Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Germaine Revuz

Équations diophantiennes exponentielles

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 13, nº 1 (1971-1972), exp. nº 3, p. 1-16
<http://www.numdam.org/item?id=SDPP_1971-1972__13_1_A2_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
13e année, 1971/72, n° 3, 16 p.

15 novembre 1971

ÉQUATIONS DIOPHANTIENNES EXPONENTIELLES

par Germaine REVUZ

Introduction. - A l'origine de ce travail se trouve le problème de Strauss : Etant donnés deux entiers naturels a et b tels que $(\log a)/(\log b)$ soit irrationnel et deux entiers naturels M et N, existe-t-il une infinité d'entiers naturels qui s'écrivent en base a avec une somme de chiffres inférieure à M, et en base b avec une somme de chiffres inférieure à N ?

S'il existe une infinité de tels entiers naturels, il y en a une infinité qui s'écrivent avec les mêmes chiffres ; il en résulte l'existence d'un infinité de solutions à l'équation

$$\sum_{i=1}^{m} \lambda_i\, a^{y_i} = \sum_{j=1}^{n} \mu_j\, b^{x_j} ,$$

où λ_i $(0 \leqslant \lambda_i \leqslant a - 1)$ et μ_j $(0 \leqslant \mu_j \leqslant b - 1)$ sont des entiers naturels donnés, et où y_i et x_j sont des entiers naturels inconnus.

Se plaçant dans un cadre en peu plus large, nous avons cherché à étudier la finitude du nombre de solutions d'une équation de ce type, où les y_i et les x_j seraient dans $\mathbb{Z}$, et où les λ_i et les μ_j seraient des nombres algébriques que l'on peut évidemment supposer entiers.

Si, pour a et b, on prend a priori des complexes quelconques, on remarque d'abord que l'existence de deux solutions pour l'équation suffit à établir l'algébricité de a et de b. Ecrivons, en effet, l'existence de ces solutions sous la forme $P(a , b) = 0$, $P'(a , b) = 0$, $P(X , Y)$ et $P'(X , Y)$ étant deux polynômes à deux indéterminées à coefficients algébriques. Le résultant de P et P', considérés comme polynômes en X (resp. en Y), est une équation vérifiée par b (resp. par a). Le problème ne se pose donc que pour a et b algébriques. En fait, nous nous sommes limités au cas où a et b sont des entiers algébriques qui ne sont pas des unités.

Remarquons ensuite que, si les équations $\sum_{i=1}^{m} \lambda_i\, a^{y_i} = 0$ et $\sum_{j=1}^{n} \mu_j\, b^{x_j} = 0$ ont chacune une solution $(Y_i) \in \mathbb{Z}^m$ et $(X_j) \in \mathbb{Z}^n$, elles en ont une infinité $(Y_i + k)$ et $(X_j + \ell)$, k et ℓ décrivant $\mathbb{Z}$ et que $(Y_i + k , X_j + \ell)$ constitue une solution de notre équation qui a donc, trivialement, une infinité de solutions. Nous conviendrons de ne nous intéresser qu'aux solutions qui donnent aux deux membres de l'équation une valeur non nulle.

Remarquons enfin, que dans le cas où il existe deux entiers naturels x_0, y_0, tels que $a^{y_0} = b^{x_0}$, l'existence d'une solution (Y_i , X_j) suffit à entraîner l'existence de l'infinité de solutions $(Y_i + Ky_0 , X_j + Kx_0)$, K décrivant $\mathbb{Z}$.

Pour que le nombre de solutions de l'équation envisagée soit fini, il est donc nécessaire que a et b vérifient la condition :

(c) a et b sont multiplicativement indépendants sur $\underset{\sim}{Z}$.

En résumé, nous étudions les solutions $(y_i, x_j) \in \underset{\sim}{Z}^{m+n}$, n'annulant pas les deux membres d'une équation

$$\text{(E)} \qquad \sum_{i=1}^{m} \lambda_i a^{y_i} = \sum_{j=1}^{n} \mu_j b^{x_j},$$

où a et b sont des entiers algébriques, qui ne sont pas des unités, et satisfont à la condition (c), et où (λ_i) et (μ_j) sont des entiers algébriques donnés.

Nous appellerons K la plus petite extension de $\underset{\sim}{Q}$ contenant les λ_i et les μ_j.

Sous ces hypothèses, nous démontrerons la finitude du nombre de solutions de (E)

1° quand a et b vérifient certaines conditions, et indépendamment du nombre de termes (i. e. du couple $m.n$) ;

2° pour a et b quelconques (quoique satisfaisant à des conditions un peu plus fortes que (c)), mais seulement pour $(m \leq 2,\ n \leq 2)$ et $(m \leq 3,\ n = 1)$ [1]

1. Généralités.

Nous allons supposer maintenant que (E) a une infinité de solutions, pour essayer d'arriver, à partir de cette hypothèse, à une contradiction.

Si E a une infinité de solutions et si, pour chacune d'elles, on range les y_i dans l'ordre naturel et les x_j dans l'ordre naturel, on obtient une permutation des indices i associée à une permutation des indices j, et, pour une infinité de solutions, ce couple de permutations est le même. En modifiant au besoin la numérotation, on a donc une infinité de solutions qui satisfont à

$$y_1 \geq y_2 \geq \cdots \geq y_m, \qquad x_1 \geq x_2 \geq \cdots \geq x_n.$$

D'autre part, considérons les différences $y_i - y_{i+1}$ et $x_j - x_{j+1}$. Elles ne peuvent être toutes bornées car, si elles l'étaient, pour une infinité de solutions, chacune conserverait une même valeur α_i ou β_j, et ces solutions vérifieraient une équation

$$(1) \qquad \lambda' a^{y_m} = \mu' b^{x_n},$$

avec

$$\lambda' = \lambda_1 a^{\alpha_1+\cdots+\alpha_{m-1}} + \lambda_2 a^{\alpha_2+\cdots+\alpha_{m-1}} + \cdots + \lambda_{m-1} a^{\alpha_{m-1}} + \lambda_m$$
$$\mu' = \mu_1 b^{\beta_1+\cdots+\beta_{n-1}} + \mu_2 b^{\beta_2+\cdots+\beta_{n-1}} + \cdots + \mu_{n-1} b^{\beta_{n-1}} + \mu_n$$

---

(1) Nous n'avons fait en général aucune hypothèse particulière sur les coefficients λ_i et μ_j. Il est clair qu'on obtiendrait des résultats immédiats mais très fragmentaires avec des hypothèses particulières.

Or, si l'équation (1) avait au moins deux solutions distincte (Y , X) et (Y_1 , X_1), on aurait $a^{Y-Y_1} = b^{X-X_1}$, ce qui contredirait (c). Supposons donc que les différences $y_i - y_{i+1}$ soient bornées, pour $i = 1 , 2 , \dots , i_0 - 1$, et que $y_{i_0} - y_{i_0+1}$ ne le soit pas.

En raisonnant comme ci-dessus, et en groupant les termes de la même façon, on voit qu'une infinité de solutions de (E) vérifieraient une équation

$$\lambda'_{i_0} a^{y_{i_0}} + \lambda_{i_0+1} a^{y_{i_I+1}} + \sum_{i_0+2}^{m} \lambda_i a^{y_i} = \sum_{j=1}^{n} \mu_j b^{x_j} ,$$

et, de cette infinité de solutions, on pourrait extraire une suite S_{k_1} de solutions telle que $\lim_{k_1 \to \infty} y_{i_0} - y_{i_0+1} = + \infty$. Pour les solutions de cette suite, considérons à nouveau les différences $y_i - y_{i+1}$ pour $i \geq i_0 + 1$; si les premières d'entre elles restent bornées, on procède comme ci-dessus, et on extrait de S_{k_1} une suite S_{k_2} de solutions vérifiant une nouvelle équation de même type et telle que les deux premières différences tendent vers l'infini avec k_2. On répétera le processus autant de fois qu'il sera nécessaire, dans le premier membre de E, puis dans le second, et on arrivera finalement à obtenir une équation

$$\text{(E')} \qquad \sum_{i'=1}^{m'} \lambda'_i a^{y_{i'}} = \sum_{j'=1}^{n'} \mu'_{j'} b^{x_{j'}} ,$$

avec $m' \leqslant m$, $n' \leqslant n$, possédant une suite de solutions telles que toutes les différences $y_{i'} - y_{i'+1}$, $x_{j'} - x_{j'+1}$ tendent vers l'infini. Les coefficients λ'_i et μ'_i sont des entiers du corps $K(a , b)$. Ces coefficients ne sont pas tous nuls car, s'ils l'étaient, c'est que les solutions considérées de (E) en annuleraient les deux membres, contrairement à ce qui a été supposé au début.

Pour simplifier l'écriture, nous supprimerons les ' dans l'écriture de l'équation (E') ainsi associée à l'équation initiale (E). Autrement dit, <u>nous supposerons dorénavant que l'équation</u>

$$\text{(E)} \qquad \sum_{i=1}^{m} \lambda_i a^{y_i} = \sum_{j=1}^{n} \mu_j b^{x_j} ,$$

<u>a une suite</u> S_k <u>de solutions, satisfaisant à</u>

$$\text{(K)} \qquad \forall i , \ \forall j , \qquad \lim_{k\to\infty} y_i - y_{i+1} = + \infty , \qquad \lim_{k\to\infty} x_j - x_{j+1} = + \infty .$$

Pour les solutions de cette suite, y_1 et y_m ne peuvent être bornés tous deux ; il en est de même pour x_1 et x_n.

Examinons d'abord le point de savoir si x_n et y_m sont minorés. Supposons que x_n ne le soit pas. S'il existait un idéal premier $\mathfrak{p}$ de $K(a , b)$, tel que $v_{\mathfrak{p}}(a) = 0$, $v_{\mathfrak{p}}(b) > 0$, la valuation $\mathfrak{p}$-adique du premier membre de (E) serait positive ou nulle, tandis que celle du deuxième membre ne serait pas minorée. On en conclut que tout idéal $\mathfrak{p}_\alpha$ qui divise b, devrait diviser a ; alors, pour $y_{m-1} - y_m$ et $x_{n-1} - x_n$ suffisamment grand, et pour tout idéal commun $\mathfrak{p}_\alpha$, on devrait avoir

(2) $$v_{\mathfrak{p}_\alpha}(\lambda_m) + y_m\, v_{\mathfrak{p}_\alpha}(a) = v_{\mathfrak{p}_\alpha}(\mu_n) + x_n\, v_{\mathfrak{p}_\alpha}(b) \ .$$

Il en résulterait d'abord que y_m ne serait pas minoré non plus et que, pour tout $\mathfrak{p}_\alpha$, les solutions appartenant à S_k, vérifieraient

$$\lim_{k\to\infty} y_m/x_n = v_{\mathfrak{p}_\alpha}(b)/v_{\mathfrak{p}_\alpha}(a) \ .$$

$v_{\mathfrak{p}_\alpha}(b)/v_{\mathfrak{p}_\alpha}(a)$ serait donc un nombre indépendant de $\mathfrak{p}_\alpha$; mais, puisque y_m ne serait pas minoré, tout idéal premier divisant a devrait diviser b. On aurait donc, en désignant par $r(a)$ le radical de l'idéal (a),

$$r(a) = r(b) = \prod_\alpha \mathfrak{p}_\alpha \ ,$$

et, pour tout α, $v_{\mathfrak{p}_\alpha}(b)/v_{\mathfrak{p}_\alpha}(a)$ serait le même rationnel p/q. Mais alors, le quotient de b^q par a^p serait une unité algébrique. Ceci nous amène à poser la définition suivante :

On dit que a et b satisfont à la condition (c) forte s'ils sont multiplicativement indépendants, modulo le groupe des unités de $K(a\ ,\ b)$.

Et nous pouvons énoncer le lemme suivant.

LEMME 1. - Si x_n est minoré, y_m l'est aussi. Il suffit, pour qu'ils le soient que a et b satisfassent à la condition (c) forte.

D'autre part, il nous sera commode par la suite que a et b satisfassent à une deuxième condition qui est, elle aussi, plus forte que (c), mais indépendante de la précédente :

(c') $\log|a|/\log|b|$ est irrationnel [2].

Nous supposerons dorénavant que a et b satisfont à (c) forte et à (c'). Il en résulte immédiatement que x_1 et y_1 ne sont pas majorés.

Ceci entraîne un premier résultat :

PROPOSITION 1. - Si $|a| > 1$ et si $|b| < 1$, l'équation (E) ne peut avoir une infinité de solutions.

En effet, pour les solutions de (E), le deuxième membre de l'équation serait majoré, et le premier ne le serait pas.

Cette proposition se généralise par la suivante :

PROPOSITION 1' - Si a et tous ses conjugués sur K sont de module supérieur à 1 (resp. < 1), et si b a un conjugué sur K, au moins, de module inférieur à 1 (resp. > 1), alors (E) ne peut avoir une infinité de solutions.

Soit a de module supérieur à 1, ainsi que tous ses conjugués ; soit b' un

---

(2) Notons que, dans le cas où a et b sont des entiers naturels, (c') et (c) forte se réduisent à la condition nécessaire (c).

conjugué de b tel que $|b'| < 1$. Plongeons $K(a, b)$ dans une extension L, galoisienne sur K. Il existe un K-automorphisme σ de L tel que $\sigma(b) = b'$. Soit $a' = \sigma(a)$; alors, toute solution (x_j, y_i) de (E) vérifie

$$\sum_{i=1}^{m} \lambda_i a'^{y_i} = \sum_{j=1}^{n} \mu_j b'^{x_j} ,$$

mais cette équation ne peut avoir une infinité de solutions du fait de la proposition 1.

Cette proposition s'applique, par exemple, au cas où $K = \mathbb{Q}$ et où a est un entier naturel, ou une racine d'un entier naturel, et b un nombre de Pisot.

2. Etude de la structure des suites éventuelles de solutions.

Etant donné ce qui précède, nous ne nous occuperons que des cas

$$|a| > 1 , \quad |b| > 1 \quad \text{et} \quad |a| < 1 , \quad |b| < 1 .$$

Dans tous les cas, x_n et y_m étant minorés, les conditions (K) entraînent

$$\lim_{k\to\infty} x_1 = \lim_{k\to\infty} y_1 = +\infty .$$

Notons d'abord le résultat suivant :

LEMME 2. - Dans le cas $|a| > 1$, $|b| > 1$, si (E) a une suite S_k de solutions, celles-ci vérifient

(3) $$\lim_{k\to\infty} x_1/y_1 = (\log |a|)/(\log |b|) .$$

En effet, on peut écrire E sous la forme

(4) $$\lambda_1 a^{y_1}(1 + \varepsilon_a) = \mu_1 b^{x_1}(1 + \varepsilon_b) ,$$

avec $\varepsilon_a = \sum_{i=2}^{m} (\lambda_i/\lambda_1) a^{y_i - y_1}$, $\varepsilon_b = \sum_{j=2}^{n} (\mu_j/\mu_1) b^{x_j - x_1}$ et

$$\lim_{k\to\infty} \varepsilon_a = \lim_{k\to\infty} \varepsilon_b = 0 .$$

En prenant les logarithmes des modules des deux membres de (4), on obtient (3). Il reste à savoir si x_n et y_m sont majorés.

S'ils le sont tous deux, alors, pour une infinité de valeurs de k, ils gardent deux valeurs fixes β et α respectivement, et de S_k, on peut extraire une sous-suite S_h de solutions de la forme $(y_1 \dots y_{m-1}, \alpha, x_1 \dots x_{n-1}, \beta)$ qui satisfont à (K), et vérifient

(5) $$\sum_{i=1}^{m} \lambda_i a^{y_i} = \sum_{j=1}^{n-1} \mu_j b^{x_j} + c ,$$

avec $c = \mu_n b^{\beta} - \lambda_m a^{\alpha}$.

Nous appellerons une telle suite de solutions, une suite de type I.

Si x_n n'est pas majoré, alors, de S_k, on peut extraire une suite $S_{k'}$ telle que $\lim_{k\to\infty} x_n = +\infty$. Si pour les solutions appartenant à $S_{k'}$, y_m est majoré, alors, pour une infinité de valeurs de k', y_m garde une même valeur α, et de

$S_{k'}$, on peut extraire une sous-suite S_h de solutions de la forme

$$(y_1 \dots y_{m-1} , \alpha , x_1 \dots x_{n-1} , x_n) ,$$

qui satisfont à (K) , telles que

$$\lim_{h\to\infty} x_n = +\infty ,$$

et qui vérifient

$$\sum_{i=1}^{m-1} \lambda_i a^{y_i} = \sum_{j=1}^{n} \mu_j b^{x_j} + c \quad \text{avec} \quad c = -\lambda_m a^{\alpha} , \tag{6}$$

(c est ici différent de 0 si on suppose $\lambda_m \neq 0$).

Nous appellerons une telle suite de solutions, <u>une suite de type II</u>, ainsi que celles obtenues par échange des rôles de a et de b .

Enfin, si pour les solutions appartenant à $S_{k'}$, y_m n'est pas majoré, alors, de $S_{k'}$, on peut extraire une sous-suite S_h de solutions qui satisfont à (K) et telles que

$$\lim_{h\to\infty} x_n = \lim_{h\to\infty} y_m = +\infty .$$

Nous appellerons une telle suite de solutions, <u>une suite de type III</u>.

Finalement, pour que l'équation initiale ait une infinité de solutions, il est nécessaire que l'équation qui lui a été associée possède au moins une suite de solutions d'un des trois types décrits ci-dessus.

<u>Remarque</u>. - Notons enfin qu'une suite de type I, avec $c = 0$, est une suite de type III pour l'équation obtenue, en amputant (E) du dernier terme de ses deux membres.

Nous avons alors les deux résultats suivants :

LEMME 3. - <u>Dans le cas</u> $|a| < 1$, $|b| < 1$, (E) <u>ne peut avoir une suite de solutions de type II, ni de type I avec</u> $c \neq 0$. <u>Si elle a une suite</u> S_h <u>de solutions de type III</u> (<u>resp. de type I avec</u> $c = 0$), <u>cette suite vérifie</u>

$$\lim_{h\to\infty} \frac{x_n}{y_m} = \frac{\log |a|}{\log |b|} \tag{7}$$

$$\left(\text{resp. } \lim_{h\to\infty} \frac{x_{n-1}}{y_{m-1}} = \frac{\log |a|}{\log |b|}\right). \tag{7 bis}$$

En effet, tous les termes autres que c , de l'équation (5) ou de l'équation (6), tendraient vers 0 quand h tend vers l'infini. D'autre part, on écrit (E) sous la forme

$$\lambda_m a^{y_m}(1 + \eta_a) = \mu_n b^{x_n}(1 + \eta_b) , \tag{8}$$

avec

$$\eta_a = \sum_{i=1}^{m-1} \frac{\lambda_i}{\lambda_m} a^{y_i - y_m} , \quad \eta_b = \sum_{j=1}^{n-1} \frac{\mu_j}{\mu_n} b^{x_j - x_n} ,$$

et

$$\lim_{k\to\infty} \eta_a = \lim_{k\to\infty} \eta_b = 0 .$$

En prenant les logarithmes des deux membres de (8), on trouve (7) pour une suite de type III (i. e. quand $\lim_{h\to\infty} x_n = \lim_{h\to\infty} y_m = +\infty$), et donc (7 bis) pour une suite de type I avec $c = 0$, en vertu de la remarque faite ci-dessus.

LEMME 4. - Dans le cas où a et b ne sont pas étrangers, (E) ne peut avoir une suite de solutions de type II, ni de type I, avec $c \neq 0$. Si elle a une suite S_h de solutions de type III (resp. de type I avec $c = 0$), pour tout idéal $\mathfrak{p}$ de $K(a , b)$, divisant a et b , cette suite vérifie

$$\lim_{h\to\infty} \frac{x_n}{y_m} = \frac{v_{\mathfrak{p}}(a)}{v_{\mathfrak{p}}(b)} , \tag{9}$$

$$\left(\text{resp. } \lim_{h\to\infty} \frac{x_{n-1}}{y_{m-1}} = \frac{v_{\mathfrak{p}}(a)}{v_{\mathfrak{p}}(b)} \right) . \tag{9 bis}$$

En effet, la valuation $\mathfrak{p}$-adique de tous les termes autres que c , de l'équation (5) ou de l'équation (6), tendrait vers l'infini avec h , ce qui est impossible pour $c \neq 0$.

D'autre part, on a la relation (2) pour $y_{m-1} - y_m$ et $x_{n-1} - x_n$ suffisamment grands. Pour une suite de type III (i. e. quand $\lim_{h\to\infty} x_n = \lim_{h\to\infty} y_m = +\infty$), on en déduit (9), et donc (9 bis), pour une suite de type I avec $c = 0$, en vertu de la remarque faite ci-dessus.

3. Résultats indépendants du nombre de termes de (E).

PROPOSITION 2. - Si a et b , sont de module inférieur à 1 et ne sont pas étrangers, alors (E) ne peut avoir une infinité de solutions.

En effet, des lemmes précédents résultent (7) et (9), ou (7 bis) et (9 bis). Si ces égalités étaient vérifiées simultanément, $\log |a|/\log |b|$ serait un rationnel, ce qui contredirait (c').

Cette proposition se généralise par la suivante.

PROPOSITION 2'. - Si a et b ne sont pas étrangers et si l'un des deux au moins a un conjugué sur K de module inférieur à 1 , alors (E) ne peut avoir une infinité de solutions.

Reprenons raisonnement et notations de la proposition 1'. Soit $b' = \sigma(b)$ tel que $|b'| < 1$, et soit $a' = \sigma(a)$. Toute solution de (E) doit vérifier

$$\sum_{i=1}^{m} \lambda_i \, a'^{y_i} = \sum_{j=1}^{n} \mu_j \, b'^{x_m} .$$

Si $|a'| > 1$, nous savons déjà qu'il est impossible que cette équation ait une infinité de solutions (Proposition 1). Si $|a'| < 1$, c'est aussi impossible, en vertu de la proposition 2 car, si a et b appartiennent à $\mathfrak{p}$, idéal premier de

$K(a, b)$, a' et b' appartiennent à $\mathfrak{p}' = \sigma(\mathfrak{p})$, idéal premier de $K(a', b')$.

PROPOSITION 3 [3]. - Si a et b appartiennent à plusieurs idéaux premiers de $K(a, b)$ et si leurs valuations relatives à ces idéaux ne sont pas proportionnelles, alors (E) ne peut avoir une infinité de solutions.

En effet, en vertu du lemme 4, une suite de solutions de (E) doit vérifier (9) ou (9 bis) pour tout idéal commun $\mathfrak{p}$.

COROLLAIRE. - (E) ne peut avoir une infinité de solutions quand a et b ont le même radical.

En effet, si $r(a) = r(b)$, et si (E) avait une suite de solutions, il existerait deux entiers naturels p et q tels que $a^p = b^q u$, u étant une unité algébrique, ce qui contredirait (c) forte [3].

Compte tenu des lemmes 3 et 4, des propositions 1' et 2 et du corollaire de la proposition 3, on peut faire, comme suit, la liste des cas qui restent à étudier, et, pour chaque cas, des types de suites de solutions, a priori possibles.

1°	$\lvert a\rvert > 1$,	$\lvert b\rvert > 1$	$(a, b) = 1$	suites I, II, III,
2°	$\lvert a\rvert > 1$,	$\lvert b\rvert > 1$	$\begin{cases} r(a) \neq r(b) \\ (a, b) \neq 1 \end{cases}$	suites III (ou I avec $c = 0$),
3°	$\lvert a\rvert < 1$,	$\lvert b\rvert < 1$	$(a, b) = 1$	suites III (ou I avec $c = 0$).

4. Equations particulières.

Etablissons d'abord le résultat suivant.

LEMME 5. - a et c étant deux nombres algébriques, $\mathfrak{p}$ un idéal premier d'un corps de nombre qui les contient et tel que $v_{\mathfrak{p}}(a) = 0$, si la congruence

---

[3] Notons qu'en fait, les propositions précédentes n'utilisent pas toutes l'hypothèse complète (c) forte + (c'). Plus précisement,

$$\begin{array}{rcl} \text{(c) forte} & \Longleftrightarrow & \text{Propositions 1 et 1'} \\ \text{(c')} & \Longleftrightarrow & \text{Proposition 2} \\ \text{(c')} + \text{(c) forte} & \Longleftrightarrow & \text{Proposition 2'} \\ \text{(c)} & \Longleftrightarrow & 3. \end{array}$$

En effet, si x_n et y_m n'étaient pas minorés, on extrairait de S_k une suite S_h de solutions telles que

$$\lim_{h\to\infty} x_n = \lim_{h\to\infty} y_m = -\infty \quad \text{et} \quad \lim_{h\to\infty} \frac{y_m}{x_n} = \frac{v_{\mathfrak{p}_\alpha}(a)}{v_{\mathfrak{p}_\alpha}(b)},$$

pour tout diviseur commun $\mathfrak{p}_\alpha$. La proposition 3 et la proposition 2 (sous l'hypothèse (c')) sont donc encore exactes, même si on ne sait pas a priori que x_n et y_m sont minorés.

(C) $$a^y \equiv c \pmod{p^x} ,$$

a une infinité de solutions en $(x, y) \in \mathbb{N}^2$, alors

$$\lim_{x\to\infty} \frac{y}{x} = +\infty .$$

Remarquons d'abord que (C) ne peut avoir de solutions que si $v_p(c) = 0$. Ceci dit, distinguons les 2 cas :

1° Il n'existe pas d'entiers rationnels r et s tels que $a^r = c^s$.

Sous cette hypothèse, un théorème de GEL'FOND ([1], théorème II), nous dit que, pour $y > y_0(\varepsilon)$, la congruence

$$a^y \equiv c \pmod{p^{\log^{3+\varepsilon} y}} ,$$

est impossible. Il en résulte que, pour y suffisamment grand,

(10) $$x < \log^{3+\varepsilon} y .$$

2° Il existe des entiers rationnels r et s non nuls tels que $a^r = c^s$.

Sous cette hypothèse, un autre théorème de GEL'FOND ([1], théorème II'), nous dit qu'il existe un nombre τ_0, tel que, pour $\tau > \tau_0$, la congruence

$$a^y \equiv c \pmod{p^{\tau \log y}} ,$$

est impossible. Il en résulte qu'on a toujours

(10 bis) $$x < \tau_0 \log y .$$

De (10) ou de (10 bis), on déduit le résultat annoncé.

LEMME 6. - Dans le cas $|a| > 1$, $|b| > 1$, une suite S_h de solutions vérifie l'une ou l'autre des deux relations

(11) $$\limsup_{h\to\infty} \frac{y_2}{y_1} = 1 , \qquad \limsup_{h\to\infty} \frac{x_2}{x_1} = 1 .$$

Dans le cas $|a| < 1$, $|b| < 1$, une suite S_h de type III vérifie l'une ou l'autre des deux relations

(12) $$\liminf_{h\to\infty} \frac{y_{m-1}}{y_m} = 1 , \qquad \liminf_{h\to\infty} \frac{x_{n-1}}{x_n} = 1 .$$

Dans le cas $|a| > 1$, $|b| > 1$, (E) peut s'écrire

$$a^{y_1} b^{-x_1} - \frac{\mu_1}{\lambda_1} = \frac{\mu_2}{\lambda_1} b^{x_2 - x_1}(1 + \theta_b) - \frac{\lambda_2}{\lambda_1} a^{y_2} b^{-x_1}(1 + \theta_a) ,$$

avec $\theta_b = \sum_{j=3}^{n} \frac{\mu_j}{\mu_2} n^{x_j - x_2}$ et $\theta_a = \sum_{i=3}^{m} \frac{\lambda_i}{\lambda_2} a^{y_i - y_2}$, et

$$\lim_{h\to\infty} \theta_a = \lim_{h\to\infty} \theta_b = 0 .$$

On en déduit

$$|a^{y_1} b^{-x_1} - \frac{\mu_1}{\lambda_1}| \leqslant 2 \sup\left(|\frac{\mu_2}{\lambda_1}||1 + \theta_b||b|^{x_2 - x_1} , \ |\frac{\lambda_2}{\lambda_1}||1 + \theta_a||a|^{y_2} |b|^{-x_1}\right) .$$

Or un théorème de GEL'FOND ([2], théorème III, p. 28), nous dit que, sous l'hypothèse, vérifiée ici, d'indépendance multiplicative de a et de b, l'inéquation

$$|a^{y_1} b^{-x_1} - \frac{\mu_1}{\lambda_1}| < \exp(-\varepsilon \sup(x_1 , y_1)) ,$$

n'a, quel que soit ε, qu'un nombre fini de solutions. Si (E) a une suite S_h de solutions, c'est donc que, pour tout ε, ces solutions vérifient, pour x_1 et y_1 assez grands,

$$\exp(-\varepsilon \sup(x_1 , y_1)) < 2 \sup(|\frac{\mu_2}{\lambda_1}| |1 + \theta_b| |b|^{x_2 - x_1} , |\frac{\lambda_2}{\lambda_1}| |1 + \theta_a| |a|^{y_2} |b|^{-x_1})$$

c'est-à-dire

$$\varepsilon \sup(x_1 , y_1) > \inf((1 - \frac{x_2}{x_1})\log|b| + \frac{k_1 + \log|1 + \theta_b|}{x_1} ,$$

$$\log|b| - \frac{y_2}{x_1} \log|a| + \frac{k_2 + \log|1 + \theta_a|}{x_2}) ,$$

k_1 et k_2 étant deux constantes.

Quand h tend vers l'infini, y_1/x_1 tend vers $1/\alpha = \log|b|/\log|a|$; $\sup(1 , y_1/x_1)$ est donc borné. Il résulte donc de cette inégalité que, quels que soient ε' et $\varepsilon'' > 0$, les solutions appartenant à S_h, doivent, pour h suffisamment grand, vérifier l'une ou l'autre des deux inégalités

$$1 - \frac{x_2}{x_1} < \frac{\varepsilon'}{\log|b|}$$

$$\frac{1}{\alpha} - \frac{y_2}{x_1} < \frac{\varepsilon''}{\log|a|}$$

x_2/x_1 étant majoré par 1, et y_2/x_1 l'étant par y_1/x_1 qui a pour limite $1/\alpha$ quand h tend vers l'infini, il en résulte que les solutions appartenant à S_h devraient vérifier l'une au moins des deux relations

$$(11) \qquad \limsup_{h\to\infty} \frac{x_2}{x_1} = 1 , \qquad \limsup_{h\to\infty} \frac{y_2}{x_1} = \frac{1}{\alpha}$$

qui entraînent respectivement

$$\limsup_{h\to\infty} \frac{x_2}{y_1} = \alpha , \qquad \limsup_{h\to\infty} \frac{y_2}{y_1} = 1 .$$

Soit maintenant $|a| < 1$, $|b| < 1$. Ecrivons cette fois (E) sous la forme

$$a^{y_m} b^{-x_n} - \frac{\mu_n}{\lambda_m} = \frac{\mu_{n-1}}{\lambda_m} b^{x_{n-1}-x_n}(1 + \theta_b') - \frac{\lambda_{m-1}}{\lambda_m} a^{y_{m-1}} b^{-x_n}(1 + \theta_a')$$

avec $\theta_b' = \sum_{j=1}^{n-2} \frac{\mu_j}{\mu_{n-1}} b^{x_j - x_{n-1}}$ $\theta_a' = \sum_{i=1}^{m-2} \frac{\lambda_i}{\lambda_{m-1}} a^{y_i - y_{m-1}}$ et

$$\lim_{h\to\infty} \theta_b' = \lim_{h\to\infty} \theta_a' = 0 ,$$

D'où

$$(13) \quad |a^{y_m} b^{-x_n} - \frac{\mu_n}{\lambda_n}| < 2 \sup(|\frac{\mu_{n-1}}{\lambda_m}| |b|^{x_{n-1}-x_n} |1 + \theta_b'| , |\frac{\lambda_{m-1}}{\lambda_m}| |a|^{y_{m-1}} |b|^{-x_n} |1 + \theta_a'|)$$

Par utilisation du même théorème de Gel'fond et, en raisonnant comme ci-dessus, on arrive au fait que les solutions appartenant à S_h satisfont, pour tout ε' et ε'' positifs à

$$\frac{x_{n-1}}{x_n} < 1 + \varepsilon' \quad \text{ou} \quad \frac{y_{m-1}}{x_n} < \frac{1}{\alpha} + \varepsilon'' ,$$

d'où

$$\liminf \frac{x_{n-1}}{x_n} = 1 \quad \text{ou} \quad \liminf \frac{y_{m-1}}{x_n} = \frac{1}{\alpha} ,$$

mais la deuxième de ces relations entraîne $\liminf \dfrac{y_{m-1}}{y_n} = 1$.

LEMME 7. - <u>Dans le cas où a et b ne sont pas étrangers, une suite S_h , de type III, de solutions de (E) vérifient l'une ou l'autre des deux relations</u>.

$$\liminf \frac{x_{n-1}}{x_n} = 1, \ \liminf \frac{y_{m-1}}{y_m} = 1 .$$

Soit $\mathfrak{p}$ tel que $v_{\mathfrak{p}}(a)$ et $v_{\mathfrak{p}}(b)$ soient positifs.

Ecrivons encore (E) sous la forme (13) ; pour h suffisamment grand,

$$v_{\mathfrak{p}}(1 + \theta'_a) = v_{\mathfrak{p}}(1 + \theta'_b) = 0 .$$

On a donc

$$|a^{y_m} b^{-x_n} - \frac{\mu_n}{\lambda_m}|_{\mathfrak{p}} \leqslant \sup(|\frac{\mu_{n-1}}{\lambda_m} b^{x_{n-1}-x_n}|_{\mathfrak{p}} , |\frac{\lambda_{m-1}}{\lambda_m} a^{y_{m-1}} b^{-x_n}|_{\mathfrak{p}} .$$

Or, la partie $\mathfrak{p}$-adique du théorème de Gel'fond ([2], théorème III, p. 28), dit que sous l'hypothèse d'indépendance multiplicative de a et de b , la congruence

$$a^{y_m} b^{-x_n} \equiv \frac{\mu_n}{\lambda_n} \pmod{\mathfrak{p}^{\delta \sup(x_n, y_m)}} ,$$

n'a, quel que soit δ , qu'un nombre fini de solutions. Si (E) a une suite S_h de solutions, c'est donc que, pour tout δ , ces solutions vérifient

$$\delta \sup(x_n , y_m) > \inf((x_{n-1} - x_n) v_{\mathfrak{p}}(b) + k_1 , y_{m-1} v_{\mathfrak{p}}(a) - x_n v_{\mathfrak{p}}(b) + k_2) ,$$

k_1 et k_2 étant deux constantes. D'où, en raisonnant comme au lemme 6 et en tenant compte de ce que, pour une suite de type III, $\lim_{h\to\infty} \frac{y_m}{x_n} = v_{\mathfrak{p}}(b)/(v_{\mathfrak{p}}(a))$, on voit que, pour tout ε' et ε'' positifs, les solutions vérifient

$$\frac{x_{n-1}}{x_n} - 1 < \varepsilon' \quad \text{ou} \quad \frac{y_{m-1}}{x_n} v_{\mathfrak{p}}(a) - v_{\mathfrak{p}}(b) < \varepsilon'' ;$$

on a donc

$$\liminf \frac{x_{n-1}}{x_n} = 1 \quad \text{ou} \quad \liminf \frac{y_{m-1}}{x_n} = \frac{v_{\mathfrak{p}}(b)}{v_{\mathfrak{p}}(a)} ,$$

la deuxième de ces relations entraînant $\liminf \dfrac{y_{m-1}}{y_m} = 1$.

Nous obtenons alors les **résultats** particuliers suivants (a et b sont toujours supposés être des entiers algébriques non nuls qui ne sont pas des unités et satisfont à (c) forte et (c')) .

PROPOSITION 4. - L'équation

$$\lambda_1\, a^{y_1} + \lambda_2\, a^{y_2} = \mu_1\, b^{x_1} + \mu_2\, b^{x_2} ,$$

ne peut avoir une infinité de solutions.

Examinons les différentes possibilités dont nous avons fait la liste.

1° Cas $|a| > 1$, $|b| > 1$, $(a , b) = 1$.

(α) Suite de type I. - Les solutions vérifieraient

$$\lambda_1\, a^{y_1} + c = \mu_1\, b^{x_1} .$$

Si $c = 0$, on a vu que l'équation ne pouvait avoir plus d'une solution sans contredire la condition (c).

Si $c \neq 0$, choisissons un idéal $\mathfrak{p}$, premier, de $K(a , b)$, tel que

$$v_{\mathfrak{p}}(a) = v > 0 , \qquad v_{\mathfrak{p}}(b) = 0 ;$$

les solutions appartenant à S_h vérifieraient

$$\mu_1\, b^{x_1} \equiv c \pmod{\mathfrak{p}^{vy_1}} ,$$

d'où (lemme 5)

$$\lim_{h\to\infty} \frac{x_1}{y_1} = +\infty ,$$

ce qui est en contradiction avec le fait que $\lim_{h\to\infty}(x_1/y_1) = \alpha$.

(β) Suite de type II. - Les solutions vérifieraient

$$\lambda_1\, a^{y_1} + \lambda_2\, a^{y_2} = \mu_1\, b^{x_1} + c ,$$

(ou une équation analogue avec échange des rôles de a et de b).

En choisissant $\mathfrak{p}$ comme ci-dessus, on obtient

$$\mu_1\, b^{x_1} \equiv - c \pmod{\mathfrak{p}^{y_2 v}}$$

d'où $\lim_{h\to\infty} \dfrac{x_1}{y_2} = +\infty$.

Mais des deux relations (11), du lemme 6, seule la seconde est ici possible, et il y a donc contradiction.

(γ) Suite de type III. - L'équation peut s'écrire

$$a^{y_2}(\lambda_1\, a^{y_1 - y_2} + \lambda_2) = b^{x_1}(\mu_1\, b^{x_1 - x_2} + \mu_2) .$$

Choisissant encore $\mathfrak{p}$ comme ci-dessus, on voit que les solutions doivent vérifier

$$\mu_1\, b^{x_1 - x_2} \equiv - \mu_2 \pmod{\mathfrak{p}^{vy_2}} ,$$

d'où $\lim_{h\to\infty} \dfrac{x_1 - x_2}{y_2} = +\infty$, donc

(14) $$\lim_{h\to\infty} \frac{x_1}{y_2} = +\infty .$$

Mais d'autre part, en considérant $\mathfrak{p}'$ tel que

$$v_{\mathfrak{p}'}(a) = 0 , \qquad v_{\mathfrak{p}'}(b) = w' > 0 ,$$

on a

(15) $$\lim_{h\to\infty} \frac{x_2}{y_1} = +\infty .$$

Les relations (14) et (15) contredisent l'ensemble des relations (11) dont l'une au moins était vraie.

2° Cas $|a| > 1$, $|b| > 1$, $(a , b) \neq 1$.

<u>Suite de type III.</u> - Etant donné que $r(a) \neq r(b)$, les hypothèses entraînent :

$$\exists\, \mathfrak{p} , \quad v_{\mathfrak{p}}(a) = v > 0 , \quad v_{\mathfrak{p}}(b) = 0 ,$$
$$\exists\, \mathfrak{p}' , \quad v_{\mathfrak{p}'}(a) = v' > 0 , \quad v_{\mathfrak{p}'}(b) = w' > 0 ,$$

ou des circonstances analogues avec échange des rôles de a et de b ($\mathfrak{p}$ et $\mathfrak{p}'$ désignant toujours des idéaux premiers de $K(a , b)$).

De l'existence de $\mathfrak{p}$, on conclut comme précédemment

(16) $$\lim_{h\to\infty} \frac{x_1}{y_2} = +\infty .$$

Mais d'autre part, $\lim_{h\to\infty} \frac{x_2}{y_2} = \frac{v'}{w'}$ d'où

(17) $$\lim_{h\to\infty} \frac{x_2}{x_1} = \lim_{h\to\infty} \frac{x_2}{y_2} \times \frac{y_2}{x_1} = \frac{v'}{w'} \times 0 = 0 .$$

L'ensemble de (16) et (17) contredit encore (11).

3° Cas $|a| < 1$, $|b| < 1$, $(a , b) = 1$.

<u>Suite de type III.</u> - (16) et (17) sont encore vraies, et leur ensemble contredit les relations (12) du lemme 6.

PROPOSITION 5. - <u>L'équation</u> $\sum_{i=1}^{m} \lambda_i\, a^{y_i} = \mu b^x$, <u>où</u> a <u>et</u> b <u>sont des entiers algébriques non nuls satisfaisant à la condition</u> (c) <u>forte, ne peut avoir une infinité de solutions, sauf, peut-être, si les quatre conditions suivantes, sont simultanément réalisées</u> :

(α) $(\mu/\lambda_m)^p = a^q u$, $p \in \mathbb{Z}$, $q \in \mathbb{Z}$, u unité algébrique,

(β) $|a| > 1$, $|b| > 1$,

(γ) $(a , b) = 1$, ou (γ') $b^s = a^r b'$, $s \in \mathbb{N}$, $r \in \mathbb{N}$,

(δ) $m > 3$, avec b' entier, $|b'| > 1$, $(a , b') = 1$.

Observons déjà qu'elle ne peut avoir une suite de solution de type III que si tout diviseur premier de a divise b (sans quoi la valuation correspondante du 1er membre tendrait vers l'infini, celle du second restant fixe). Ceci montre déjà qu'il ne peut y avoir une infinité de solutions quand $|a| < 1$, $|b| < 1$ (lemme 4 et proposition 2).

Nous devons donc supposer $|a| > 1$, $|b| > 1$. Par ailleurs, l'existence d'une suite de type I étant clairement impossible, les seules possibilités à examiner sont :

1° $(a , b) = 1$, suite de type II.

2° $r(a)|r(b)$, suite de type III. Notons alors que, du fait du lemme 4, les idéaux premiers communs auront, dans ce cas, des exposants proportionnels, c'est-à-dire qu'il existera deux entiers naturels r et s , tels que $b^r = a^s$ avec $(a , b') = 1$, b' entier.

Nous devrons avoir (γ) ou (γ') .

Eximinons alors la première possibilité, c'est-à-dire celle de l'existence d'une infinité de solutions où y_m garde une valeur fixe. Pour tout idéal $\mathfrak{p}$ divisant a , on aurait, pour $y_{m-1} - y_m$ assez grand,

$$y_m \, v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(\mu) - v_{\mathfrak{p}}(\lambda_m) \; .$$

Il en résulte que $(v_{\mathfrak{p}}(\mu) - v_{\mathfrak{p}}(\lambda_m))/v_{\mathfrak{p}}(a)$ est un entier rationnel q indépendant de l'idéal $\mathfrak{p}$. La condition (α) est donc nécessaire pour que cette première possibilité puisse se réaliser.

Examinons maintenant la deuxième. Nous avons :

$$b^r = a^s \, b' \; , \qquad (a , b') = 1 \; .$$

Soient d et f tels que

$$d^r = a \; , \qquad f^r = b' \; ;$$

on a $b = d^s fu$, u étant une racine de 1 ; en posant $fu = g$, (E) s'écrit donc

$$\sum_{i=1}^m \lambda_i \, d^{ry_i} = \mu d^{sx} g^x \; ,$$

ou, en posant $rg_i - sx = z_i$,

$$\sum_{i=1}^m \lambda_i \, d^{z_i} = \mu g^x \; . \tag{18}$$

Si (E) a une infinité de solutions, l'équation (18) a aussi une infinité de solutions en (z_i , x) . Or d et g sont des entiers algébriques qui ne sont pas des unités (car si g en était une, b' en serait une aussi, et a et b ne satisferaient pas à (c) forte.) Ils sont premiers entre eux, puisque a et b' le sont. Ils satisfont donc à (c) forte. Ils satisfont aussi à (c') puisque

$$\frac{\log|g|}{\log|d|} = \frac{\log|b'|}{\log|a|} = r\,\frac{\log|b|}{\log|a|} - s \; ,$$

est irrationnel. Nous sommes donc ramenés au cas précédent et, pour que (18) aient des solutions, il faut que $\mu/\lambda_m = d^q u$ $(q \in \underset{\sim}{Z})$, donc $(\mu/\lambda_m)^r = a^q u^r$; la condition (α) est encore nécessaire. Il faut aussi que d et g soient de modules supérieurs à 1 , ce qui exige que b' le soit.

Reste à montrer que l'équation n'a pas une infinité de solutions quand $m = 3$

et, d'après ce qu'on vient de voir, il suffit de montrer que, sous l'hypostèse (γ), elle ne peut avoir une suite de type II de solutions, puisqu'on se ramène à ce cas dans le cas (γ').

D'après le lemme 6, on a

$$(19) \qquad \lim_{h\to\infty} \frac{y_2}{x} = \frac{1}{\alpha} .$$

Mais d'autre part, les solutions d'une suite de type II vérifieraient

$$\lambda_1 a^{y_1} + \lambda_2 a^{y_2} + c = \mu b^x .$$

En choisissant p tel que $v_p(a) = v > 0$, $v_p(b) = 0$, on devrait avoir

$$\mu b^x \equiv c \pmod{p^{vy_2}} ,$$

d'où $\lim_{h\to\infty} \frac{x}{y_2} = +\infty$ contrairement à (19), ce qui termine la démonstration.

PROPOSITION 6. - <u>Quand a et b ne sont pas étrangers, l'équation</u>

$$\lambda_1 a^{y_1} + \lambda_2 a^{y_2} + \lambda_3 a^{y_3} = \mu_1 b^{x_1} + \mu_2 b^{x_2} ,$$

<u>ne peut avoir une infinité de solutions.</u>

La seule éventualité, a priori possible, est celle d'une suite de type III, dans le cas $|a| > 1$, $|b| > 1$. Comme lors de l'étude de la même éventualité pour l'équation de la proposition 4, choisissons p et p' tels que

$$v_p(a) = v > 0 , \quad v_p(b) = 0 ,$$

$$v_{p'}(a) = v' > 0 , \quad v_{p'}(b) = w' > 0 .$$

On en déduira de la même façon, d'une part

$$\lim_{h\to\infty} \frac{x_1 - x_2}{vy_3} = +\infty ,$$

d'où $\lim_{h\to\infty} \frac{x_1}{y_3} = +\infty$, d'autre part

$$\lim_{h\to\infty} \frac{x_2}{y_3} = \frac{v'}{w'} ,$$

et de ces deux relations, on déduit

$$(20) \qquad \lim_{h\to\infty} \frac{x_1}{x_2} = +\infty .$$

Or, en vertu du lemme 6, on peut extraire de S_h, soit une suite $S_{h'}$, telle que $\lim_{h'\to\infty} \frac{x_2}{x_1} = 1$, ce qui est impossible en vertu de (20), soit une suite $S_{h''}$ telle que $\lim_{h''\to\infty} \frac{y_2}{y_1} = 1$.

Considérons donc $S_{h''}$. En vertu du lemme 7, on peut en extraire une sous-suite S_ℓ telle que

$$\lim_{\ell\to\infty} \frac{x_2}{x_1} = 1 ,$$

ce que nous avons déjà exclu, ou une sous-suite $S_{\ell'}$ telle que

$$\lim_{\ell' \to \infty} \frac{y_2}{y_3} = 1 .$$

On aurait donc, pour $S_{\ell'}$,

$$\lim_{\ell' \to \infty} \frac{y_1}{y_3} = 1 ,$$

mais ceci est incompatible avec

$$\lim_{\ell' \to \infty} \frac{x_1}{y_1} = \alpha , \qquad \lim_{\ell' \to \infty} \frac{x_1}{y_3} = + \infty ,$$

ce qui termine la démonstration.

BIBLIOGRAPHIE

[1] GEL'FOND (A. O.). - Sur la divisibilité de la différence des puissances de deux nombres entiers par une puissance d'un idéal premier, Mat. Sbornik, Nouvelle Série, t. 7, 1940, p. 7-25.

[2] GEL'FOND (A. O.). - Transcendental and algebraic numbers. Translated from the 1rst (1952) russian edition. - New York, Dover Publications, 1960.

(Texte reçu le 29 novembre 1971)

Germaine REVUZ
Université de Poitiers
Mathématiques
40 avenue du Recteur Pineau
86022 POITIERS