3 - 9n_1^3m_2n_2^2) - (m_1n_2^3 - 3m_1^2m_2n_1n_2^2 + 3m_1m_2^2n_1^2n_2 - m_2n_1^3)] \\ &= 3(m_1m_2 + 3n_1n_2)^2(m_1n_2 - m_2n_1) - 3(m_1n_2 - m_2n_1)^3 = 3mn^2 - 3n^3 \end{aligned}$$

Así, los enteros $m = m_1m_2 + 3n_1n_2$ y $n = m_1n_2 - m_2n_1$, satisfacen $s^3 = a^2 + 3b^2$ y cumplen la parametrización

$$s = m^2 + 3n^2, \quad a = m^3 - 9mn^2, \quad b = 3m^2n - 3n^3.$$

Esto completa la prueba del lema $\square$.

El Último Teorema de Fermat

Damos solución al último Teorema de Fermat, para $n = 3$. Usamos descenso infinito.

Sea $(x, y, z) \in (\mathbb{Z}^+)^3$ una solución de la ecuación $x^3 + y^3 = z^3$, con xyz mínimo. Como cualquier factor común de dos de estos números es también factor del tercero, podemos suponer sin pérdida que x, y, z no tienen divisores comunes dos a dos. En particular, uno de éstos debe ser par.

Note que $x = y$ es imposible, caso contrario, tendríamos $2x^3 = z^3$, y el exponente de la mayor potencia de dos en el lado derecho es múltiplo de 3, mientras que del lado izquierdo esto no ocurre. Podemos suponer que $x > y$.

Suponga primero que x, y son ambos impares, y z es par. Podemos escribir, $x = p + q$, $y = p - q$, con $p, q > 0$, primos relativos de paridad distinta. De ahí

$$\begin{aligned}x^3 + y^3 &= (x + y)(x^2 - xy + y^2) = 2p((p + q)^2 - (p + q)(p - q) + (p - q)^2) \\&= 2p(p^2 + 2pq + q^2 - p^2 + q^2 + p^2 - 2pq + q^2) \\&= 2p(p^2 + 3q^2).\end{aligned}$$

El Último Teorema de Fermat

Portanto, $2p(p^2 + 3q^2) = z^3$ es un cubo perfecto. De igual forma, en el caso z impar y alguno de x ó y par, podemos suponer sin pérdida que y es impar, y sustituyendo $z = p + q$, $y = q - p$, resulta

$$\begin{aligned}x^3 &= z^3 - y^3 = (z - y)(z^2 + zy + y^2) = 2p((p + q)^2 + (p + q)(q - p) + (q - p)^2) \\&= 2p(p^2 + 2pq + q^2 - p^2 + q^2 + p^2 - 2pq + q^2) \\&= 2p(p^2 + 3q^2).\end{aligned}$$

Calculando el máximo divisor común entre p y $p^2 + 3q^2$, resulta

$(p, p^2 + 3q^2) = (p, 3q^2) = (p, 3)$. Tenemos portanto dos casos: $(p, 3) = 1$ ó $(p, 3) = 3$.

1. En el primer caso, existen $a, b \in \mathbb{N}$ tales que $a^3 = 2p$ y $b^3 = p^2 + 3q^2$. Por el Lema anterior, existen enteros $m, n \in \mathbb{Z}$, de diferente paridad y primos relativos, tales que

$$b = m^2 + 3n^2, \quad p = m^3 - 9mn^2, \quad q = 3m^2n - 3n^3.$$

Luego, $a^3 = 2m(m - 3n)(m + 3n)$. Observe que los números $2m, m - 3n, m + 3n$ son

El Último Teorema de Fermat

1. primos relativos (de lo contrario, m, n no serían coprimos), de modo que existen $e, f, g \in \mathbb{Z}^+$ tales que $2m = e^3$, $m - 3n = f^3$, $m + 3n = g^3$. En particular, tenemos que

$$f^3 + g^3 = (m - 3n) + (m + 3n) = 2m = e^3,$$

lo que implica que (e, f, g) es solución de la eq. de Fermat. Además, $efg \leq (efg)^3 = a^3 = 2p = x + y < xyz$, y esto contradice la minimalidad de (x, y, z) .

2. En el caso $(p, 3) = 3$, esto implica que $p = 3r$, con $(r, q) = 1$. Luego, $z^3 = 2p(p^2 + 3q^2) = 18r(3r^2 + q^2)$, y portanto existen enteros positivos a, b tales que $18r = a^3$ y $3r^2 + q^2 = b^3$. De nuevo por el Lema, existen enteros $m, n \in \mathbb{Z}^+$ tales que

$$b = m^2 + 3n^2, \quad q = m^3 - 9mn^2, \quad r = 3m^2n - 3n^3.$$

De aquí se sigue que $a^3 = 27(2n)(m - n)(m + n)$. De igual forma que en el caso anterior, los números $2n, m - n, m + n$ son primos relativos $\Rightarrow$ existen $e, f, g \in \mathbb{Z}^+$ tales que $2m = e^3$, $m - n = f^3$, $m + n = g^3$. En particular, tenemos que $f^3 + g^3 = (m - n) + (m + n) = 2m = e^3$, y (e, f, g) es solución de la eq. de Fermat.

El Último Teorema de Fermat

2. Finalmente, $efg \leq (efg)^3 = \frac{a^3}{27} < \frac{a^3}{3} = \frac{1}{3}(18r) = 6r = 2p$, lo que contradice nuevamente la minimalidad de (x, y, z) .

En cualquier caso, la existencia de una solución minimal (x, y, z) de la ecuación de Fermat, produce otra solución (e, f, g) todavía menor. Portanto, la ecuación $x^3 + y^3 = z^3$ no tiene soluciones enteras positivas. $\square$