Formas lineales en logaritmos

Francisco Gallardo

1. Introducción histórica

La primera definición de número trascendente, como conocemos hoy, fue dada por Euler en el siglo XVIII. En 1768, Lambert conjetura que e y π son trascendentes en el mismo artículo donde prueba que π es irracional. Sin embargo, no fue hasta 1844 que Liouville logró demostrar la existencia de números trascendentes. En 1873, Hermite demuestra que e es trascendente y en 1874 Cantor demuestra que estos abundan usando su teoría de cardinales infinitos. En 1882, Lindemann demuestra que π es trascendente y, más en general:

Teorema 1.1 (Lindemann, 1882): Si $\alpha \neq 0$ es algebraico, entonces e^{α} es trascendente.

Así, si π fuese algebraico, entonces $2\pi\mathrm{i}$ también, y luego $e^{2\pi\mathrm{i}} = 1$ sería trascendente por el teorema anterior, lo que es absurdo.

En 1885, Weierstrass generaliza el teorema de Lindemann:

Teorema 1.2 (Lindemann-Weierstrass, 1885): Sean $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ distintos. Luego $e^{\alpha_1}, \ldots, e^{\alpha_n}$ son linealmente independientes sobre $\overline{\mathbb{Q}}$.

Y en el año 1900 Hilbert postula, dentro de su lista de 23 problemas, uno que tendría relación con trascendencia:

> **Séptimo problema de Hilbert:** Si $\alpha \neq 0, 1$ es algebraico y $b \notin \mathbb{Q}$, ¿es $a^b := \exp(b \log a)$ trascendente?

Nótese que a^b es multivaluado, puesto que el logaritmo complejo lo es, así que la pregunta hace alusión a cualquiera de los posibles valores.

En 1934, Gelfond y Schneider independientemente dan una respuesta afirmativa al séptimo problema de Hilbert y, por ende, el resultado adquiere el nombre de «teorema de Gelfond-Schneider».

En 1966, Alan Baker generalizó el teorema de Gelfond-Schneider usando *formas lineales en logaritmos*, de las cuales tratará esta exposición. Cabe destacar que, después de las ideas de Baker, la llamada *teoría de la trascendencia* ha tenido sorpresivas repercusiones en las ecuaciones diofántincas, la

Fecha: 17 de mayo de 2024.

geometría diofántica y la aproximación diofántica; por lo que, resulta una herramienta esencial para teoristas de números.

2. Formas lineales en logaritmos

Empezamos con nuestro estudio de logaritmos de números algebraicos.

Proposición 2.1: Sea $\alpha \neq 0, 1$ algebraico. Luego $\log \alpha$ es trascendente.

Demostración: Como $\alpha \neq 1$, entonces $\log \alpha \neq 0$. Si $\beta = \log \alpha$ fuera algebraico, entonces por el teorema de Lindemann se tendría que $\alpha = e^{\beta}$ sería trascendente, lo que es absurdo. □

La pregunta a continuación es si existe un Lindemann-Weierstrass logarítmico, vale decir:

Definición 2.2: Diremos que se satisface la propiedad $L(n)$ para $n \geq 1$ entero si: Para todo conjunto $\alpha_1, \ldots, \alpha_n$ de números algebraicos no nulos tales que $\log \alpha_1, \ldots, \log \alpha_n$ son $\mathbb{Q}$-linealmente independientes, se satisface que $\log \alpha_1, \ldots, \log \alpha_n$ son $\mathbb{Q}^{\text{alg}}$-linealmente independientes.

Observación 2.2.1: Los α's del problema son distintos de 1 y distintos entre si, pues de lo contrario el conjunto de logaritmos no sería $\mathbb{Q}$-linealmente independiente. Una combinación $\mathbb{Q}^{\text{alg}}$-lineal de tales logaritmos se denomina una ***forma lineal en logaritmos***.

El caso $n = 1$ es por supuesto trivial. Sin embargo, el caso $n = 2$ ya es bastante complicado:

Proposición 2.3: Son equivalentes:

1. Se satisface el teorema de Gelfond-Schneider.
2. La afirmación $L(2)$ es válida.

Demostración: $1 \implies 2$. Supongamos que

$$\beta_1 \log \alpha_1 + \beta_2 \log \alpha_2 = 0.$$

Si $\beta_1 = 0$, entonces β_2 también pues $\log \alpha_2 \neq 0$. Luego $\log \alpha_2 = -\frac{\beta_1}{\beta_2} \log \alpha_1$ y entonces $\alpha_2 = \alpha_1^{\gamma}$ con $\gamma = -\beta_1/\beta_2$. Como α_2 es algebraico, el teorema de Gelfond-Schneider implica que $\alpha_1 \in \{0, 1\}$ o bien que $\gamma \in \mathbb{Q}$. Así pues, necesariamente $\gamma \in \mathbb{Q}$. En dicho caso dividiendo la relación de dependencia original por β_2 da un relación de dependencia sobre $\mathbb{Q}$ entre $\log \alpha_1$ y $\log \alpha_2$, lo que es absurdo.

$2 \implies 1$. Sea $\alpha \notin \{0, 1\}$ algebraico y sea $\beta \notin \mathbb{Q}$. Supongamos, por contradicción, que $\gamma := \alpha^{\beta}$ es algebraico. Luego $1 \cdot \log \gamma + (-\beta) \log \alpha = 0$ y

α, γ son algebraicos distintos de 0 y 1. Por $L(2)$ se tiene que $\beta = 0 \in \mathbb{Q}$, lo que es absurdo. □

Sorprendentemente, $L(n)$ es cierto para todo n. Esto fue una consecuencia del teorema de Baker:

Teorema 2.4 (Baker, 1966): Sean $\alpha_1, \ldots, \alpha_n \neq 0$ algebraicos tales que $\log \alpha_1, \ldots, \log \alpha_n$ son $\mathbb{Q}$-linealmente independientes. Luego

$$1,\ \log \alpha_1,\ \ldots,\ \log \alpha_n$$

son $\mathbb{Q}^{\text{alg}}$-linealmente independientes.

En otras palabras, dados $\alpha_1, \ldots, \alpha_n \neq 0, 1$ algebraicos el teorema nos da condiciones para que la expresión

$$\Lambda = \beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n, \quad \beta_i \in \overline{\mathbb{Q}}, \quad 1 \leq i \leq n.$$

sea no nula. Por ejemplo, si los logaritmos de los α_i's son $\mathbb{Q}$-linealmente independientes, entonces $\Lambda \neq 0$ por el teorema. Como corolario tenemos lo siguiente:

Corolario 2.4.1: Si $\beta_0 \neq 0$, entonces $\Lambda \neq 0$. Si $\beta_0 = 0$ y $\beta_1, \ldots, \beta_n$ son $\mathbb{Q}$-linealmente independientes.

Es importante que no se pida la independencia de los logaritmos.

Si bien conocer que $\Lambda \neq 0$ es ya de interés, para aplicaciones es necesario dar una cota inferior de $|\Lambda|$ en caso de que sea no nulo. En esta línea tenemos el siguiente resultado de Baker, 9 años después:

Teorema 2.5 (Baker, 1975): Sean $\alpha_1, \ldots, \alpha_n \neq 0, 1$ algebraicos. Existe una constante (computable) $C > 0$ que depende solo de los α_j que satisface lo siguiente:

Si $\beta_1, \ldots, \beta_n \in \mathbb{Z}$ cumplen que $\Lambda \neq 0$, entonces

$$|\Lambda| \geq (1 + B)^{-C}$$

donde $B = \max_j |\beta_j|$. Es decir, $-\log |\Lambda| \leq C \log(1 + B)$.

Esto ha sido mejorado y generalizado en varias direcciones. Al día de hoy el mejor resultado en $\mathbb{C}$ es de Matveev. Para enunciarlo definimos la altura de un número racional p/q con $\gcd(p, q) = 1$ como

$$H(p/q) = \log \max\{|p|, |q|\}.$$

Además, para $t \geq 0$ definimos $\log^* t := \max\{1, \log t\}$.

Teorema 2.6 (Matveev, 2000): Sean $\alpha_1, \ldots, \alpha_n \in \mathbb{Q}$ no nulos y sean $b_1, \ldots, b_n \in \mathbb{Z}$ tales que $\Lambda \neq 0$. Entonces

$$-\log|\Lambda| \leq \kappa^n (\log^* B) \prod_{j=1}^{n} \log^* H(\alpha_j),$$

donde $B = \max_j |b_j|$ y $\kappa \leq 100$ es una constante computable.

En particular, nos da una versión explícita del teorema de Baker, con

$$C = 100^n \prod_{j=1}^{n} \log^* H(\alpha_j).$$

Para aplicaciones esta fórmula para C es crucial.

Además, uno puede traducir los resultados de Baker y Matveev a una versión multiplicativa usando la siguiente observación de cálculo:

Lema 2.7: Sea $L \in \mathbb{R}$ con $|L| \leq 1$. Entonces

$$|1 - e^L| \geq \frac{|L|}{2}.$$

Demostración: Sea $-1 \leq L \leq 1$ un número real. La expansión de Taylor-MacLaurin de $f(L) = \frac{e^L - 1}{L}$ es

$$1 + \frac{L}{2} + \frac{L^2}{6} + \frac{L^3}{24} + \cdots$$

Si $L \geq 0$, es claro que $|f(L)| \geq 1 \geq 1/2$. Si L es negativo luego es claro que $|f(L)| \geq \frac{1}{2}$. □

En particular, los «espacios» (eng. *gaps*) se vuelven arbitrariamente grandes.

Teorema 2.8 (Baker, versión multiplicativa): Sean $\alpha_1, \ldots, \alpha_n \neq 0, 1$ algebraicos. Existe una constante computable $C > 0$ tal que, si $\beta_1, \ldots, \beta_n \in \mathbb{Z}$ son tales que $\Lambda \neq 0$, entonces

$$-\log|1 - \alpha^{\beta_1} \cdots \alpha_n^{\beta_n}| \leq C \log^* B.$$

Demostración: Por el lema anterior,

$$\begin{aligned} -\log|1 - \alpha^{\beta_1} \cdots \alpha_n^{\beta_n}| &= -\log|1 - e^{\Lambda}| \\ &\leq -\log \frac{|L|}{2} \leq C \log\left(1 + \frac{B}{2}\right) \leq C \log^* B. \end{aligned}$$ □

Similarmente obtenemos:

Teorema 2.9 (Matveev, versión multiplicativa): Sean $\alpha_1, \dots, \alpha_n \in \mathbb{Q}$ no nulos y sean $b_1, \dots, b_n \in \mathbb{Z}$ tales que $\alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n} =: e^{\Lambda} \neq 1$. Entonces

$$-\log|1 - \alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n}| \leq \kappa^n (\log^* B) \prod_{j=1}^{n} \log^* H(\alpha_j),$$

donde $B = \max_j |b_j|$ y $\kappa \leq 100$ es una constante computable.

Cuando las formas cuentan con solo dos términos hay cotas mucho mejores.

Teorema 2.10 (Laurent-Mignotte-Festerenko, 1995): Sean $a_1, a_2 \neq 1$ racionales y b_1, b_2 enteros no nulos tales que $\Lambda = b_1 \log a_2 - b_2 \log a_1 \neq 0$. Luego

$$\log|\Lambda| \geq$$
$$-22 \left(\max \left\{ 21, \log\left(\frac{|b_1|}{\log H(a_2)} + \frac{|b_2|}{\log H(a_1)} \right) + 0{,}06 \right\} \right)^2 \log H(a_1) \log H(a_2).$$

Antes de continuar a las aplicaciones, cabe mencionar que estos resultados tienen análogos en el mundo p-ádico y estos son también importantes en muchas aplicaciones. Por ejemplo:

Teorema 2.11 (Yu, 1986): Sea p un número primo y $a_1, \dots, a_m$ racionales no-nulos y no divisibles por p. Sean además $b_1, \dots, b_m$ enteros tales que $a_1^{b_1} \cdots a_m^{b_m} \neq 1$ y sea $B = \max_{1 \leq i \leq m} |b_i|$. Luego

$$|a_1^{b_1} \cdots a_m^{b_m} - 1|_p \geq (eB)^{-C}$$

para una constante computable C que depende de p y $a_1, \dots, a_m$.

3. Aplicaciones de formas lineales en logaritmos

Proposición 3.1: Sean $a, b \geq 2$. Luego existe una constante computable C, dependiendo de a y b, tal que para todo $m, n \in \mathbb{Z}_{>0}$ se cumple que

$$|a^m - b^n| \geq \frac{\max\{a^m, b^n\}}{\max\{m, n\}^C}.$$

En particular, podemos tomar $C = 10000 \log^* a \log^* b$.

Demostración: Sea $k = a^m - b^n$. Por el teorema de Matveev

$$-\log|k/a^m| = -\log|1 - a^{-m} b^n| \leq \log^* \max\{m, n\}.$$

Como $\max\{m, n\} \geq 3 > e$, reescribiendo el término de la izquierda obtenemos

$$m \log a - \log|k| \leq C \log \max\{m, n\}$$

y luego

$$|k| \geq \frac{a^m}{\text{máx}\{m,n\}^C}.$$

El mismo análisis se puede hacer si dividimos por b^n en vez de a^m al principio y el teorema sigue. □

Como consecuencia, si $a^m - b^n = 1$ con a, b fijos, entonces m y n están acotados por una constante computable C'. En 1844 Catalan conjeturó que la ecuación $a^m - b^n = 1$ con $a, b > 0$ y $m, n > 1$ tenía solo por solución: $3^2 - 2^3 = 1$. La proposición que acabamos de probar muestra que la conjetura de Catalan admite finitos contraejemplos, fijando a y b. Sin embargo, la constante C es ridículamente grande en nuestra proposición y no sirve para probar la conjetura.

En su lugar, una proposición un tanto mejor fue dada por Tijdeman:

Teorema 3.2 (Tijdeman, 1976): Sea K un cuerpo numérico. Existen una constante computable C tal que las soluciones de la ecuación diofántica exponencial

$$x^m - y^n = 1, \qquad m, n \in \mathbb{N}_{>1};\ x, y \in \mathbb{Z}_{>0}$$

satisfacen que $\text{máx}\{m, n, |x|, |y|\} \leq C$. En consecuencia, posee a lo más finitas soluciones.

Demostración: Cfr. Bilu *et al.* [**2,** págs. 176 ss.], Thm. 13.19. □

Éste todavía no nos permite responder la conjetura de Catalan, puesto que las cotas siguen siendo demasiado grandes para computadores; pero el teorema de Tijdeman sigue siendo útil puesto que tiene validez en contexto de S-enteros (vid. Brindza [**3**]).

Respecto a la conjetura original de Catalan, esta fue resuelta por Preda Mihăilescu. Una demostración completa y autocontenida está expuesta en el libro de Bilu *et al.* [**2**].

Para la siguiente aplicación nos planteamos primero la siguiente situación. Ciertamente, el TFA asegura que todo número se puede escribir como producto de primos. Sin embargo, si restringimos los primos a un conjunto finito, podríamos preguntarnos qué números pueden escribirse como producto de ellos. Más precisamente, para todo conjunto finito de primos S tenemos el conjunto de

$$\mathbb{N}_S := \left\{ \prod_{p \in S} p^{\alpha_p} : \alpha_p \geq 0 \right\}.$$

Como $\mathbb{N}_S$ es numerable, enumeraremos por $s_1, s_2, s_3, \ldots$ sus elementos y preguntarnos sobre los saltos entre estos (i.e, $g_n = s_{n+1} - s_n$).

Proposición 3.3: Sea $S = \{p_1, \dots, p_t\}$ un conjunto finito de primos y sean s_n y g_n como en la discusión anterior. Luego existen constantes computables c_1, c_2 que dependen de S y tales que

$$g_n \geq \frac{s_n}{c_1(\log s_n)^{c_2}}$$

para todo $n \geq 1$.

DEMOSTRACIÓN: Sea $s_n = p_1^{a_1} \cdots p_t^{a_t}$ y $s_{n+1} = p_1^{b_1} \cdots p_t^{b_t}$. Luego por Baker multiplicativo obtenemos

$$-\log \frac{g_n}{s_n} = -\log \left| \frac{g_n}{s_n} \right| = -\log \left| 1 - \frac{s_{n+1}}{s_n} \right| = \log |1 - p_1^{b_1 - a_1} \cdots p_t^{b_t - a_t}| \leq C \log^* B$$

donde $B = \max_{1 \leq i \leq t}\{|b_i - a_i|\}$.

Primero notemos que, como $p_i^{a_i} \leq s_n$, entonces

$$a_i \leq \frac{\log s_n}{\log p_i} \leq \frac{\log s_n}{\log 2}.$$

Además, como $a_{n+1} \leq a_n^2$, tenemos

$$b_i \leq \frac{\log s_{n+1}}{\log p_i} \leq \frac{2 \log s_n}{\log 2}.$$

Esto muestra que $B \leq \frac{2 \log s_n}{\log 2}$.

Juntando esto con la desigualdad dada del teorema de Baker obtenemos

$$|g_n| \geq \frac{s_n}{c_1(\log s_n)^{c_2}}.$$

□

Por último daremos una aplicación a las estimaciones del teorema 2.10.

Proposición 3.4: La ecuación

$$x^n - 2y^n = 1, \quad x, y \in \mathbb{Z}_{\geq 2}$$

no tiene soluciones para $n > 6726$.

DEMOSTRACIÓN: Sean x, y, n enteros con $x, y \geq 2$, $n \geq 3$ y $x^n - 2y^n = 1$. Luego $|1 - 2(y/x)^n| = 1/x^n \leq 1/2$. Usando la cota

$$|\log(1 + z)| \leq 2|z|, \quad z \in \mathbb{R},\ |z| \leq \frac{1}{2}$$

con $z = 2(y/x)^n - 1$ obtenemos

$$|\log 2 + n \log(y/x)| \leq 2/x^n = 2e^{-n \log x}.$$

Por otro lado el teorema 2.10 usando $\Lambda = \log 2 + n \log(y/x)$ implica

$$\log |\Lambda| \geq -22 \left(\max \left\{ 21, \log \left(\frac{1}{\log x} + \frac{n}{\log 2} \right) + 0{,}06 \right\} \right)^2 \log 2 \log x$$

$$\geq -22\left(\text{máx}\left\{21, \log\left(\frac{n+1}{\log 2}\right) + 0{,}06\right\}\right)^2 \log 2 \log x$$
$$\geq -22(\text{máx}\{21, \log(n+1) + 0{,}43\})^2 \log 2 \log x.$$

Combinando esta cota inferior con la superior obtenida al principio sigue que

$$n \log x - \log 2 \leq 22(\text{máx}\{21, \log(n+1) + 0{,}43\})^2 \log 2 \log x.$$

Dividiendo por $\log x$ y usando $\log x \geq \log 2$ obtenemos

$$n \leq 22(\text{máx}\{21, \log(n+1) + 0{,}43\})^2 \log 2 + 1.$$

Si el máximo en cuestión es 21, obtenemos $n \leq 22 \cdot (21)^2 \log 2 + 1 < 6726$. Si el máximo es $\log(n+1) + 0{,}43$, entonces obtenemos

$$n \leq \log 2(\log(n+1))^2 + 0{,}86 \log(n+1) \log 2 + 0{,}1849 \log 2 + 1.$$

Con un cálculo sencillo, es fácil ver de que esta desigualdad es imposible para $n > 760$. □

4. Relación con *abc*

Como habíamos mencionado antes, la teoría de formas lineales en logaritmos se generaliza a los números p-ádicos y en este contexto se obtienen teoremas similares en cuanto a la no anulación efectiva de este tipo de formas. Usando esta teoría, se obtienen los siguientes resultados relacionados al problema *abc*.

Teorema 4.1 (Stewart-Tijdeman, 1986): Existe una constante computable K tal que, para todos los $a, b, c \in \mathbb{Z}$ con $a + b = c$ y $\gcd(a, b, c) = 1$ se tiene

$$\log c < K \cdot \text{Rad}(abc)^{15}.$$

Con resultados más innovadores de Yu en cuanto a formas lineales en logaritmos p-ádicos, se mejoró a lo siguiente.

Teorema 4.2 (Stewart-Yu,1991): Para todo $\varepsilon > 0$, existe una constante computable K_ε tal que, para todos los $a, b, c \in \mathbb{Z}$ con $a + b = c$ y $\gcd(a, b, c) = 1$ se tiene

$$\log c < K_\varepsilon \cdot \text{Rad}(abc)^{\frac{2}{3}+\varepsilon}.$$

Finalmente en 2001, los mismo autores lograron mejorar su resultado:

Teorema 4.3 (Stewart-Yu, 2001): Para todo $\varepsilon > 0$, existe una constante computable K_ε tal que, para todos los $a, b, c \in \mathbb{Z}$ con $a + b = c$ y $\gcd(a, b, c) = 1$ se tiene

$$\log c < K_\varepsilon \cdot \text{Rad}(abc)^{\frac{1}{3}+\varepsilon}.$$

Terminaremos esta sección dando un resultado demostrado por Pastén en 2022, donde el exponente de los teoremas anterior baja a ε cuando asumimos que el $a < c^{1-\eta}$ para algún η positivo. En el curso de la demostración usaremos el siguiente lema que incluimos sin demostración:

Lema 4.4: Sea $\varepsilon > 0$. Luego para n suficientemente grande se tiene que

$$\omega(n) < (1+\varepsilon)\frac{2\log n}{\log\log n}$$

donde $\omega(n) = \#\{p \text{ primo} : p \mid n\}$.

Teorema 4.5 (Pastén, 2022): Sean $\eta, \varepsilon > 0$. Existe una constante $K_{\eta,\epsilon} > 0$ que cumple lo siguiente: Dados enteros positivos coprimos a, b, c, con $a + b = c$ y $a < c^{1-\eta}$, se tiene

$$\log c < K_{\eta,\varepsilon} \cdot \mathrm{Rad}(abc)^{\varepsilon}.$$

Demostración: Sea S el conjunto de primos que divide a bc. Sea $R = \mathrm{Rad}\, bc = \prod_{q\in S} q$ y sea $n = \omega(R) = \#S$.

Luego,

$$\frac{a}{c} = 1 - \frac{b}{c} = 1 - \prod_{q\in S} q^{e_q}$$

donde $e_q \in \mathbb{Z}$ para $q \in S$. Sea $B = \max_{q\in S} |e_q|$.

Por el teorema de Matveev (v. multiplicativa) y el hecho de que $a < c^{1-\eta}$, obtenemos que

$$\eta \log c = -\log \frac{a}{c} = -\log \left| 1 - \prod_{q\in S} q^{e_q} \right| \leq \kappa^n \log B \prod_{q\in S} \log q.$$

Afirmamos que $B \leq \log H(b/c) = \log c$. Ciertamente, si escribimos

$$\frac{b}{c} = \frac{\prod\limits_{\substack{q\in S \\ e_q>0}} q^{e_q}}{\prod\limits_{\substack{q\in S \\ e_q<0}} q^{-e_q}},$$

entonces $\log H(b/c) = \sum_{\substack{q\in S \\ e_q<0}} |e_q| \log q \geq |e_q|$ para todo $q \in S$ con $e_q < 0$. Si $q \in S$ con $e_q > 0$, entonces

$$|e_q| = e_q \leq \sum_{\substack{q\in S \\ e_q>0}} e_q \log q = \log b \leq \log c = \log H(b/c).$$

Esto muestra lo afirmado. Usando esto y la desigualdad proveniente de Matveev obtenemos

$$\frac{\eta \log c}{\log\log c} \leq \kappa^n \cdot \prod_{q\in S} \log q.$$

Usando la desigualdad ma-mg obtenemos

$$\prod_{q\in S} \log q \leq \left(\frac{1}{n}\sum_{q\in S} \log q\right)^n = \left(\frac{1}{n}\log R\right)^n$$

y entonces se sigue que

$$\frac{\eta \log c}{\log\log c} \leq \left(\frac{\kappa}{n}\log R\right)^n.$$

Cuando $c \gg_\eta 1$ (i.e, c es suficientemente grande dependiendo de η), entonces

$$\sqrt{\log c} < \frac{\eta \log c}{\log\log c}$$

y obtenemos

$$\sqrt{\log c} < \left(\frac{\kappa}{n}\log R\right)^n.$$

A continuación obtendremos una desigualdad para el lado derecho. Consideremos la función $f\colon (0,\infty) \to \mathbb{R}$ dada por

$$f(t) = \log\left(\left(\frac{A}{t}\right)^t\right) = t\log A - t\log t$$

para A fijo. Luego $f'(t) = \log A - \log t - 1$ y entonces $f'(t) \geq 0$ para $1 \leq t \leq A/e$. Esto implica que f es creciente en ese tramo.

Notemos que $f(n) = \left(\frac{\kappa}{n}\log R\right)^n$ con $A = \kappa \log R$.

Además, $n = \omega(R) < 2\log R/\log\log R$ para $R \gg 1$, y para $R \gg 1$ (aún más grande posiblemente) $n < \kappa \log R/e$. Como en dicho tramo la función es creciente, entonces

$$\begin{aligned} f(n) = \left(\frac{\kappa}{n}\log R\right)^n &\leq \left(\frac{\kappa \log\log R}{2}\right)^{\frac{2\log R}{\log\log R}} \\ &= \left(\frac{\kappa R}{2}\right)^{\frac{2\log\log\log R}{\log\log R}} \ll_\varepsilon R^\varepsilon, \end{aligned}$$

donde la última desigualdad viene de que el exponente tiende a 0 cuando R crece y la igualdad viene de que

$$(\log\log R)^{\log R} = (\log R)^{\log\log\log R}$$

(si aplica log a ambos números será evidente la igualdad).

Juntando nuestras desigualdades obtenemos

$$\sqrt{\log c} \ll_\varepsilon R^\epsilon$$

para $c \gg_\eta 1$ y $R \gg 1$. Elevando al cuadrado obtenemos lo pedido. □

5. Ecuaciones de unidades: Introducción y caso 1

Sea K un cuerpo de característica 0 y $\Gamma \subseteq K^\times$ un subgrupo finitamente generado.

Una ecuación de unidades es una ecuación de la forma

$$a_1x_1 + \cdots + a_nx_n = 1$$

donde los a_i están en $K^\times$ y se busca resolver para $x_i \in \Gamma$.

Lo interesante de estas ecuaciones es que muchas ecuaciones diofánticas se pueden llevar a una de este tipo. Típicamente K es un cuerpo numérico y $\Gamma = \mathcal{O}_K^\times$.

Nos concentraremos en ecuaciones de unidad para $n = 2$, i.e, la ecuación

$$ax + by = 1, \quad a, b \in K^\times,\ x, y \in \Gamma. \tag{1}$$

En este contexto, Siegel probó en 1921 la finitud de soluciones para el caso en que K es un cuerpo numérico y $\Gamma = \mathcal{O}_K^\times$. Mahler en 1933 probó finitud en el caso $K = \mathbb{Q}$ y Γ el conjunto de S-unidades (i.e, S es un conjunto finito de primos en $\mathbb{Z}$ y una S-unidad es un racional cuyo numerador y denominador solo contiene potencias de los primos en S). Para S-unidades en cuerpo numérico la finitud fue probada por Parry en 1950. El caso general con K cuerpo de característica 0 y $\Gamma \leq K^\times$ finitamente generado fue probado por Lang en 1960. De esta forma, tenemos el siguiente teorema:

Teorema 5.1 (Siegel-Mahler-Parry-Lang, 1960): La ecuación (1) tiene finitas soluciones.

En 1979, Győry encontró una cota para las alturas de la soluciones de (1) usando los resultados efectivos de Baker sobre formas lineales en logaritmos.

En esta sección probaremos el teorema 5.1 en el caso $K = \mathbb{Q}$ y en el caso que K es cuerpo numérico y $\Gamma = \mathcal{O}_K^\times$.

Lidiemos con el primer caso. Lo primero que veremos es que nos podemos reducir al caso de S-unidades. Ciertamente, si $\gamma_1, \ldots, \gamma_r$ son generadores de Γ, entonces si $S = \{p_1, \ldots, p_t\}$ denota el conjunto de primos que ocurren en las factorizaciones de los numeradores y denominadores de $a, b, \gamma_1, \ldots, \gamma_r$, entonces $a, b, \gamma_1, \ldots, \gamma_r$ son S-unidades, i.e, viven dentro de

$$\mathbb{Z}_S^\times = \{\pm p_1^{e_1} \cdots p_t^{e_t} \mid e_t \in \mathbb{Z}\}.$$

Si (x, y) es solución de (1) (en el caso que estamos cubriendo), entonces ax y by son S-unidades también, de modo que nos reducimos a probar la finitud de las soluciones de

$$x + y = 1, \quad x, y \in \mathbb{Z}_S^\times. \tag{2}$$

Teorema 5.2: La ecuación (1) tiene finitas soluciones y el conjunto de soluciones se puede determinar de manera efectiva cuando $K = \mathbb{Q}$.

DEMOSTRACIÓN: Como ya habíamos dicho, basta reducirse al caso de S-unidades y considerar la ecuación (2).

Sean entonces $x, y \in \mathbb{Z}_S^\times$ tales que $x + y = 1$. Primero escribimos $x = u/w$ $y = v/w$ con u, v, w enteros y $\gcd(u, v, w) = 1$. Así, $u + v = w$.

Luego los enteros u, v y w están compuestos por primos en S y además $\gcd(u, v, w) = 1$ y $u + v = w$ implica que u, v, w son coprimos dos a dos.

Reordenando posiblemente nuestra lista de primos podemos y nuestro enteros u, v, w podemos asumir que

$$u = \pm p_1^{b_1} \cdots p_r^{b_r}, \quad v = \pm p_{r+1}^{b_{r+1}} \cdots p_s^{b_s}, \quad w = \pm p_{s+1}^{b_{s+1}} \cdots p_t^{b_t},$$

con $0 \leq r \leq s \leq t$ y b_i enteros no negativos.

Estamos listos si logramos probar que $B = \max\{b_1, \ldots, b_t\}$ está acotado superiormente por una constante computable. Por simetría podemos asumir $B = p_t$. Como

$$-\left(\frac{u}{v}\right) - 1 = -\left(\frac{w}{v}\right),$$

tenemos que

$$p_t^{-B} = p_t^{-b_t} = |w/v|_{p_t} = |\pm p_1^{b_1} \cdots p_r^{b_r} p_{r+1}^{-b_{r+1}} \cdots p_s^{-b_s} - 1|_{p_t} > 0.$$

Del teorema 2.11 obtenemos que

$$| \pm p_1^{b_1} \cdots p_r^{b_r} p_{r+1}^{-b_{r+1}} \cdots p_s^{-b_s} - 1|_{p_t} > (eB)^{-C}$$

donde C es computable en términos de los p_i.

Pero luego

$$p_t^{-B} > (eB)^{-C}$$

y entonces

$$\frac{B}{1 + \log B} \leq \frac{C}{\log p_t}.$$

Esto implica que B está acotado (el lado de la izquierda tiende a infinito cuando B crece). □

6. Ecuaciones de unidades: Caso 2

Ahora veremos el caso 2, i.e, consideramos la ecuación (1) con K un cuerpo numérico y $\Gamma = \mathcal{O}_K^\times$.

Para ello, recuérdese el siguiente resultado clásico:

Teorema 6.1 (de las unidades de Dirichlet): Sea K un cuerpo numérico con r_1 lugares reales y r_2 lugares imaginarios, donde $r := r_1 + r_2 - 1$. La función

$$\operatorname{Log}\colon \mathcal{O}_K^\times \longrightarrow \mathbb{R}^r, \qquad \alpha \longmapsto (\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_r(\alpha)|)$$

es un homomorfismo de grupos, su núcleo $\ker(\operatorname{Log})$ es el grupo μ de raíces de la unidad en K e $\operatorname{Img}\operatorname{Log}$ es un reticulado de rango r. En particular, $\mathcal{O}_K^\times \cong \mathbb{Z}^r \times \mu$.

DEMOSTRACIÓN: Cfr. NEUKIRCH [**5,** págs. 42, 358], Thm. I.7.4 y Prop. VI.1.1. □

Esto implica que existen $\varepsilon_1, \ldots, \varepsilon_r \in \mathcal{O}_K^\times$ tales que para todo $\varepsilon \in \mathcal{O}_K^\times$,

$$\varepsilon = \zeta \varepsilon_1^{b_1} \cdots \varepsilon_r^{b_r}, \quad \zeta \in U_K,\ b_i \in \mathbb{Z}.$$

Más aún, la matriz

$$M = \begin{pmatrix} \log|\sigma_1(\varepsilon_1)| & \cdots & \log|\sigma_1(\varepsilon_r)| \\ \vdots & \ddots & \vdots \\ \log|\sigma_r(\varepsilon_1)| & \ldots & \log|\sigma_r(\varepsilon_r)| \end{pmatrix}$$

es invertible.

Por último, necesitaremos el siguiente lema.

Lema 6.2: Existe una constante $C > 0$ tal que, si $\varepsilon \in \mathcal{O}_K^\times$ con $\varepsilon = \zeta \prod_{i=1}^r \varepsilon_i^{b_i}$, entonces

$$\max_{1\le i\le r} |b_i| \le C \cdot \max_{1\le i\le d} \log|\sigma_i(\varepsilon)|.$$

DEMOSTRACIÓN: Sea $v = (b_1 \cdots b_r)^t$ el vector columna asociado. Luego $L(\varepsilon) = Mv$, de modo que $v = M^{-1}L(\varepsilon)$. Escribiendo $M^{-1} = (a_{ij})$ obtenemos

$$b_i = \sum_{j=1}^r a_{ij} \log \sigma_j(\varepsilon)$$

para $1 \le i \le r$. Usando la desigualdad triangular concluimos que

$$\max_{1\le i\le r} |b_i| \le \left(\max_{1\le i\le r} \sum_{j=1}^r |a_{ij}| \right) \cdot \max_{1\le i\le r} \log|\sigma_j(\varepsilon)|. \qquad \square$$

Ahora sí, el teorema.

Teorema 6.3: La ecuación (1) tiene finitas soluciones y estas se pueden determinar de manera efectiva, en el caso en que K es cuerpo numérico y $\Gamma = \mathcal{O}_K^\times$.

DEMOSTRACIÓN: Sean $x, y \in \mathcal{O}_K^\times$ y $a, b \in K^\times$ tales que

$$ax + by = 1.$$

Escribimos

$$x = \zeta_1 \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r} \qquad x = \zeta_2 \varepsilon_1^{b_1} \cdots \varepsilon_r^{b_r}$$

con $a_i, b_i \in \mathbb{Z}$ y $\zeta_1, \zeta_2 \in U_K$. Luego

$$a\zeta_1 \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r} + b\zeta_2 \varepsilon_1^{b_1} \cdots \varepsilon_r^{b_r} = 1.$$

Daremos cotas inferiores y superiores de

$$\Lambda_i := |\sigma_i(a)\sigma_i(\zeta)\sigma_i(\varepsilon_1)^{a_1} \cdots \sigma_i(\varepsilon_r)^{a_r} - 1| = |\sigma_i(b)\sigma_i(y)|$$

para un valor específico de i.

Sean i y j los índices que minimizan y maximizan resp. a los $|\sigma_k(y)|$ para $1 \leq k \leq d$. Luego

$$|\sigma_i(y)|^{d-1}|\sigma_j(y)| \leq \prod_{i=d}^{r} |\sigma_i(y)| = |\mathrm{Nm}_{K/\mathbb{Q}}(y)| = 1. \tag{3}$$

Del lema anterior sigue $B \leq C \cdot \log|\sigma_j(y)|$. Luego $e^{B/C} \leq |\sigma_j(y)|$ y entonces $|\sigma_j(y)|^{-\frac{1}{d-1}} \leq e^{-\frac{B}{C(d-1)}}$. Juntando esto con (3) se sigue que

$$|\sigma_i(y)| \leq e^{-\frac{B}{C(d-1)}}.$$

Se sigue que

$$|\Lambda_i| \leq |\sigma_i(b)|e^{-\frac{B}{C(d-1)}}.$$

Por otro lado, el teorema de Baker implica

$$|\Lambda_i| \geq (1+B)^{-C'}$$

para una constante computable C' que depende de a, las unidades fundamentales $\varepsilon_1, \ldots, \varepsilon_r$ y la finitas raíces de la unidad en K. Deducimos entonces que

$$(1+B)^{-C'} \leq |\sigma_i(b)|e^{-\frac{B}{C(d-1)}}$$

y nos entrega una cota computable para B. □

En 1984, Evertse mostró que la cantidad de soluciones de dicha ecuación está acotado por $3 \cdot 7^{d+2r}$ donde $d = [K : \mathbb{Q}]$. En 1996, Beukers y Schlickewei dieron la cota uniforma 512^{r+2}.

7. Aplicaciones de ecuaciones de unidades

La primera aplicación será dar finitud a ciertas formas binarias.

Proposición 7.1: Sea $F(x,y) = a_0x^d + a_1x^{d-1}y + \cdots + a_{d-1}xy^{d-1} + a_dy^d \in \mathbb{Z}[x,y]$ una forma binaria irreducible de grado $d \geq 3$ tal que $F(x,1)$ tiene al menos 3 ceros distintos en $\mathbb{C}$. Luego la ecuación

$$F(x,y) = m$$

para un $m \in \mathbb{Z}$ tiene finitas soluciones enteras y estas pueden ser determinadas de manera efectiva.

Demostración: Primero nos reducimos al caso $a_0 = 1$. Ciertamente, $G(x,y) := F(a_0x, y) = a_0^{d-1}F(x,y)$ es una forma binaria con coeficientes enteros y sus soluciones se corresponden con las de la ecuación $G(x,y) = a_0^{d-1}m$. Esto muestra que la reducción es posible.

Sea K el cuerpo de escisión de $F(x,1)$, de modo que

$$F(x,y) = (x - \alpha_1 y)(x - \alpha_1 y)\cdots(x - \alpha_d y)$$

con $\alpha_1, \ldots, \alpha_d \in \mathcal{O}_K$. Luego la ecuación $F(x,y) = m$ implica que los $(x - \alpha_i y)$ dividen a $m \in \mathcal{O}_K$ y por ende

$$(x - \alpha_i y) = \mu_i \beta_i, \quad \mu_i \in \mathcal{O}_K,\ \beta_i \in \mathcal{O}_K^\times$$

para todo $1 \leq i \leq d$. Como $\mathrm{Nm}_{K/\mathbb{Q}}(\mu_i) \leq \mathrm{Nm}_{K/\mathbb{Q}}(m)$ para todo i, solo hay finitas elecciones para los μ_i. Veremos que también es el caso para los β_i.

Reordenando si es necesario, supongamos que α_1, α_2 y α_3 son ceros distintos. Mediante combinaciones lineales de los $(x - \alpha_i y) = \mu_i \beta_i$, $i = 1, 2, 3$ podemos eliminar los x e y para obtener:

$$(\alpha_2 - \alpha_3)\mu_1\beta_1 + (\alpha_3 - \alpha_1)\mu_2\beta_2 = (\alpha_1 - \alpha_2)\mu_3\beta_3.$$

Pero entonces

$$\left(\frac{(\alpha_2 - \alpha_3)\mu_1}{(\alpha_1 - \alpha_2)\mu_3}\right)\frac{\beta_1}{\beta_3} + \left(\frac{(\alpha_3 - \alpha_1)\mu_2}{(\alpha_1 - \alpha_2)\mu_3}\right)\frac{\beta_2}{\beta_3} = 1$$

donde $\beta_1/\beta_2, \beta_1/\beta_3 \in \mathcal{O}_K^\times$ y los coeficientes que acompañan a estos bichos están en $K^\times$ (ojo que usamos que los ceros son distintos para poder dividir).

Por el teorema 6.3, existen finitas elecciones para el cocientes β_1/β_2. Usando las relaciones $(x - \alpha_i) = \mu_i \beta_i$ vemos que entonces hay finitas elecciones para el cocientes $(x - \alpha_1 y)/(x - \alpha_2 y)$. Esto implica finitas elecciones para el cociente x/y y entonces hay finitas soluciones para $F(x,y) = m$ como buscábamos. □

Proposición 7.2: Sea $f(x) \in \mathbb{Z}[x]$ libre de cuadrados y con al menos tres ceros distintos en $\mathbb{C}$. Luego la ecuación $y^2 = f(x)$ tiene finitas soluciones enteras.

Referencias

1. Baker, A. *Transcendental number theory* (Cambridge University Press, 1975).
2. Bilu, Y. F., Bugeaud, Y. y Mignotte, M. *The Problem of Catalan* (Springer International Publishing Switzerland, 2014).
3. Brindza, B. On S-integral solutions of the Catalan equation. *Acta Arithmetica* **48,** 397-412. doi:10.4064/aa-48-4-397-412 (1987).
4. Evertse, J.-H. y Győry, K. *Unit Equations in Diophantine Number Theory Cambridge Studies in Advanced Mathematics* **146** (Cambridge University Press, 2016).
5. Neukirch, J. *Algebraic Number Theory* trad. por Schappacher, N. (Springer-Verlag Berlin Heidelberg, 1992).
6. Stewart, C. L. y Tijdeman, R. On the Oesterlé-Masser conjecture. *Monatsh. Math.* **102,** 251-257. doi:10.1007/BF01294603 (1986).
7. Stewart, C. y Yu, K. On the *abc* conjecture I, II. *Math. Ann.* **291,** 225-230. doi:10.1007/BF01445201 (1991).

Correo electrónico: francisco.gallardo@uc.cl

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