Mixba'al
Revista Metropolitana de Matemáticas
No. 1, Vol. V, junio 2014, 19–24

CONJETURA DE CATALAN

MARIO HUICOCHEA

Resumen. El siguiente texto tiene un doble propósito. El primero es ver algunas de las muchas herramientas utilizadas y desarrolladas en la búsqueda de la demostración de la Conjetura de Catalan. El segundo es dar una muy breve idea de los principales pasos en la demostración de la Conjetura de Catalan realizada por P. Mihăilescu.

1. Introducción

Si un profesor de secundaria pregunta a sus alumnos qué números enteros satisfacen la ecuación

$$x^2 - y^2 = 1,$$

no serán pocos los que demuestren que $(x, y) \in \{(1, 0), (-1, 0)\}$. Del mismo modo, habrá varios que demuestren que si n es un número natural mayor a 1, entonces la ecuación

$$x^n - y^n = 1$$

tiene únicamente las soluciones $(x, y) \in \{(1, 0), (-1, 0)\}$ si n es par y $(x, y) \in \{(1, 0), (0, -1)\}$ si n es impar. Es más, un alumno de secundaria o bachillerato suficientemente avispado y motivado puede demostrar que si n y m son números naturales mayores a 1 y existe un número natural d mayor a 1 que divide a n y m, entonces alguno de los enteros x y y que resuelven la ecuación

$$x^n - y^m = 1$$

es cero; en particular esto nos permite encontrar fácilmente las soluciones enteras. Es natural entonces preguntarnos qué tantas soluciones existen si n y m son números naturales mayores que 1, posiblemente sin algún factor común, de la ecuación antes mencionada. El matemático belga Eugène Catalan [3] conjeturó en 1844 lo siguiente

Conjetura 1. (Catalan) *Si n y m son números naturales mayores que* 1 *tales que la ecuación*

$$x^n - y^m = 1 \tag{1}$$

tiene solución en los enteros distintos de 0*, entonces $n = 2, m = 3, x = 3$ y $y = 2$.*

Esta conjetura sería una de las más asediadas e intrigantes por más de 150 años; específicamente sería hasta el año 2003 que el matemático Preda Mihăilescu daría una demostración completa de la Conjetura de Catalan. El propósito de este trabajo es, en la primera parte, dar un rápido recorrido cronológico por los resultados parciales e intentos fallidos, no por ello poco enriquecedores, de la demostración de dicha conjetura y, en la segunda parte, dar una breve explicación de las ideas que llevaron a Mihăilescu a la demostración de esta famosa e interesante conjetura.

Antes de concluir esta introducción, estableceremos la notación que utilizaremos en adelante. Los conjuntos de los números racionales, enteros y naturales serán denotados por $\mathbb{Q}$, $\mathbb{Z}$ y $\mathbb{N}$ respectivamente; consideramos que el cero no es un número natural. El anillo de los enteros gaussianos es $\mathbb{Z}[i] := \{a+ib : \ a, b \in \mathbb{Z}\}$, donde $i^2 = -1$. Si $a, b \in \mathbb{Z}$, escribimos $a|b$ si existe $c \in \mathbb{Z}$ tal que $ac = b$. Si $a_1, \ldots, a_k \in \mathbb{Z}$, $\mathrm{MCD}(a_1, \ldots, a_k)$ es su máximo común divisor. Si R es un anillo, entonces $\langle a \rangle$ denota el ideal generado por

2010 *Mathematics Subject Classification.* 11-03, 11D41 ,11D45.
Palabras clave. Conjetura de Catalan, P. Mihăilescu.

$a \in R$ y R^* es el conjunto de elementos con inverso multiplicativo también conocidos como unidades. Si $\mathbb{K}$ es una extensión finita de $\mathbb{Q}$, $\mathcal{O}_{\mathbb{K}}$ el anillo de enteros de $\mathbb{K}$ es el conjunto de elementos en $\mathbb{K}$ que son raíces de polinomios mónicos con coeficientes en $\mathbb{Z}$. $\mathcal{O}_{\mathbb{K}}$ es un anillo, ver [11, Cap. 1 Sec. 2]; $I \subseteq \mathbb{K}$ es un ideal fraccionario si es un $\mathcal{O}_{\mathbb{K}}-$submódulo de $\mathbb{K}$ tal que existe un $r \in \mathcal{O}_{\mathbb{K}}, r \neq 0$ el cual cumple que $rI \subseteq \mathcal{O}_{\mathbb{K}}$, además decimos que I es principal si es generado por un elemento de $\mathbb{K}$. Si $I_{\mathbb{K}}$ es el conjunto de ideales fraccionarios y $P_{\mathbb{K}} \subseteq I_{\mathbb{K}}$ es el subconjunto de ideales fraccionarios principales, entonces $I_{\mathbb{K}}$ es un grupo (con la multiplicación), $P_{\mathbb{K}}$ es un subgrupo de $I_{\mathbb{K}}$ y el número de clases $h_{\mathbb{K}} := [I_{\mathbb{K}} : P_{\mathbb{K}}]$ es finito, ver por ejemplo [11, Cap. 1 Sec. 6]. Si $n \in \mathbb{N}$, $\zeta = \zeta_n$ denota una raíz enésima primitiva de la unidad y $\mathbb{Q}(\zeta)$ el enésimo campo ciclotómico; un resultado clásico de teoría de números, consulte por ejemplo [11, Cap. 1 Sec. 10], es que $\mathcal{O}_{\mathbb{Q}(\zeta)}$, el anillo de enteros de $\mathbb{Q}(\zeta)$, es igual a $\mathbb{Z}[\zeta]$. Finalmente, si A es un grupo conmutativo y $k \in \mathbb{N}$, entonces $[A]_k := \Big\{x \in A : \ x^{kr} = 1 \text{ para algún } r \in \mathbb{N}\Big\}$.

2. La historia de la Conjetura de Catalan

Antes de comenzar con el recorrido por la historia de la Conjetura de Catalan, notemos que basta demostrar que la conjetura es cierta en el caso en el que m y n son primos; en efecto, si encontramos una solución $x = x_0$ y $y = y_0$ de (1) cuando $x_0 y_0 \neq 0$ y alguno de m y n no es primo, sin pérdida de generalidad $m = m'm''$ con $m', m'' > 1$ enteros, entonces $x = x_0$ y $y = y_0^{m''}$ es una solución de la ecuación

$$x^n - y^{m'} = 1$$

con x y y enteros tales que $xy \neq 0$. Por lo tanto, de ahora en adelante supondremos que n y m son primos distintos.

2.1. Primeros años. El primer avance que se tiene registrado en la demostración de la Conjetura de Catalan es el caso $m = 2$ gracias a V. A. Lebesgue [7] en 1850. La herramienta fundamental es la estructura aritmética de $\mathbb{Z}[i]$.

Más de un siglo después Ko Chao [6] demostró la Conjetura de Catalan en el caso $n = 2$. También en este caso las herramientas e ideas son accesibles para cualquier persona que haya tomado un curso básico de teoría de números o teoría algebraica de números; sin embargo, las ideas son tanto ingeniosas como útiles para resolver otros problemas. Cabe mencionar que el caso $(n, m) = (2, 3)$ fue resuelto mucho antes por L. Euler [4] en 1738 con el método del descenso infinito, a grandes rasgos esto quiere decir que bajo ciertas hipótesis se demuestra que si existe una solución de números naturales a una ecuación entonces se puede encontrar otra donde los valores son menores a los valores de la solución original por lo que se puede llegar a una contradicción suponiendo que la solución original era mínima.

Un avance significativo fue el que obtuvo J.W.S. Cassels [2] en 1960.

Lema 2. (Cassels) *Si n y m son primos impares con x y y enteros distintos de cero que resuelven (1), entonces $n|y$ y $m|x$.*

De nuevo, la demostración utiliza únicamente métodos elementales. Más específicamente

$$(y+1)\left(\frac{y^m+1}{y+1}\right) = x^n \qquad \text{y} \qquad (x-1)\left(\frac{x^n-1}{x-1}\right) = y^m;$$

por otro lado

$$\text{MCD}\left((y+1), \left(\frac{y^m+1}{y+1}\right)\right) = 1 \qquad \text{ó} \qquad m|\text{MCD}\left((y+1), \left(\frac{y^m+1}{y+1}\right)\right)$$

y

$$\text{MCD}\left((x-1), \left(\frac{x^n-1}{x-1}\right)\right) = 1 \qquad \text{ó} \qquad n|\text{MCD}\left((x-1), \left(\frac{x^n-1}{x-1}\right)\right);$$

después se puede demostrar, tratando los casos por separado y notando que las potencias de los números crecen *rápido*, que $n|y^m$ y $m|x^n$ de donde se deduce el resultado.

2.2. Tijdeman *casi* lo logra. Se puede decir que los resultados hasta ahora mencionados, son obtenidos únicamente con métodos elementales[1]. El siguiente resultado de C. L. Siegel, ver [13], implica que si m y n son números fijos, entonces (1) tiene un número finito de soluciones.

TEOREMA 3. (Siegel) *Si $\mathbb{K}$ es una extensión finita de $\mathbb{Q}$, $\mathcal{O}_{\mathbb{K}}$ su anillo de enteros y C una curva suave de género positivo definida sobre $\mathbb{K}$ en un espacio afín, entonces $C(\mathcal{O}_{\mathbb{K}})$, el conjunto de puntos de C con coordenadas en $\mathcal{O}_{\mathbb{K}}$, es finito.*

Sin embargo, uno de los principales problemas de esta afirmación es que no es efectiva; en este contexto, que no sea efectivo quiere decir que aunque sepamos que el número de soluciones es finito, no sabemos desde dónde y hasta dónde buscarlas. Algunos años después A. Baker obtuvo uno de los resultados más importantes de la teoría de números del siglo XX.

TEOREMA 4. (Baker) *Sean $\alpha_1, \ldots, \alpha_n, \beta_0, \ldots, \beta_n \in \mathbb{Z}$, $\beta := \max_{0\leq i\leq n} \beta_i$ y*

$$\Lambda := \beta_0 + \sum_{i=1}^{n} \beta_i \log(\alpha_i).$$

Existe una constante c independiente de β, por ende independiente de $\beta_0, \ldots, \beta_n$, tal que si $\Lambda \neq 0$, entonces

$$\log|\Lambda| > -c \max\{\log(\beta), 1\}.$$

Este resultado tiene varias aplicaciones y a través de los años se han mejorado las cotas para c, consulte por ejemplo [1]. En particular, R. Tijdeman [15] encontró una fascinante aplicación de este resultado.

TEOREMA 5. (Tijdeman) *Si existe una solución de (1) con $xy \neq 0$, entonces existen $c_1, c_2 > 0$ constantes absolutas, tales que*

$$m \leq c_1 \log(n)^3 \qquad y \qquad n \leq c_2 m \log(n)^2.$$

En particular, existe $c_3 > 0$ una constante absoluta, tal que $\max\{m, n\} \leq c_3$.

Combinando una versión efectiva del teorema de Siegel, al menos para las curvas particulares definidas por (1), y el teorema de Tijdeman, se debería de poder concluir la demostración de la Conjetura de Catalan. Desgraciadamente, incluso con las mejoras posteriores, las constantes c_i del teorema de Tijdeman son demasiado grandes por lo que aun con otras técnicas existen $0 < c_4 < c_3$, constantes absolutas, por ejemplo $c_3 = 10^{17}$, tales que no se sabía si la Conjetura de Catalan era válida para valores de m y n tales que $c_4 < \max\{m, n\} < c_3$.

3. Demostración de Mihăilescu

Nos disponemos a dar un breve resumen de la demostración de la Conjetura de Catalan realizada por Mihăilescu; pueden consultarse [8] y [12] para ver resúmenes de la demostración más completos. Recordemos que, por lo visto anteriormente, podemos suponer que m y n son dos primos impares distintos.

[1]En matemáticas decir que algo se resuelve con métodos elementales significa que no se utilizan resultados de análisis o teorías sofisticadas; de cualquier modo el término nos parece ambiguo y fácilmente discutible.

3.1. Analogías con el Último Teorema de Fermat. A principio de los años noventa, K. Inkeri [5] tuvo la idea de realizar un trabajo similar al efectuado por E. Kummer en su intento de resolver el último teorema de Fermat. Una de las consecuencias del lema de Cassels (Lema 2) es que

$$\frac{x^n-1}{x-1}=nb^m \qquad \text{con MCD}(n,b)=1$$

y por otro lado $n=\prod_{k=1}^{n-1}(1-\zeta_n^k)$. De lo anterior, obtenemos que

$$\prod_{k=1}^{n-1}\frac{x-\zeta_n^k}{1-\zeta_n^k}=b^m.$$

No es muy difícil darse cuenta de que $\frac{x-\zeta_n^k}{1-\zeta_n^k}\in\mathbb{Z}[\zeta_n]$ y los ideales $\left\langle\frac{x-\zeta_n^k}{1-\zeta_n^k}\right\rangle$ son primos relativos por lo que existe un ideal J_k de $\mathbb{Z}[\zeta_n]$ tal que $\left\langle\frac{x-\zeta_n^k}{1-\zeta_n^k}\right\rangle=J_k^m$. Sin embargo, no siempre $\mathbb{Z}[\zeta_n]$ es un dominio de ideales principales; en particular, no podemos asegurar que J_k es generado por un elemento de $\mathbb{Z}[\zeta_n]$. En el caso en el que m es primo relativo con el número de clases de $\mathbb{Q}(\zeta_n)$ entonces J_k sí es principal; trabajando con aritmética elemental podemos concluir en este caso que $m^2|n^{m-1}-1$. De un modo muy similar se puede demostrar que si n es primo relativo con el número de clases de $\mathbb{Q}(\zeta_m)$, entonces $n^2|m^{n-1}-1$. Recapitulando, si h_n y h_m son los números de clases de los campos $\mathbb{Q}(\zeta_n)$ y $\mathbb{Q}(\zeta_m)$ respectivamente y $\text{MCD}(h_n,m)=\text{MCD}(h_m,n)=1$, entonces

$$m^2|n^{m-1}-1 \qquad \text{y} \qquad n^2|m^{n-1}-1. \tag{2}$$

Inkeri demostró que, sujetos a las condiciones $\text{MCD}(h_n,m)=\text{MCD}(h_m,n)=1$, los primos m y n tienen que ser muy particulares; tan raros son los primos que satisfacen (2) que sólo se conocen siete pares de ellos cuando $\text{máx}\{m,n\}<10^{15}$. Uno de los grandes logros de Mihăilescu, ver [9], fue demostrar que (2) debería ser cierta a pesar de que $\text{MCD}(h_n,m)>1$ ó $\text{MCD}(h_m,n)>1$.

3.2. Anuladores. A partir de esta sección, $\zeta:=\zeta_n$ es una raíz enésima primitiva de la unidad. Sea $\mathbb{K}:=\mathbb{Q}(\zeta)\cap\mathbb{R}=\mathbb{Q}\big(\zeta+\zeta^{-1}\big)$. Uno de los conjuntos que juega un papel fundamental en la demostración de la Conjetura de Catalan es $E:=\mathbb{Z}\big[\zeta+\zeta^{-1}\big]^*$ que coincide con el conjunto de unidades de $\mathcal{O}_{\mathbb{K}}$. Otro conjunto que juega un papel fundamental es C, el subgrupo de E generado por -1 y $\frac{\zeta^{\frac{k}{2}}-\zeta^{\frac{-k}{2}}}{\zeta^{\frac{1}{2}}-\zeta^{\frac{-1}{2}}}$ con $1\leq k\leq\frac{n-1}{2}$. Un hecho interesante es que $[E:C]$ no es tan sólo finito sino que además es igual a $h_{\mathbb{K}}$.

Denotamos por $\text{Gal}(\mathbb{K}/\mathbb{Q})$ al grupo de Galois de $\mathbb{K}/\mathbb{Q}$; sea G el subgrupo de $\text{Gal}(\mathbb{K}/\mathbb{Q})$ generado por los automorfismos $\tau_k:\mathbb{K}\to\mathbb{K}$ para $1\leq k\leq\frac{n-1}{2}$, donde τ_k es el automorfismo que deja fijo a $\mathbb{Q}$ y que satisface $\tau_k(\zeta+\zeta^{-1})=\zeta^k+\zeta^{-k}$. Escribimos

$$\mathbb{Z}[G]:=\left\{\sum_{k=1}^{\frac{n-1}{2}}n_k\tau_k:\ n_k\in\mathbb{Z}\text{ para todo }1\leq k\leq\frac{n-1}{2}\right\}$$

el cual actúa en $\mathbb{K}^*$ de la siguiente forma: si $g:=\sum_{k=1}^{\frac{n-1}{2}}n_k\tau_k\in\mathbb{Z}[G]$, entonces

$$x^g:=\prod_{k=1}^{\frac{n-1}{2}}\tau_k(x^{n_k})$$

para todo $x\in\mathbb{K}^*$. De manera natural, $I_{\mathbb{K}}/P_{\mathbb{K}}$ y E/C son $\mathbb{Z}[G]-$módulos . Para un $k\in\mathbb{N}$, $[I_{\mathbb{K}}/P_{\mathbb{K}}]_k$ y $[E/C]_k$ son submódulos de $I_{\mathbb{K}}/P_{\mathbb{K}}$ y E/C respectivamente.

El teorema de F. Thaine, ver [14], menciona lo siguiente

TEOREMA 6. (Thaine)[2] *Si* $m \nmid \frac{n-1}{2}$, *entonces un* $g \in \mathbb{Z}[G]$ *que anula a* $[E/C]_m$ *también anula a* $[I_{\mathbb{K}}/P_{\mathbb{K}}]_m$.

Otro resultado relativo a los anuladores, por muchos considerado el teorema que llevó a Mihăilescu [10] a la demostración de su resultado, es el siguiente.

TEOREMA 7. (Mihăilescu) *Si* $g := \sum_{k=1}^{\frac{n-1}{2}} n_k \tau_k \in \mathbb{Z}[G]$,

$$\left((x-\zeta)(x-\zeta^{-1})\right)^g \in \left\{x^m : \ x \in \mathbb{K}^*\right\},$$

y $m | \sum_{k=1}^{\frac{n-1}{2}} n_k$, *entonces* $m | n_k$ *para todo* $1 \leq k \leq \frac{n-1}{2}$.

3.3. Conclusión de la demostración. Supongamos que la conjetura es falsa. Como en la sección 2.1, $\left\langle \frac{x-\zeta}{1-\zeta} \right\rangle = J^m$ para algún ideal J de $\mathbb{Z}[\zeta]$ y de la misma manera lo es el ideal conjugado por lo que

$$\left\langle \frac{(x-\zeta)(x-\zeta^{-1})}{(1-\zeta)(1-\zeta^{-1})} \right\rangle = \left(J\overline{J}\right)^m.$$

El teorema de Thaine implica que si $g := r \sum_{i=1}^{\frac{n-1}{2}} \tau_i \in \mathbb{Z}[G]$ para algún $r \in \mathbb{N}$ satisface $E^g \subseteq C$, entonces

$$\left\langle \frac{(x-\zeta)(x-\zeta^{-1})}{(1-\zeta)(1-\zeta^{-1})} \right\rangle^g = \left\langle \gamma \right\rangle^m.$$

por lo que existe una unidad υ tal que

$$\left(\frac{(x-\zeta)(x-\zeta^{-1})}{(1-\zeta)(1-\zeta^{-1})}\right)^g = \upsilon\gamma^m. \tag{3}$$

Sin embargo $\left((1-\zeta)(1-\zeta^{-1})\right)^g \in \{\pm 1\}$. Es importante notar que υ es única módulo $(\mathbb{K}^*)^m$, en otras palabras υ' satisface (3) si y sólo si $\upsilon' = \upsilon b^m$ con $b \in \mathbb{K}^*$. Una parte técnica y difícil de la demostración es probar que existe $\eta \in C_m := \left\{z \in C : \ \exists\, s \in \mathbb{N} \text{ con } z^{sm} - 1 \in \left\langle m^2 \right\rangle\right\}$ tal que

$$((x-\zeta)(x-\zeta^{-1}))^g = \eta\lambda^m$$

con $\lambda \in \mathbb{K}$; si tomamos g' un anulador de C_m, entonces

$$((x-\zeta)(x-\zeta^{-1}))^{gg'} = \mu^m$$

con $\mu \in \mathbb{K}$, de donde se puede concluir, gracias al teorema 7, que $gg' = m\tau$ con $\tau \in \mathbb{Z}[G]$. Como $\epsilon^g \in C$ para todo $\epsilon \in E$, se puede concluir que $\epsilon^{g'} \in C$ y se demuestra que g' no tan sólo anula a C_m sino que también anula a C. Con lo anterior se puede demostrar que $C = C_m$, lo cual es imposible como demostramos a continuación. Sea C_0 el subgrupo de $\mathbb{Z}[\zeta]^*$ generado por C y ζ; como $C = C_m$ y $\zeta^{dm} = \zeta$ si $dm \equiv 1 (\text{mód } n)$, tenemos que para todo $\eta \in C_0$ existe $\rho \in \mathbb{Z}[\zeta]^*$ tal que $\eta - \rho^m \in \left\langle m^2 \right\rangle$; en particular, $1 + \zeta^m - \rho^m \in \left\langle m^2 \right\rangle$ por lo que $(1+\zeta)^m - \rho^m \in \left\langle m \right\rangle$ y concluimos que

$$(1+\zeta)^m - 1 - \zeta^m \in \left\langle m^2 \right\rangle.$$

El polinomio $P(x) = \frac{1}{m}((1+x)^m - 1 - x^m) \in \mathbb{Z}[\zeta]/\left\langle m \right\rangle[x]$ tiene al menos $n-1$ ceros en $\mathbb{Z}[\zeta]/\left\langle m \right\rangle$, por ejemplo $\zeta, \ldots, \zeta^{n-1}$ son soluciones de $P(x)$, sin embargo $P(x)$ tiene grado $m-1$ por lo que obtenemos que $n - 1 \leq m - 1$. Intercambiando los papeles de n y m llegamos a que $n - 1 \geq m - 1$ pero esto es imposible ya que asumimos que m y n no pueden ser iguales.

Agradecimientos. Agradezco a Pedro Luis Del Ángel la motivación e interés para escribir este texto y al árbitro por las múltiples y muy valiosas observaciones.

[2]Este resultado fue demostrado por primera vez antes de que Thaine lo hiciese en [14], ver [8, p.51] para más información.

Referencias

[1] Baker, A., Wüstholz, G., *Logarithmic forms and Diophantine geometry*, New Mathematical Monographs 9, Cambridge University Press, (2007).

[2] Cassels, J.W.S., *On the equation* $a^x - b^y = 1$*, II*, Proc. Cambridge Philos. Soc. 56 (1960), 97-103.

[3] Catalan, E., *Note extraite d'une lettre adressée à l'éditeur*, J. Reine Angew. Math. 27 (1844), 192.

[4] Euler, L., *Theorematum quorundam arithmeticorum demonstrationes* 56-68, Commenmationes Arithmeticae, Opere Omnia Series I, Vol II. Teubner (1915).

[5] Inkeri, K., *On Catalan's conjecture*, J. Number Theory 34 (1990), 142-152.

[6] Ko Chao, *On the diophantine equation* $x^2 = y^n + 1$*,* $xy \neq 0$, Sichun Daxue Xuebao 1 (1962), 1-6.

[7] Lebesgue, V. A., *Sur l'impossibilité en nombres entiers de l'équation* $x^m = y^2 + 1$, Nouv. Ann. Math. 9 (1850), 178-181.

[8] Metsänkylä, T., *Catalan's Conjecture: Another Old Diophantine Problem Solved*, Bull. Amer. Math. Soc. 41 (2003), 43-57.

[9] Mihăilescu, P., *A class number free criterion for Catalan's conjecture*, J. Number Theory 99 (2003), 225-231.

[10] Mihăilescu, P., *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math. 572 (2004), 167-195.

[11] Neukirch, J., *Algebraic Number Theory (Grundlehren der mathematischen Wissenschaften) vol. 322*, Springer-Verlag (2002).

[12] Schoof, R., *Catalan's Conjecture*, Universitext, Springer-Verlag, (2008).

[13] Siegel, C. L., *Über einige Anwendungen diophantischer Approximationen.* Abh. Preuss. Akad. Wiss. Phys. Math. Kl. 1 (1929), 41-69.

[14] Thaine, F., *On the ideal class groups of real abelian number fields*, Ann. of Math. 128 (1988), 1-18.

[15] Tijdeman, R., *On the equation of Catalan*, Acta Arith. 29 (1976), 197-209.

Dirección del autor:
Mario Huicochea
ETH-Zürich,
Rämistrasse 101
8006 Zürich
e-mail: `mario.huicochea@math.ethz.ch`