Conjetura de Catalan: Inkeri, Mihăilescu y Wieferich

José Cuevas Barrientos

Resumen. En ésta charla se expone un resultado de Mihăilescu que impone una *condición de Wieferich doble* (cf. corolario 2.11.1 para más precisión) sobre los exponentes de un hipotético contraejemplo a la conjetura de Catalan. Esto se puede lograr de manera casi elemental empleando un conocimiento introductorio de los cuerpos ciclotómicos, en conjunto al teorema más profundo del ideal de Stickelberger.

Índice

1. Preliminares

§1.1 Sobre cuerpos ciclotómicos. Recuérdese que una ***raíz n-ésima de la unidad*** $\omega \in \mathbb{C}$ es un número complejo para el cual $\omega^n = 1$. En el cuerpo de los complejos, todas las raíces n-ésimas de la unidad pueden ser generadas como potencias enteras de

$$\zeta_n := \exp\left(\frac{2\pi}{n}\mathrm{i}\right) = \cos\left(\frac{2\pi}{n}\right) + \mathrm{i}\sin\left(\frac{2\pi}{n}\right) \in \mathbb{C}.$$

Una raíz n-ésima de la unidad ω se dice ***primitiva*** si $\omega^k \neq 1$ para todo $0 < k < n$ entero. El teorema de De Moivre prueba que ζ_n es una raíz n-ésima primitiva de la unidad.

Definición 1.1: Un ***cuerpo ciclotómico*** es aquel de la forma $\mathbb{Q}(\zeta_n)$ para algún $n \geq 1$.

Algunos autores emplean la terminología *cuerpo ciclotómico* para los subcuerpos de algún $\mathbb{Q}(\zeta_n)$, lo cual es más general. No obstante, no emplearemos estos objetos en lo sucesivo.

Fecha: 22 de septiembre de 2023.

Teorema 1.2: Sea $q := p^r$ una potencia de un primo y sea $\zeta := \zeta_q$.

1. El anillo de enteros algebraicos de $\mathbb{Q}(\zeta)$ es $\mathbb{Z}[\zeta]$.
2. El elemento $\pi := 1 - \zeta$ es primo en $\mathbb{Z}[\zeta]$ y, como ideales, $(p) = (\pi)^{\phi(q)}$.
3. p es el único primo que se ramifica; es decir, si r es otro primo en $\mathbb{Z}$, entonces su factorización prima en ideales es $r = \mathfrak{q}_1 \cdots \mathfrak{q}_g$, donde los $\mathfrak{q}_i \lhd \mathbb{Z}[\zeta]$ son primos distintos.

Demostración: Cf. Washington [**4,** págs. 2, 11], lemma 1.4 y thm. 2.6; o Janusz [**2,** pág. 52], thm. 10.1. □

Proposición 1.3: Sea $p > 2$ primo, y sea $\zeta := \zeta_p$. Dado $\epsilon \in \mathbb{Z}[\zeta]^\times$, existen $\epsilon' \in \mathbb{Q}(\zeta + \zeta^{-1})$ y $r \in \mathbb{Z}$, tales que $\epsilon = \zeta^r \epsilon'$.

Demostración: Cf. [**4,** pág. 3], prop. 1.5. □

Definición 1.4: Un ***dominio de Dedekind*** A es un dominio íntegro en donde hay factorización prima única sobre ideales, vale decir, donde todo ideal propio $\mathfrak{a} \lhd A$ se escribe de manera única (salvo orden) como

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n},$$

donde cada $\mathfrak{p}_i$ es un ideal primo distinto.

Si incluímos a los *ideales fraccionarios* entonces los ideales no nulos (con el producto de ideales) forman un grupo multiplicativo abeliano libre generado por los ideales primos. El cociente de ese grupo, por el subgrupo de los ideales principales, se denomina el ***grupo de clases*** $\operatorname{Cl} A$ de A. El orden de dicho grupo se llama el ***número de clases*** $h(A)$ de A.

Es un resultado clásico de la teoría algebraica de números que todo anillo de enteros es un dominio de Dedekind (cf. [**2,** págs. 26, 46], thm. 6.1); por ello enfatizamos factorizaciones de ideales. El siguiente también es un resultado folclórico:

Teorema 1.5: Sea A un anillo de enteros algebraicos. Entonces su grupo de clases $\operatorname{Cl} A$ (y, por tanto, su número de clases $h(A)$) es finito.

Demostración: Cf. [**2,** pág. 72], thm. 13.8. □

La última noción nueva es la de *álgebra de grupo*:

Definición 1.6: Sea G un grupo. Definimos el anillo $\mathbb{Z}[G]$ como el grupo libre (en notación aditiva) con generadores en G con la siguiente multiplicación:

$$\left(\sum_{g \in G} a_g g\right) \cdot \left(\sum_{g \in G} b_g g\right) = \sum_{h \in G} \sum_{h = g_1 g_2} a_{g_1} b_{g_2} h.$$

Sea $K/\mathbb{Q}$ una extensión de Galois con $G := \mathrm{Gal}(K/\mathbb{Q})$, entonces $\mathbb{Z}[G]$ tiene una acción sobre el grupo multiplicativo $K^\times$ dada por (en notación exponencial):

$$\alpha^{\sum_{\sigma\in G} b_\sigma \sigma} := \prod_{\sigma\in G} \sigma(\alpha)^{b_\sigma}.$$

§1.2 Sobre la conjetura de Catalan. Recordemos que la ***ecuación de Catalan*** es

$$x^n - y^m = 1, \qquad n, m > 1;$$

es decir, si dos potencias son consecutivas. Salta a la vista que $1^n - 0^m = (-1)^{2n} - 0^m = 0^n - (-1)^{2m+1} = 1$ son soluciones que denominaremos ***triviales***.

Definición 1.7: La ***conjetura de Catalan*** dice que la única solución no trivial de la ecuación de Catalan es $(\pm 3)^2 - 2^3 = 1$. Un ***contraejemplo de Catalan*** es una cuadrupla (x, y, p, q) tal que $x^p - y^q = 1$ distinta de las soluciones triviales y de la solución descrita arriba.

La prueba de Preda Mihăilescu de la conjetura de Catalan es una larga demostración por contradicción en la que vamos imponiendo condiciones cada vez más restrictivas sobre un contraejemplo de Catalan.

Una observación elemental: basta probar que no hay contraejemplos de Catalan con exponentes primos distintos. Que los exponentes sean distintos sale trivialmente de la cota

$$(x+1)^p - x^p = px^{p-1} + \cdots > p,$$

para $x > 0$. Que los exponentes sean primos se sigue de que si $n = ap, m = bq$, entonces

$$x^n - y^m = (x^a)^p - (y^b)^q.$$

Proposición 1.8: Sean A, B enteros coprimos y p un número primo.

1. Si p divide a uno de los números $\dfrac{A^p - B^p}{A - B}$ o $A - B$, entonces divide al restante.
2. Sea $d := \mathrm{mcd}\left(\dfrac{A^p - B^p}{A - B}, A - B\right)$ entonces $d \in \{1, p\}$.
3. Si $p > 2$ y $d = p$, entonces:

$$\nu_p\left(\frac{A^p - B^p}{A - B}\right) = 1.$$

Demostración: Cf. Bilu *et al.* [**1,** pág. 15], lemma 2.8. □

Teorema 1.9 (Euler-Lebesgue-Ko Chao): Un contraejemplo de Catalan tiene exponentes impares.

Demostración: Cf. [**1,** págs. 11-25], thm. 2.1, thm. 2.10, thm. 2.15. □

La ventaja es que, de éste modo, un contraejemplo de Catalan $x^p - y^q = 1$ implica que $(-y)^q - (-x)^p = 1$ también sea un contraejemplo de Catalan. Esta simetría será útil más adelante.

Teorema 1.10 (relaciones de Cassels): Si (x, y, p, q) es un contraejemplo de Catalan, entonces $p \mid y$ y simétricamente $q \mid x$.

Demostración: Cf. [**1,** pág. 28], thm. 3.3. □

Nótese que éste es una generalización de un teorema de Nagell (cf. [**1,** pág. 16], thm. 2.9) para el caso de exponentes pares.

Corolario 1.10.1: Si (x, y, p, q) es un contraejemplo de Catalan, entonces existen a, b no nulos y $u, v > 0$ tales que:

$$x - 1 = p^{q-1}a^q, \qquad \frac{x^p - 1}{x - 1} = pu^q, \qquad y = pau,$$

y simétricamente

$$y + 1 = q^{p-1}b^p, \qquad \frac{y^q + 1}{y + 1} = qv^p, \qquad x = qbv.$$

2. Teoremas de divisibilidad superior

Lema 2.1 (principal): Sea (x, y, p, q) un contraejemplo de Catalan. Sea $\zeta := \zeta_p$. Entonces el número

$$\lambda := \frac{x - \zeta}{1 - \zeta} \in \mathbb{Z}[\zeta]$$

es un entero algebraico, y existe un ideal $\mathfrak{a} \lhd \mathbb{Z}[\zeta]$ tal que $(\lambda) = \mathfrak{a}^q$.

Demostración: Recuérdese (teorema 1.2) que $\pi := 1 - \lambda$ es un primo de $\mathbb{Z}[\zeta]$ y que $(p) = (\pi)^{p-1}$. Por las relaciones de Cassels, $p \mid x - 1$, de modo que $x \equiv 1 \equiv \zeta \pmod{\pi}$, pero $\pi^2 \nmid x - \zeta$ (¿por qué?), de modo que λ es un entero algebraico y $\pi \nmid \lambda$.

Definiendo $\lambda_j := x - \zeta^j/(1 - \zeta^j)$, entonces lo mismo se concluye para λ_j. Como

$$\zeta^n - \zeta^m = (x - \zeta^m) - (x - \zeta^n) = (1 - \zeta_p^m)\lambda_m - (1 - \zeta_p^n)\lambda_n,$$

de modo que para $1 \leq n < m < p$ tenemos que si $\gamma \mid \zeta^n$ y $\gamma \mid \zeta^m$, entonces $(\gamma) \supseteq (\zeta^n - \zeta^m) = (\pi)$; de modo que los números $\lambda_1, \ldots, \lambda_{p-1}$ son coprimos dos a dos.

Ahora, como

$$\Phi_p(t) := \frac{t^p - 1}{t - 1} = (t - \zeta)(t - \zeta^2) \cdots (t - \zeta^{p-1})$$

se tiene que

$$\frac{x^p-1}{x-1}\cdot\frac{1}{p}=\frac{\Phi_p(x)}{\Phi_p(1)}=\lambda_1\cdots\lambda_{p-1}.$$

Por las relaciones de Cassels, tenemos que $\lambda_1\cdots\lambda_{p-1}=u^q$ para algún $u\in\mathbb{Z}$ y, como los λ_i's son coprimos dos a dos, entonces cada $(\lambda_i)=\mathfrak{a}^q$. □

Proposición 2.2: Sea (x,y,p,q) un contraejemplo de Catalan. Entonces $q^2\mid x$ syss $p^{q-1}\equiv 1 \pmod{q^2}$.

Demostración: Como $q\mid x$ por las relaciones de Cassels, entonces $p^{q-1}a^q\equiv -1 \pmod q$. Como $p^{q-1}\equiv 1\ (q)$ por el pequeño teorema de Fermat, entonces $a^q\equiv -1\ (q)$ y $a\equiv -1\ (q)$.

Por el lema 1.8, si $A^q\equiv B^q\ (q)$, entonces $A^q\equiv B^q\ (q^2)$ y, en particular, $a^q\equiv -1\ (q)$. Así, que $p^{q-1}\equiv 1\ (q^2)$ equivale a que $q^2\mid x$. □

Proposición 2.3: Sea (x,y,p,q) un contraejemplo de Catalan tal que $q\nmid h_p$, donde h_p es el número de clases de $\mathbb{Q}(\zeta_p)$. Entonces

$$\mu:=\frac{1-\zeta_p x}{1-\overline{\zeta}_p x}\in\mathbb{Q}(\zeta_p)$$

es una potencia q-ésima (en $\mathbb{Q}(\zeta_p)$).

Pista: Empleamos el lema principal notando que la condición de que $q\nmid h_p$ implica que el ideal $\mathfrak{a}$ del enunciado sea principal. Los elementos del lema se recuperan salvo una unidad que, con la proposición 1.3 podemos suponer real. □

Lema 2.4: Sea K un cuerpo numérico, sea $\mathfrak{q}\lhd\mathcal{O}_K$ un primo y sean

$$\alpha,\beta\in\mathfrak{o}_{\mathfrak{q}}:=\{\gamma\in K:\nu_{\mathfrak{q}}(\gamma)\geq 0\}.$$

Sea $(q)=\mathfrak{q}\cap\mathbb{Z}$. Si $\alpha^q\equiv\beta^q \pmod{\mathfrak{q}}$, entonces $\alpha^q\equiv\beta^q \pmod{\mathfrak{q}^2}$.

Demostración: Como $0\equiv\alpha^q-\beta^q\equiv(\alpha-\beta)^q\ (\mathfrak{q})$, entonces se sigue que $\alpha\equiv\beta\ (\mathfrak{q})$, vale decir, existe $\gamma\in\mathfrak{q}$ tal que $\alpha=\beta+\gamma$. Luego

$$\alpha^q=\beta^q+\gamma\sum_{j=1}^{q-1}\binom{q}{j}\gamma^{j-1}+\gamma^q.$$

Basta notar que $q\mid\gamma$ y $q\mid q=\binom{q}{1}$ para concluir. □

Lema 2.5: Sea K un cuerpo numérico y sea $\mathfrak{q}\lhd\mathcal{O}_K$ primo. Para todo $n\in\mathbb{Z}$ y todo $\alpha\in K$ con $\nu_{\mathfrak{q}}(\alpha)>0$, se tiene que

$$(1+\alpha)^n\equiv 1+n\alpha \pmod{\mathfrak{q}^2}.$$

Teorema 2.6 (de divisibilidad de Inkeri): Sea (x, y, p, q) un contraejemplo de Catalan. Si $q \nmid h_p$, entonces $q^2 \mid x$.

Demostración: Sean $\zeta := \zeta_p$ y $K := \mathbb{Q}(\zeta)$. Como q no se ramifica en K, basta probar que $\mathfrak{q}^2 \mid x$ para algún $\mathfrak{q} \mid q$ en $\mathcal{O}_K$. Como $q \mid x$ (por las relaciones de Cassels), entonces $\mu := (1-\zeta x)/(1-\overline{\zeta}x)$ satisface que $\mu \equiv 1 \pmod{\mathfrak{q}}$ y, como μ es una potencia q-ésima, entonces por el lema 2.4 tenemos que $\mu \equiv 1 \pmod{\mathfrak{q}^2}$.

Por otro lado, el lema anterior implica que $(1-\overline{\zeta}x)^{-1} \equiv 1+\overline{\zeta}x \pmod{\mathfrak{q}^2}$, de modo que

$$1 \equiv \mu \equiv (1-\zeta x)(1+\overline{\zeta}x) = 1 + (\overline{\zeta}-\zeta)x \pmod{\mathfrak{q}^2},$$

y como $\nu_{\mathfrak{q}}(\overline{\zeta}-\zeta) = 0$ (¿por qué?), concluimos que $\mathfrak{q}^2 \mid x$ como se quería probar. □

Corolario 2.6.1: Sea (x, y, p, q) un contraejemplo de Catalan. Entonces, o bien $q \mid h_p$ o $p^{q-1} \equiv 1 \pmod{q^2}$.

La segunda condición se llama *condición de Wieferich* y sus implicancias son enormes, reduciendo bastante la cantidad de primos.

Proposición 2.7: Sea (x, y, p, q) un contraejemplo de Catalan. Sean $\zeta := \zeta_p, K := \mathbb{Q}(\zeta), G := \mathrm{Gal}(K/\mathbb{Q})$ e $\iota \in G$ la conjugación compleja. Si $\theta \in \mathbb{Z}[G]$ aniquila el grupo de clases $\mathrm{Cl}(\mathbb{Z}[\zeta])$, vale decir, si para todo ideal $\mathfrak{a} \lhd \mathbb{Z}[\zeta]$ se cumple que $\mathfrak{a}^\theta$ es principal. Entonces $(1-\zeta x)^{(1-\iota)\theta}$ es una q-ésima potencia en K.

Demostración: Sea $\lambda := (x-\zeta)/(1-\zeta) \in \mathbb{Z}[\zeta]$ (por el lema principal) y sea $(\lambda) =: \mathfrak{a}^q$. Por hipótesis, $\mathfrak{a}^\theta = (\alpha)$, por lo que, $\lambda^\theta = \eta\alpha^q$ para algun $\eta \in \mathbb{Z}[\zeta]^\times$ y, quizá modificando α, podemos suponer que η es real. Luego $(\lambda/\overline{\lambda})^\theta = (\alpha/\overline{\alpha})^q$ es una potencia q-ésima, por lo que

$$(1-\zeta x)^{(1-\iota)\theta} = \left(\frac{1-\zeta x}{1-\overline{\zeta}x}\right)^\theta = \left(\frac{\zeta}{\overline{\zeta}} \cdot \frac{1-\overline{\zeta}}{1-\zeta}\right)^\theta \cdot \left(\frac{\overline{\lambda}}{\lambda}\right)^\theta = (-\zeta)^\theta \left(\frac{\overline{\alpha}}{\alpha}\right)^q,$$

la cual es una potencia q-ésima. □

Proposición 2.8: Sea (x, y, p, q) un contraejemplo de Catalan. Sean $\zeta := \zeta_p, K := \mathbb{Q}(\zeta), G := \mathrm{Gal}(K/\mathbb{Q})$ e $\iota \in G$ la conjugación compleja. Si $\theta \in \mathbb{Z}[G]$ satisface que $(1-\zeta x)^\theta$ sea una potencia q-ésima y tal que $q \nmid \theta$ (en $\mathbb{Z}[G]$). Entonces $q^2 \mid x$ (en $\mathbb{Z}$).

Demostración: Sea $\mathfrak{q} \lhd \mathbb{Z}[\zeta]$ un primo tal que $\mathfrak{q} \cap \mathbb{Z} = q\mathbb{Z}$ (sin fijar). Basta probar que $\mathfrak{q}^2 \mid x$. Como $q \mid x$ por relaciones de Cassels, entonces $\mathfrak{q} \mid x$, de modo que $(1-\zeta x)^\theta \equiv 1 \pmod{\mathfrak{q}}$ y como $(1-\zeta x)^\theta$ es una potencia q-ésima,

entonces por el lema 2.4, tenemos que

$$(1-\zeta x)^{\theta} \equiv 1 \pmod{\mathfrak{q}^2}.$$

Sea $\theta := \sum_{\sigma\in G} a_\sigma \sigma$, como $q \nmid \theta$, entonces $q \nmid a_\tau$ para un $\tau \in G$. Como $\{\sigma\zeta : \sigma \in G\}$ es una $\mathbb{Z}$-base de $\mathbb{Z}[\zeta]$, entonces $q \nmid \sum_{\sigma\in G} a_\sigma \zeta^\sigma =: \alpha$. Debido a que q no se ramifica en $\mathbb{Z}[\zeta]$, entonces sea $\mathfrak{q}$ un primo tal que $\mathfrak{q} \mid q$ y $\mathfrak{q} \nmid \alpha$.

Aplicando el lema 2.5 tenemos que

$$(1-\zeta x)^{\theta} = \prod_{\sigma\in G} (1-\zeta^\sigma x)^{a_\sigma} \equiv 1 - x\sum_{\sigma\in G} a_\sigma \zeta^\sigma = 1-\alpha x \pmod{\mathfrak{q}^2},$$

como $(1-\zeta x)^\theta \equiv 1 \ (\mathfrak{q}^2)$ concluimos que $\nu_{\mathfrak{q}}(\alpha x) \geq 2$, pero $\nu_{\mathfrak{q}}(\alpha) = 0$ por construcción, por lo que $\mathfrak{q}^2 \mid x$ como se quería probar. □

Entonces lo que necesitamos es un θ que cumpla lo anterior, lo que viene dado por:

Definición 2.9: Sea $p > 2$ primo, $K := \mathbb{Q}(\zeta_p)$ un cuerpo ciclotómico y denotemos por $G := \mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_p\}$ donde $\sigma_j(\zeta_p) = \zeta_p^j$. Definimos el ***elemento de Stickelberger***

$$\Theta_S := \sum_{a=1}^{p-1} a\sigma_a^{-1} \in \mathbb{Q}[G].$$

Teorema 2.10 (de Stickelberger): El elemento de Stickelberger aniquila el grupo de clases de $\mathbb{Z}[\zeta_p]$.

Demostración: Cf. [**4,** pág. 94], thm. 6.10. □

Teorema 2.11 (de Mihăilescu): Sea (x, y, p, q) un contraejemplo de Catalan, entonces $q^2 \mid x$, y simétricamente $p^2 \mid y$.

Corolario 2.11.1: Sea (x, y, p, q) un contraejemplo de Catalan, entonces $p^{q-1} \equiv 1 \pmod{q^2}$, y simétricamente $q^{p-1} \equiv 1 \pmod{p^2}$.

Definición 2.12: Un par de primos distintos $\{p, q\}$ tales que $p^{q-1} \equiv 1 \ (q^2)$ y $q^{p-1} \equiv 1 \ (p^2)$ se dice un ***par de Wieferich doble***.

Para dimensionar lo fuerte que es la condición de Wieferich doble, gracias a un computador podemos buscar ejemplos y todos los que existen con $\min\{p, q\} \leq 3{,}2 \times 10^8$ son (cfr. Keller y Richstein [**3**]):

$$(2, 1093), \quad (3, 1006003), \quad (5, 1645333507), \quad (5, 188748146801),$$
$$(83, 4871), \quad (911, 318917), \quad (2903, 18787).$$

Referencias

1. Bilu, Y. F., Bugeaud, Y. y Mignotte, M. *The Problem of Catalan* (Springer International Publishing Switzerland, 2014).
2. Janusz, G. J. *Algebraic Number Fields* 2.ª ed. *Graduate Studies in Mathematics* **7** (American Mathematical Society, 1973).
3. Keller, W. y Richstein, J. Solutions of the congruence $a^{p-1} \equiv 1 \pmod{p^r}$. *Math. Comp.* **74,** 927-936. www.jstor.org/stable/4100096 (2005).
4. Washington, L. C. *Introduction to Cyclotomic Fields Graduate Texts in Mathematics* **83** (Springer-Verlag New York, 1982).

Correo electrónico: josecuevasbtos@uc.cl

Departamento de Matemáticas, Pontificia Universidad Católica de Chile.
Facultad de Matemáticas, 4860 Av. Vicuña Mackenna, Macul, RM, Chile
URL: josecuevas.xyz