Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Serge Lang

# La conjecture de Catalan

*Séminaire Delange-Pisot-Poitou. Théorie des nombres*, tome 17, n° 2 (1975-1976), exp. n° 29, p. 1-9

<http://www.numdam.org/item?id=SDPP_1975-1976__17_2_A5_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
17e année, 1975/76, n° 29, 9 p.



24 mai 1976

# LA CONJECTURE DE CATALAN

par Serge LANG
(d'après R. TIJDEMAN [4])

Une conjecture classique de Catalan dit que l'équation

$$x^p - y^q = 1$$

n'a qu'un nombre fini de solutions en entiers $x$ , $p$ , $y$ , $q$ . La difficulté est de borner $p$ , $q$ . Pour $p$ , $q$ fixe, l'équation est superelliptique et peut être traitée par les méthodes de SIEGEL-CHABAUTY-KUBERT-LANG, par réduction au cas elliptique. TIJDEMAN a récemment renforcé une égalité de BAKER [1], [4], qui lui a permis de montrer que l'équation de Catalan n'a qu'un nombre fini de solution, de façon effective. Nous énoncerons l'inégalité, montrerons comment elle s'applique au problème de Catalan, puis donnerons un résumé de la démonstration de l'inégalité diophantienne portant sur des combinaisons linéaires de logarithmes de nombres algébriques, à coefficients entiers.

## 1. Énoncé de l'inégalité

Soient $\alpha_j$ $(j = 1 , \dots , n)$ des nombres algébriques dans un corps de nombre $K$ , soit $u_j = \log \alpha_j$ (détermination principale). On pose

$$U_j = \log H_K(\alpha_j) , \qquad U_j \leqslant U_{j+1} ,$$

où la hauteur $H_K(\alpha)$ est définie par le produit

$$\prod_v \max(1 , |\alpha|_v)^{n_v}$$

étendu sur les valeurs absolues de $K$ , normalisées pour induire la valeur absolue ordinaire sur $\underset{\sim}{Q}$ , ou les valeurs $p$-adiques telles que $|p|_{v_p} = 1/p$ . Les exposants $n_v$ sont les multiplicités locales, donnant lieu à la formule du produit.

INÉGALITÉ de Baker-Tijdeman. - Soient $\beta_1 , \dots , \beta_n$ des nombres rationnels tels que

$$\beta_1 u_1 + \dots + \beta_n u_n \neq 0 .$$

Posons $B = \max H_k(\beta_j)$ , et

$$\tau(B , u) = (\log B) U_n U_{n-1}^{\theta} ,$$

où $\theta$ est un nombre positif convenable, dépendant de $r$ , par exemple

$$\theta = (2n + 3)(n + 3) + 1$$

suffira. Alors on a une inégalité

$$|\beta_1 u_1 + \dots + \beta_n u_n| \geqslant C_0^{-\tau(B,u)} ,$$

où $C_0$ est une constante suffisamment grande, dépendant seulement de $n$ et du degré $[K : \mathbb{Q}]$.

BAKER avait obtenu une telle inégalité, mais laissant indéterminée la dépendance de $\tau(B , u)$ par rapport à $U_{n-1}$. On notera aussi que l'apparence de $U_n$ avec exposant 1, est essentielle pour les applications qu'on a en vue.

L'inégalité de Baker-Tijdeman sera ramenée à une autre inégalité.

INÉGALITÉ de Baker-Fel'dman. - Soient $\beta_1, \dots , \beta_n$ des nombres rationnels tels que

$$\beta_1 u_1 + \dots + \beta_n u_n \neq 0 .$$

Alors on a

$$|\beta_1 u_1 + \dots + \beta_n u_n| \geqslant C_0^{-(\log B)^{\varkappa}} ,$$

où $C_0$ est une constante suffisamment grande, et $\varkappa$ est un nombre positif convenable (par exemple $\theta - 1$).

Dans cette inégalité, on pose $U = \max U_j$. On voit que les deux inégalités diffèrent dans l'exposant de $U_n$, qui est plus précis dans la première inégalité que dans la seconde. Le passage de l'une à l'autre constitue une sorte de récurrence sur les hauteurs, et permet de traiter les cas où $B$ est grand ou petit par rapport à $U$.

## 2. Application à Catalan

On peut supposer que $p$, $q$ sont des nombres premiers impairs (le cas où l'un d'eux est 2 peut être traité séparément). On doit montrer que $p$, $q$ sont bornés.

Nous analysons d'abord une propriété de divisibilité. On peut écrire

$$x^p = y^q + 1 = (y + 1)(y^{q-1} - y^{q-2} + \dots - 1) .$$

Les deux facteurs à droite ont un p. g. c. d. égal à 1 ou $q$. En effet, si $\ell$ est premier divisant tous les deux, donc

$$y \equiv -1 \pmod{\ell} ,$$

on a

$$y^{q-1} - y^{q-2} + \dots + - 1 \equiv -q \pmod{\ell} ,$$

et par conséquent $\ell = q$. Il en découle aussi que seule la première puissance de $q$ peut diviser les deux facteurs. Un argument semblable, appliqué à $y^q = x^p - 1$, montre donc : il existe $\delta$, $\delta' = 0 , 1 , -1$ tels que

$$x = p^{\delta} X^{q} + 1 , \quad \text{et} \quad y = q^{\delta'} Y^{p} - 1 ,$$

avec des entiers $X$ , $Y$ convenables.

On a une symétrie évidente entre les termes en $x$ et $y$ . Supposons pour fixer les idées que

$$q \leqslant p \quad \text{et} \quad 0 < y < x .$$

Les autres cas peuvent être traités de la même manière.

Premier pas. - On montre $q \ll (\log p)^{c}$ avec une constante $c$ .

Démonstration. - Remarquons d'abord que

$$(p^{\delta} X^{q})^{p} \quad \text{et} \quad (q^{\delta'} Y^{p})^{q}$$

ont le même ordre de grandeur. On a également

$$\begin{aligned} \log(x-1)^{p} - \log(y+1)^{q} &\leqslant |\log(x-1)^{p} - \log x^{p}| + |\log x^{p} - \log y^{q}| + |\log y^{q} - \log(y+1)^{q}| \\ &\ll \frac{p^{2}}{x^{q}} = \exp(-q \log X + 2 \log p) . \end{aligned}$$

Employons la factorisation de $x - 1$ et $y + 1$ à nouveau. On trouve

$$|p \log(p^{\delta} X^{q}) - q \log(q^{\delta'} Y^{p})| \ll p^{2}/X^{q} ,$$

d'où

$$|p\delta \log p - q\delta' \log q + pq \log(X/Y)| \ll p^{2}/X^{q} .$$

L'inégalité de Baker-Tijdeman donne alors

$$C_{0}^{-[(\log p)(\log q)^{\theta} \log X]} \leqslant C_{1} \exp(-q \log X + 2 \log p) .$$

On ramène à gauche le terme exponentiel $2 \log p$ , puis on se sert du fait que $\log X$ intervient à la première puissance pour l'éliminer des deux côtés. Puisque $q \leqslant p$ , on obtient

$$q \ll (\log p)^{c}$$

avec une constante $c$ convenable.

C. Q. F. D.

Deuxième pas. - On a $p \ll (\log p)^{c}$ avec une constante $c$ .

Démonstration. - Cette fois-ci, on commence directement avec l'inégalité

$$|p \log x - q \log y| \ll 1/x^{p} ,$$

d'où, par les mêmes arguments qu'avant, on trouve

$$|p \log x - q \log(q^{\delta'} Y^{p})| \ll p^{2}/Y^{p} ,$$

et donc

$$|p \log(x/Y^q) - q\delta' \log q| \ll p^2/Y^p = \exp(-p \log Y + 2 \log p) .$$

L'inégalité de Baker-Tijdeman montre alors que

$$C_0^{-(\log p)^\theta \log Y^q} \leq C_1 \exp(-p \log Y + 2 \log p) .$$

Le premier pas nous donne déjà une borne de $q$ en fonction de $\log p$ . Cette fois-ci, on élimine $\log Y$ des deux côtés, et on arrive à

$$p \ll q(\log p)^\theta ,$$

ce qui démontre que $p$ est borné, comme il fallait le faire.

On observera que l'inégalité de Baker-Tijdeman n'est appliquée qu'à des combinaisons linéaires de deux et trois logarithmes de nombres rationnels.

## 3. Réduction au cas d'indépendance linéaire

Tout d'abord, il convient de se ramener au cas où les $u_j$ sont linéairement indépendants sur les rationnels. On fait ça au moyen du lemme suivant, dont la démonstration emploie une technique de STARK [3] .

THÉORÈME 3.1. - *Soit* $K$ *un corps de nombres. Soient* $\alpha_1 , \ldots , \alpha_r$ *des éléments* $\neq 0$ *de* $K$ , *multiplicativement indépendants. Soit* $\alpha \neq 0$ *dans* $K$ , *et* $N$ *la période de* $\alpha$ *par rapport au groupe engendré par* $\alpha_1 , \ldots , \alpha_r$ *et par* $K^*_{\mathrm{tor}}$ (= *racines de l'unité dans* $K$ ). *Alors* $N$ *satisfait à la borne*

$$\Phi(N) \ll (h_1 + \ldots + h_r)^r ,$$

*où la constante implicite dans* $\ll$ *ne dépend que de* $[K : \underset{\sim}{Q}]$ .

*Démonstration.* - On écrit

$$\alpha_1^{m_1} \ldots \alpha_r^{m_r} \zeta = \alpha^N ,$$

où $\zeta$ est une racine de l'unité. On peut supposer

$$(m_1 , \ldots , m_r , N) = 1 .$$

Par le principe des tiroirs de Dirichlet appliqué à

$$(qm_1/N , \ldots , qm_r/N) \pmod{\underset{\sim}{Z}^r}$$

on peut trouver un entier $q > C$ premier à $N$ avec $C < q < N$ tel que

$$|qm_j/N - s_j| \ll \Phi(N)^{-1/r} ,$$

avec des entiers $s_j$ convenables. Posons $n_j = qm_j - Ns_j$ , de sorte que

$$|n_j| \ll N\Phi(N)^{-1/r} .$$

On obtient

$$\alpha_1^{n_1} \dots \alpha_r^{n_r} \zeta_0 = \beta^N \quad \text{avec} \quad \beta \in K^* .$$

Donc

$$H_K(\beta)^N = H_K(\beta^N) \leq (H_1 \dots H_r)^n , \qquad \text{où} \quad n = \max |n_j| .$$

Comme les hauteurs d'éléments de $K$ qui ne sont pas des racines de l'unité admettent une borne inférieure effective, ceci termine la démonstration.

COROLLAIRE. - Soient $\alpha_1 , \dots , \alpha_{r+1}$ des éléments $\neq 0$ de $K$. Supposons qu'ils ont rang multiplicatif $r$. Alors il existe une relation multiplicative

$$\alpha_1^{m_1} \dots \alpha_{r+1}^{m_{r+1}} = 1$$

avec des entiers $m_j$ pas tous égaux à $0$, et tels que $M = \max |m_j|$ satisfait à

$$\Phi(M) \ll (h_1 + \dots h_r)^r .$$

Démonstration. - Elle est évidente.

Supposons qu'on veuille démontrer une inégalité comme dans le théorème. On suppose qu'elle soit fausse, donc qu'on ait

$$|\beta_1 u_1 + \dots + \beta_n u_n| \leq C_0^{-\tau(B,U)} .$$

Supposons que $u_1 , \dots , u_r$ soient un sous-ensemble maximal d'éléments linéairement indépendants parmi $u_1 , \dots , u_{n-1}$. Si $u_n$ dépend de $u_1 , \dots , u_{n-1}$, on écrit une relation linéaire, et on trouve tout de suite une combinaison linéaire d'éléments linéairement indépendants, satisfaisant à l'inégalité

$$|\beta'_1 u_1 + \dots + \beta'_r u_r| \leq C_0^{-\tau(B,U)} ,$$

où $B' = \max H_K(\beta'_j)$ satisfait à

$$B' \ll B . U^r \log \log U .$$

(Le log log provient d'une estimation triviale de la fonction d'Euler.) Ceci contredit alors l'inégalité de Baker-Fel'dman. Un raisonnement semblable ramène l'inégalité de Baker-Fel'dman au cas linéairement indépendant.

Cette réduction, très simple, permet de simplifier, considérablement, certaines démonstrations, par exemple celle donnée par BAKER dans son livre [1] pour le théorème de Baker-Fel'dman, chapitre 3. Les lemmes 3, 7 et la récurrence deviennent inutiles (cf. la remarque à la fin de la page 35). Même sans la borne explicite donnée par le corollaire ci-dessus, la réduction pouvait s'appliquer puisque BAKER ne précise pas la dépendance de la constante par rapport aux hauteurs des $\alpha_j$.

## 4. Démonstration de l'inégalité diophantienne

Nous supposerons connue l'inégalité de Baker-Fel'dman, et nous indiquerons brièvement comment on passe de celle-ci à l'autre. La difficulté tient à l'exposant 1 pour $U_n$.

On suppose donc qu'on a des nombres rationnels $\beta_j$ tels que

$$|\beta u_1 + \dots + \beta_r u_r - u_{r+1}| \leqslant C_0^{-r}(B,u) \quad , \tag{1}$$

avec $C_0$ suffisamment grande, et on veut trouver une contradiction.

On peut supposer que $U_{r+1}$ est grand par rapport à $U_r$, de façon précise

$$U_{r+1} \geqslant 4rU_r \quad ,$$

sans cela on est dans le cas Baker-Fel'dman.

On peut aussi supposer $B \geqslant C_1 U_r^{\theta}$, car dans le cas contraire, une inégalité triviale du type Liouville donne la contradiction.

On pose avec FEL'DMAN, pour $k$ entier,,

$$\Delta(x , k) = \frac{(x + 1)(x + 2) \dots (x + k)}{k!} \quad .$$

Ces polynômes ont l'avantage qu'on peut donner facilement des estimations de leur valeur absolue, et de leurs dénominateurs quand $x$ est rationnel. Ceci a été fait par FEL'DMAN, et BAKER a ensuite donné des bornes précises pour leurs dérivées, légèrement améliorées par TIJDEMAN. Par exemple, si $x$ est un nombre rationnel positif, on trouve

$$\frac{1}{m!} D^m(\Delta(x , k)^{\ell}) \leqslant 4^{(x+k)\ell}$$
$$\text{dén} \frac{1}{m!} D^m \Delta(a/d , k)^{\ell} \leqslant d^{2k\ell} e^{4km/3} \quad ,$$

où $D$ est la dérivée $d/dx$, et $x = a/d$ est exprimé comme quotient de nombres entiers premiers entre eux.

Pour tout vecteur

$$(\lambda) = (\lambda_{-1} , \lambda_0 , \dots , \lambda_{r+1}) \quad \text{et} \quad (m) = (m_0 , \dots , m_{r+1})$$

d'entiers $\geqslant 0$, on pose

$$x_j(\lambda) = \lambda_j + \beta_j \lambda_{r+1}$$

et

$$\Psi_{\lambda,m}(x) = \Psi(x , \lambda , m , r) = \frac{1}{m_C!} D_0^{m_C} \Delta^{\lambda_0}(x + \lambda_{-1} , N) \prod_{j=1}^{r} \Delta(x_j(\lambda) , m_j) \quad ,$$

où $N = [\log B]$. C'est un polynôme en $x$, de nature spéciale, adaptée à nos besoins.

LEMME PRINCIPAL. - Si $M_*$ est suffisamment grand, il existe un nombre $C_0$ ayant

la propriété suivante. Si l'on a une inégalité

$$|\beta_1 u_1 + \dots + \beta_r u_r - u_{r+1}| \leqslant C_0^{-T}(B,u) ,$$

alors il existe des coefficients entiers $a_{(\lambda)}$ pas tous nuls, tels que

$$(*) \qquad \sum_{(\lambda)} a_{(\lambda)} \Psi(\frac{n}{q} , m.\lambda , r)\, \alpha_1^{n\lambda_1/q} \dots \alpha_{r+1}^{n\lambda_{r+1}/q} = 0 ,$$

pour un nombre premier $q$ tel que $L_{r+1} < q < 2L_{r+1}$ , et pour $(m)$ , $n$ entier positif satisfaisant

$$0 \leqslant m_j \leqslant L , \qquad n \leqslant M_* N .$$

La somme sur $(\lambda)$ est prise pour $0 \leqslant \lambda_j \leqslant L_j$ . Les valeurs $L_j$ sont déterminées en fonction des $U_j$ , et de façon précise,

$$L_{r+1} = M_*^{\sigma} U_r^{\rho} ,$$

$$L = L_0 = \dots = L_r = M_*^{\sigma'} U_r^{\rho'} U_{r+1} ,$$

$$L_{-1} = N ,$$

avec des nombres réels positifs $\sigma$ , $\sigma'$ , $\rho$ , $\rho'$ qu'on détermine au fur et à mesure de la démonstration pour que ça marche. Une infinité de choix est possible, et la valeur précise de ces paramètres est sans conséquence, mais pour le lecteur avide de précision, disons que les valeurs doivent satisfaire à des inégalités

$$(r+1)\sigma + \sigma' \geqslant r+1 , \qquad \sigma , \sigma' < 1 ,$$

$$(r+1)\rho + \rho' \geqslant t(r+1) , \qquad \rho + 1 < t \text{ et } \rho' < t ,$$

avec $t$ positif. On fait alors le choix

$$\sigma = 1 - \frac{1}{4(r+1)} , \qquad \sigma' = \frac{1}{2}$$

$$t = 2r + 3 , \quad \rho = t - 2 , \qquad \rho' = t - 1 .$$

Ces valeurs précises n'interviendront pas dans la partie de la démonstration que nous allons résumer.

Les équations (*) sont des relations polynomiales pour $\alpha_{r+1}^{n/q}$ par rapport au corps

$$K_r = K(\alpha_1^{n/q} , \dots , \alpha_r^{n/q}) .$$

Du fait qu'on a beaucoup de telles équations, c'est-à-dire que les polynômes

$$\Delta(x , 0) , \Delta(x , 1) , \dots , \Delta(x , L)$$

sont linéairement indépendants, on obtient par récurrence que, pour chaque valeur $\lambda_1 , \dots , \lambda_{r+1}$ , le polynôme

$$\sum_{\lambda_{-1},\lambda_0} a_{(\lambda)} \Delta(x + \lambda_{-1} ; N)^{\lambda_0}$$

s'annule en toutes les fractions $n/q$ avec multiplicité $\geqslant L$ .

On voit alors que ce polynôme a un nombre de zéros plus grand que son degré, donc qu'il est identiquement nul, donc que les $a_{(\lambda)}$ sont tous nuls, contradiction.

Il s'ensuit que $\alpha_{r+1}^{n/q}$ est de degré $< q$ sur $K_r$.

On procède maintenant à une récurrence qui ramène le théorème au cas où la hauteur de $\alpha_{r+1}$ est du même ordre de grandeur que les autres hauteurs des $\alpha_j$. Par la théorie de Kummer, il existe une relation multiplicative

$$\alpha_{r+1}\, \alpha_1^{\nu_1} \cdots \alpha_r^{\nu_r} = \alpha_{r+1}^{(1)q}, \qquad 0 \leqslant \nu_j < q$$

avec un élément $\alpha_{r+1}^{(1)} \neq 0$ dans $K$. On écrit ceci additivement,

$$u_{r+1} + \nu_1 u_1 + \cdots + \nu_r u_r = q u_{r+1}^{(1)} + \nu \cdot 2\pi i ,$$

avec $|\nu| \ll q$. On peut supposer, sans perte de généralité, que $u_1 = 2\pi i$. Par la sous-multiplicativité de la hauteur, on trouve

$$H_K(\alpha_{r+1}^{(1)}) \leqslant H_K(\alpha_{r+1})^{1/q}\, H_1 \cdots H_r .$$

Posons $U_{r+1}^{(1)} = \log H_K(\alpha_{r+1}^{(1)})$ comme il se doit. On trouve

$$U_{r+1}^{(1)} \leqslant \frac{1}{q}\, U_{r+1} + rU_r .$$

On substitue l'expression linéaire pour $u_{r+1}$ dans l'inégalité fondamentale du lemme principale. On trouve alors

$$|\beta_1 u_1 + \cdots + \beta_r u_r - u_{r+1}| = |\beta_1^{(1)} u_1 + \cdots + \beta_r^{(1)} u_r - q u_{r+1}^{(1)}| \leqslant C_0^{-\tau}(B,u) ,$$

où les $\beta_j^{(1)}$ sont de nouveaux coefficients, satisfaisant

$$\text{Hauteur des } \beta_j^{(1)} \leqslant B^{(1)} \qquad \text{et} \quad B^{(1)} = BC_* U_r^{\rho} .$$

La constante $C_*$ ne dépend que de $M_*$ et de $r$.

Cette nouvelle combinaison linéaire où $u_{r+1}$ est remplacé par $u_{r+1}^{(1)}$ a pour effet de remplacer $B$ par $B^{(1)}$ (le début d'une progression géométrique), mais de faire décroître $U_{r+1}$ à $U_{r+1}^{(1)}$.

Sous l'hypothèse

$$B \geqslant C_1 U_r^{\theta} \quad \text{et} \quad U_{r+1} \geqslant 4rU_r ,$$

on a

$$\tau(B^{(1)}, u^{(1)}) \leqslant \tau(B, u) ,$$

et par conséquent

$$|\beta_1^{(1)} u_1 + \cdots + \beta_r^{(1)} u_r - q u_{r+1}^{(1)}| \leqslant C_0^{-\tau}(B^{(1)}, u^{(1)}) .$$

La démonstration est immédiate. Ceci implique que nous pouvons procéder à une récurrence $s$ fois, avec $s \leq 2 \log U_{r+1}$, pour obtenir une inégalité

$$|\beta_1^{(s)} u_1 + \ldots + \beta_r^{(s)} u_r - \beta_{r+1}^{(s)} u_{r+1}^{(s)}| \leq C_0^{-\tau}(B^{(s)}, u^{(s)}) ,$$

avec des coefficients $\beta_j^{(s)}$ tels que Hauteur $\beta_j^{(s)} \leq B^{(s)}$. On peut continuer la récurrence jusqu'à ce que

$$U_{r+1}^{(s)} \leq 4rU_r ,$$

ce qui ramène le théorème de Baker-Tijdeman au théorème de Baker-Fel'dman, comme on se l'était proposé.

Quant au lemme principal, il se démontre de la façon habituelle, encore qu'un peu plus compliquée, avec des fonctions entières auxiliaires et le procédé d'extrapolation qui leur donne beaucoup de zéros. Nous n'entrons pas dans cet aspect de la démonstration ici.

BIBLIOGRAPHIE

[1] BAKER (A.). - A sharpening of the bounds for linear forms in logarithms, Acta Arithm., Warszawa, t. 21, 1972, p. 117-129.

[2] FEL'DMAN (N. I.). - Improved estimate for a linear form of the logarithms of algebraic numbers, Math. USSR-Sbornik, t. 6, 1968, p. 393-406 ; et [en russe] Mat. Sbornik, t. 77, 1968, p. 423-436.

[3] STARK (H.). - Further advances in the theory of linear forms in logarithms, "Diophantine approximation and its applications", p. 255-293. - London, Academic Press, 1973.

[4] TIJDEMAN (R.). - On the equation of Catalan, Acta Arithm., Warszawa, t. 24, 1976, p. 197-209.

(Texte reçu le 13 septembre 1976)

Serge LANG
Yale University
Box 2155 Yale Station
NEW HAVEN, Conn. 06520
(Etats-Unis)