La Ecuación de Fermat

Alan Reyes-Figueroa
Teoría de Números

(Aula 24) 19.octubre.2021

Descenso de Fermat

Dada una ecuación

$$f(x_1, x_2, \ldots, x_n) = 0,$$

el método del descenso infinito permite mostrar que esta ecuación no posee soluciones enteras positivas o, sobre ciertas condiciones, permite hallar todas sus soluciones enteras.

Si el conjunto de soluciones $A = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n : \; f(x_1, \ldots, x_n) = 0\}$ es no vacío, nos gustaría considerar la solución "mínima" en cierto sentido. En otras palabras, queremos construir una función $\phi : A \to \mathbb{N}$ y considerar la solución $(x_1, \ldots, x_n) \in A$ con $\phi(x_1, \ldots, x_n)$ mínimo.

El **método del descenso** (**descenso de Fermat**, o **descenso infinito**) consiste en obtener, a partir de esta solución mínima, otra todavía menor, lo cual claramente conduce a una contradicción, probando que A debe ser vacío.

Descenso de Fermat

Ejemplo: Encontrar todas las soluciones enteras positivas de la ecuación

$$m^2 - mn - n^2 = \pm 1.$$

Solución: Observe que $m^2 = n^2 + mn \pm 1 \geq n^2, \implies m \geq n$. Con igualdad si, y sólo si, $mn = -1 \iff (m, n) = (1, 1)$. Esta es claramente una solución.

Consideramos ahora una solución (m, n), con $m > n$. Demostramos que $(n, m - n)$ también es solución. Para ello, observe que

$$\begin{aligned} n^2 - n(m-n) - (m-n)^2 &= n^2 - nm + n^2 - m^2 + 2mn - n^2 \\ &= n^2 + nm - m^2 = -(m^2 - mn - n^2) = \mp 1. \end{aligned}$$

Así, si tenemos una solución (m, n), podemos hallar una cadena descendente de soluciones, y este proceso se detendrá cuando hallemos una solución (a, b), con $a = b$. Invirtiendo el proceso, encontramos todas las soluciones: Si (m, n) es solución, entonces $(m + n, n)$ también lo es. Portanto, todas las soluciones de la ecuación son

$$(1, 1), (2, 1), (3, 2), (5, 3), \ldots, (F_{n+1}, F_n), \ldots$$

donde F_n es el n-ésimo número de Fibonacci.

UNIVERSIDAD DEL VALLE DE GUATEMALA

Descenso de Fermat

Ejemplo: La ecuación de MARKOV. Consideramos la ecuación diofantina en enteros positivos

$$x^2 + y^2 + z^2 = 3xyz.$$

De entrada, $(1, 1, 1)$ y $(1, 1, 2)$ son soluciones. Además, como la ecuación es simétrica, sin pérdida de generalidad podemos considerar solamente las soluciones de la forma $x \leq y \leq z$, con coordenadas de forma no decreciente.
($(1, 1, 2)$ solución $\Longrightarrow$ $(1, 2, 1)$ y $(2, 1, 1)$ son soluciones).

Sea (x, y, z) una solución con $x \leq y \leq z$, y con $z \geq 1$. El polinomio cuadrático

$$T^2 - 3xyT + (x^2 + y^2) = 0,$$

posee dos soluciones: una de ellas es z, la otra es $z' = 3xy - z = \frac{x^2+y^2}{z} \in \mathbb{Z} - \{0\}$.

Veamos que si $y > 1$, entonces $z' < y$, y así (z', x, y) también es solución de la ecuación de Markov. Para ello, suponga por contradicción que $\frac{x^2+y^2}{z} = z' \geq y$, esto es, $yz \leq x^2 + y^2 \leq 2y^2$. En particular $z \leq 2y$. Se sigue que

Descenso de Fermat

$$5y^2 \geq y^2 + z^2 = 3xyz - x^2 = x(3yz - x) \geq x(3yz - y) \geq xy(3z - 1),$$

y portanto, $5y \geq x(3z - 1)$.

Ahora, observe que si $x \geq 2$, entonces $5y \geq 2(3z - 1) \geq 5z$, y portanto $x = y = z = 2$, que no es solución, lo que es un absurdo.

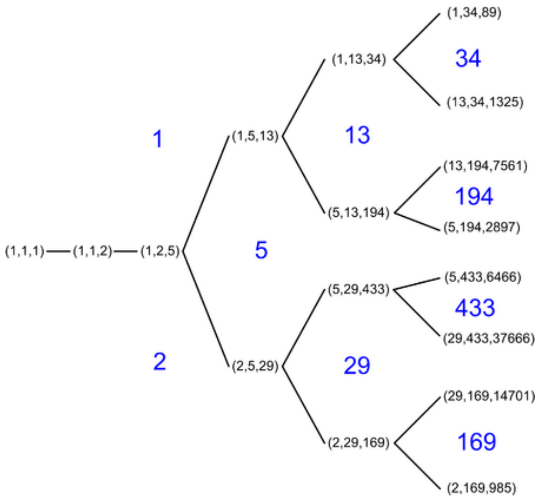
Luego, $x = 1$ y $\frac{1+y^2}{y} \geq z \;\Rightarrow\; \frac{1}{y} + y \geq z \geq y$. Portanto,

- o tenemos que $\frac{1}{y} + y = z$, y en este caso $y = 1$ y $z = 2$, lo que contradice $y > 1$;
- ó $y = z$, y sustituyendo en la ecuación original, tenemos que $1 + y^2 + y^2 = 3y^2$, lo que implica que $y = z = 1$, lo que contradice $z > 1$.

Esto muestra que $z' < y$, y (z', y, x) es solución de Markov.

Lo anterior muestra que dad una solución (x, y, z) de la ecuación de Markov, con $z \geq 2$, siempre es posible encontrar una solución menor (z', y, x), y este proceso se detiene sólo cuando alcanzamos la solución trivial $(1, 1, 1)$.

Descenso de Fermat



El Último Teorema de Fermat

Uno de los problemas más famosos en la historia de las matemáticas y talvez uno de los que más inspiró el desarrollo de nuevas teorías es el llamado **Último Teorema de Fermat**.

Pierre de Fermat (1601-1665), tenía costumbre de hacer anotaciones en las márgenes de su ejemplar de la *Arithmetica* de Diofanto. Una de estas notas, dice lo siguiente:

«Cubum autem in duos cubos, aut quadratoquadratum in duos quadratosquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere: cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.»

«Es imposible encontrar la forma de convertir un cubo en la suma de dos cubos, una potencia cuarta en la suma de dos potencias cuartas, o en general cualquier potencia más alta que el cuadrado, en la suma de dos potencias de la misma clase. He descubierto para el hecho una demostración excelente. Pero este margen es demasiado pequeño para que (la demostración) quepa en él.» Pierre de Fermat.

El Último Teorema de Fermat

Básicamente afirma que es imposible encontrar enteros $x, y, z \in \mathbb{Z}$ tales que

$$x^n + y^n = z^n,$$

cuando $n > 2$.

- 1665. FERMAT prueba el caso $n = 4$ usando el método del descenso. Muere sin dejar rastro de la prueba en el caso general.
- 1753. EULER prueba el caso $n = 3$.
- 1820. Se muestra que basta resolver los casos $n = p$ primo, los cuales se dividen en dos casos: si $p \nmid xyz$, y (caso difícil) si $p \mid xyz$.
- 1821. SOPHIE GERMAIN probó el primer caso para todo p tal que $2p + 1$ también es primo.
- 1825. LEGENDRE demuetra el caso para $n = 5$. Prueba el teorema para p primo cuando $4p + 1$, $8p + 1$, $10p + 1$, $14p + 1$ ó $16p + 1$ es primo.
- 1839. LAMÉ prueba el caso $n = 7$.

El Último Teorema de Fermat

- 1843. Kummer afirma haber demostrado el teorema pero Dirichlet encuentra un error. Prueba para todos los p primos *regulares*.
- 1909. Wiefrich prueba que si la ecuación de Fermat tiene solución para p primo, entonces $2^{p-1} \equiv 1 \pmod{p^2}$; (*primos de Wiefrich*).
- 1910s. Mirimanoff y Vandiver prueban $3^{p-1} \equiv 1 \pmod{p^2}$, $5^{p-1} \equiv 1 \pmod{p^2}$ respectivamente. Frobenius prueba para 11 y 17.
- 1995. Andrew Wiles y Richard Taylor publica la demostración del teorema, apoyados en la *Conjetura de Taniyama-Shimura-Weil*.

Solución para el caso $n = 4$:

Teorema (Fermat)

La ecuación $x^4 + y^4 = z^2$ no admite soluciones enteras positivas.

Prueba: Suponga que hay una solución entera $x^4 + y^4 = z^2$, con $x, y, z > 0$, con z el menor valor posible. Observe que (x^2, y^2, z) forman una terna pitagórica. Sin pérdida de generalidad, vamos a asumir que es x es impar, así que escribimos

$$x^2 = m^2 - n^2, \qquad y^2 = 2mn, \qquad z = m^2 + n^2,$$

para ciertos $m, n \in \mathbb{Z}$, primos relativos, $m > n$, que no son ambos impares.

La primera ecuación implica que también (x, n, m) forma una terna pitagórica, con x impar, de modo que podemos escribir

$$x = r^2 - s^2, \qquad n = 2rs, \qquad m = r^2 + s^2,$$

para $r, s \in \mathbb{Z}^+$, primos relativos, $r > s$, no ambos impares.

La última de estas tres ecuaciones implica que r, s, m son primos relativos a pares (de lo contrario, r y s no serían coprimos) y de $y^2 = 2mn = 4rsm$, deducimos que $r = a^2$, $s = b^2$ y $m = c^2$, para algunos $a, b, c \in \mathbb{Z}^+$.
(si $y = 2^k p_1^{k_1} \cdots p_t^{k_t}$, $\Rightarrow y^2 = 2^{2k} p_1^{2k_1} \cdots p_t^{2k_t}$, y estos primos se reparten entre m, r y s.)

Sustituyendo de vuelta estos valores en la ecuación para $r^2 + s^2 = m$, obtenemos $a^4 + b^4 = c^2$. Esto es, (a, b, c) sería otra solución de la ecuación original. Sin embargo

$$c \leq c^2 = m \leq m^2 < m^2 + n^2 = z,$$

y $c \neq 0$. Esto contradice la minimidad de z. Portanto, no existen soluciones enteras positivas de la ecuación. $\square$

Corolario (Último Teorema de Fermat, caso $n = 4$)

La ecuación $x^4 + y^4 = z^4$ no admite soluciones enteras positivas.

Prueba: Si $(x, y, z) \in (\mathbb{Z}^+)^3$ fuese una solución de $x^4 + y^4 = z^4$, entonces (x, y, z^2) sería solución entera positiva de $x^4 + y^4 = z^2$. $\square$

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

Lema

Todas las soluciones enteras positivas de $s^3 = a^2 + 3b^2$, *tales que* $(a, b) = 1$ *y* s *es impar, son dadas por*

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

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

Prueba: Es relativamente fácil verificar que tales números s, a, b, producen una solución de la ecuación:

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

El Último Teorema de Fermat

Además,

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

Recíprocamente, suponga que (a,b,c) es una solución entera positiva de la ecuación. Sea p un número primo tal que $p \mid s$. Note que, como $(a,b)=1$, y s es impar, entonces $p \nmid a$, $p \nmid b$ y $p>3$. Entonces, $a^2-3b^2 \pmod p$. Como b es invertible módulo p, por la ley de reciprocidad cuadrática, tenemos

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

Por el ejemplo de la clase anterior (generalización de la ecuación de suma de 2 cuadrados), 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 $d=3m_1^2n_1-3n_1^3$.

Observe que $(p,m_1)=(p,n_1)=1$ y $p>3$, de modo que $(p,c)=(p,d)=1$, como en la prueba arriba de que $(a,b)=1$.

El Último Teorema de Fermat

Procederemos por inducción sobre el número de divisores primos de s.
Si $s = 1$, el resultado es inmediato. El caso en que s tiene un divisor primo es exactamente el resultado anterior. Agora, supongamos que el resultaulo vale para todo s que posee k fatores primos (no necessarianente distintos). Si s tiene $k+1$ fatores primos, digamos $s = pt$, con p prino ($p > 3$), observemos que

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

Además, como

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

entonces $p^3 \mid (ad+bc)(ad-bc)$.
Si p divide a los dos factores, tendremos que $p \mid ad$ y $p \mid bc$. Como $(p,c) = (p,d) = 1$, esto implica que $p \mid a$ y $p \mid b$, lo que contradice la hipótesis $(a,b) = 1$. Así, p^3 divide exactamente uno de los factores, y tomando adecuadamente los signos, se tiene

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

son enteros tales que $t^3 = u^2 + 3v^2$.
Como t tiene k factores primos, se sigue de la hipótesis inductiva que

$$t = m_2^2 + 3n_2^2, \qquad u = m_2^3 - 9m_2n_2^2, \qquad v = 3m_2^2n_2 - 3n_2^3.$$

Ahora, dado que $a = uc + 3vd$ y $b = \pm(ud - vc)$, sustituyendo t, u, v, c, d en términos de m_i y n_i, para $i = 1, 2$, en s, a y b, y haciendo

$$m = m_1m_2 + 3n_1n_2, \qquad n = m_1n_2 - m_2n_1,$$

obtenemos lo que se quería demostrar.

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 pérdidad 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

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

UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

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

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

Como p^3+2q^3 es impar y $2p(p^3+3q^3)$ es cubo perfecto, tenemos que p debe ser par. 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
$$b=m^2+3n^2, \qquad p=m^3-9mn^2, \qquad q=3m^2n-3n^3.$$

El Último Teorema de Fermat

1. Luego, $a^3 = 2m(m-3n)(m+3n)$. Observe que los números $2m$, $m-3n$, $m+3n$ son primos relativos (de lo contrario, m, n no serías 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
$$b = m^2 + 3n^2, \qquad q = m^3 - 9mn^2, \qquad r = 3m^2n - 3n^3.$$
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. $\square$