**Zeitschrift:** L'Enseignement Mathématique
**Herausgeber:** Commission Internationale de l'Enseignement Mathématique
**Band:** 33 (1987)
**Heft:** 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

**Artikel:** SUITES RÉCURRENTES LINÉAIRES Propriétés algébriques et arithmétiques
**Autor:** Cerlienco, L. / Mignotte, M. / Piras, F.
**Kapitel:** II. MÉTHODES p-ADIQUES
**DOI:** https://doi.org/10.5169/seals-87887

— Si $m \not\equiv 0 \pmod 3$ on a $(F_m, L_m) = 1$ donc $F_m = y^2$ et $L_m = z^2$. Par conséquent $m = 1$ ou $3$, $F_n = 1$ ou $8$; le seul carré est encore 1.

— Si $m \equiv 0 \pmod 3$ alors $(F_m, L_m) = 2$ et donc $F_m = 2y^2$ et $L_m = 2z^2$. Si $m$ est impair on a $z^4 - 5y^4 = -1$, ce qui est impossible modulo 8. Si $m = 2m'$ alors $F_{m'} L_{m'} = 2y^2$. Si $m'$ est impair on a $F_{m'} = 2t^2$ et $L_{m'} = w^2$ donc $m' = 1$ ou $3$ et $F_n = 1$ ou $144$. Si $m'$ est pair alors $F_{m'} = t^2$; dans ce cas, tout ce qui précède montre que $n = 3 \cdot 2^s s \geqslant 3$ et que les nombres de Fibonacci d'indices $n/4$, $n/16$... sont tous des carrés mais, comme $F_6 = 8$ et $F_{48}$ ne sont pas des carrés, ce dernier cas est impossible. [Il n'est pas nécessaire de calculer $F_{48}$: si $F_{48} = x^2$ alors $F_{24} = 2y^2$ puis $L_{12} = 2z^2$, mais $L_{12} = 322$.]

## II. Méthodes $p$-adiques

Pour une introduction aux nombres $p$-adiques, le lecteur pourra consulter Borevitch et Schafarevitch [10] ou J. P. Serre [54], et pour une étude plus détaillée de l'analyse $p$-adique Y. Amice [2] ou K. Mahler [36].

### 1. *Le théorème de Skolem-Mahler*

Théorème. *Soit $(\xi_n)$ une suite récurrente linéaire à valeurs entières. Alors l'ensemble des indices $n$ tels que $\xi_n$ soit nul est égal à une union finie de progressions arithmétiques (certaines de ces progressions peuvent être de raison nulle et l'union peut même être vide!).*

Comme en A.I.3, écrivons $\xi_n$ sous la forme

$$\xi_n = P_1(n)\,\omega_1^n + \ldots + P_k(n)\,\omega_k^n \quad \text{pour} \quad n \geqslant 0\,,$$

les $P_j$ étant des polynômes à coefficients dans le corps de nombres $L = \mathbf{Q}(\omega_1, \ldots, \omega_k)$, et soit $\mathfrak{P}$ un idéal premier de $L$ tel que les $\omega_j$ soient tous des $\mathfrak{P}$-unités. Il est facile de voir que, pour tout $\varepsilon > 0$, il existe un entier $T$ tel que

$$|\,\omega_j^T - 1\,|_{\mathfrak{P}} < \varepsilon\,, \quad j = 1, \ldots, k\,.$$

En particulier, il existe un entier $T$ tel que chacune des $T$ fonctions (à valeurs dans le complété $L_{\mathfrak{P}}$ de $L$)

$$f_m : x \to P_j(xT+m)\omega_j^m \exp\big((\operatorname{Log} \omega_j^T)x\big)\,, \quad m = 0, 1, \ldots, T-1\,,$$

où exp et Log sont l'exponentielle et le logarithme $\mathfrak{P}$-adiques, soient définies et analytiques pour $x$ parcourant l'anneau $\mathbf{Z}_p$ des entiers $p$-adiques ($p$ étant le nombre premier au-dessous de $\mathfrak{P}$).

Bien sûr, pour $n$ entier, on a $f_m(n) = \xi_{nT+m}$. Donc, si la suite $(\xi_n)$ possède une infinité de zéros, il en est de même pour certaines des fonctions $f_m$. Or, chaque $f_m$ est une fonction analytique sur l'ensemble compact $\mathbf{Z}_p$ et, à moins d'être identiquement nulle, elle ne possède qu'un nombre fini de zéros. D'où la conclusion. □

COROLLAIRE. *Si* $(\xi_n)$ *admet une infinité de zéros, alors, si* $\xi_n$ *s'écrit comme plus haut*

$$\xi_n = P_1(n)\,\omega_1^n + \ldots + P_k(n)\,\omega_k^n,$$

*où les* $P_j$ *sont des polynômes non nuls et les* $\omega_j$ *des nombres algébriques non nuls; pour tout* $i$ *il existe un indice* $j \neq i$ *tel que* $\omega_i/\omega_j$ *soit une racine de l'unité.*

Soit en effet $m$ tel que l'on ait $\xi_{nT+m} = 0$ pour tout $n$. La conclusion résulte de la formule

$$P_1(nT+m)\,\omega_1^m \cdot \omega_1^{Tn} + \ldots + P_k(nT+m)\,\omega_k^m \cdot \omega_k^T = 0, \qquad n \geqslant 0,$$

et du fait qu'un polynôme exponentiel $\Sigma\, R_h(n)\,\rho_h^n$, relatifs à des $\rho_h$ deux à deux distincts, ne peut s'annuler que si les polynômes $R_h$ sont tous nuls (ce qu'on a déjà vu en A.III.3.c)). □

On peut se poser le problème de savoir décider si $(\xi_n)$ comporte ou non une infinité de zéros. Pour cela, remarquons d'abord que l'idéal $\mathfrak{P}$ et le nombre $T$ qui apparaissent dans la démonstration ci-dessus peuvent être déterminés effectivement; il suffit, par exemple, de choisir $\mathfrak{P}$ au-dessus d'un nombre premier qui ne divise pas le produit $\omega_1 \ldots \omega_k$. Discr $(\omega_1, \ldots, \omega_k)$, on peut alors prendre $T = p^f - 1$ avec $f = [L:\mathbf{Q}]$ (donc $f \leqslant k!$). On considère alors les $T$ suites $(\xi_{nT+m})_{n\geqslant 0}$, $m = 0, 1, \ldots, T-1$ et on a vu que $(\xi_n)$ a une infinité de zéros si, et seulement si, une de ces suites est (identiquement) nulle. Enfin comme chacune de ces $T$ suites est une s.r.l. d'ordre $k$, elle est identiquement nulle si, et seulement si, ses $k$ premières valeurs sont nulles. Pour répondre à la question il suffit donc de calculer les $Tk$ premières valeurs $\xi_n$. (A ce sujet, voir aussi Berstel-Mignotte [6].)

Par contre la preuve du théorème de Skolem-Mahler ne permet pas de déterminer effectivement tous les zéros de $(\xi_n)$, mais seulement — comme nous venons de voir — tous les zéros sauf peut-être un nombre fini d'entre eux. Cependant, le théorème suivant — dû à Strassman — permet de majorer le nombre de zéros de $(\xi_n)$, lorsque ce nombre est fini.

THÉORÈME. *Soit* $f(x) = \sum_{k \geqslant 0} a_k x^k$, *les* $a_k$ *appartenant à un corps* $\mathfrak{P}$*-adique* $K_{\mathfrak{P}}$, *une série qui converge sur l'anneau* $O_{\mathfrak{P}}$, *et qui n'est pas identiquement nulle. Alors le nombre de zéros de* $f$ *dans l'ensemble* $O_{\mathfrak{P}}$ *est majoré par la quantité* $\max \{k \geqslant 0 ; | a_k |_{\mathfrak{P}}$ *est maximal*$\}$.

On trouvera une démonstration dans l'article de Lewis [32]. □

## 2. *Un exemple*

Avec de la chance, on peut quelquefois déterminer l'ensemble des zéros d'une suite récurrente linéaire en n'utilisant que l'analyse $p$-adique.

Considérons l'exemple suivant, dû à J. Berstel, de la suite définie par

$$\xi_0 = \xi_1 = 0, \quad \xi_2 = 1, \quad \xi_{n+3} = 2\xi_{n+3} - 4\xi_{n+1} + 4\xi_n \quad \text{pour} \quad n \geqslant 0.$$

On constate que l'on a

$$\xi_0 = \xi_1 = \xi_4 = \xi_6 = \xi_{13} = \xi_{52} = 0.$$

Nous allons montrer que les zéros trouvés ci-dessus sont les seuls. Choisissons $p = 53$. Modulo $p$, le polynôme $G = X^3 - 2X^2 + 4X - 4$ se décompose en facteurs linéaires distincts. Soient $\omega_1$, $\omega_2$ et $\omega_3$ les racines de $G$ dans le corps $\mathbf{Q}_p$, ce sont des $p$-unités. Comme $p$ divise les $\omega_j^{p-1} - 1$, les 52 fonctions

$$n \mapsto \xi_{52n+m}, \quad m = 0, 1, ..., 51,$$

se prolongent en des fonctions analytiques $f_m$ de $\mathbf{Z}_p$ dans lui-même. Posons

$$f_m(x) = \sum_{k \geqslant 0} a_{k,m} x^k ;$$

on vérifie facilement que l'on a

$$(*) \qquad p^i \mid a_{k,m} \quad \text{si} \quad k \geqslant i, \quad \text{pour} \quad i = 1, 2, 3$$

(où le symbole | signifie divise).
On constate que

$$p \nmid f_m(0) = \xi_m \quad \text{si} \quad m \notin \{0, 1, 4, 6, 13\} \quad \text{et} \quad 0 \leqslant m \leqslant 51,$$

et dans ce cas une égalité

$$f_m(x) = a_{0,m} + (\sum_{k \geqslant 1} a_{k,m} x^k) = 0$$

est impossible pour $x$ dans $\mathbf{Z}_p$ [puisque $p$ divise la somme entre parenthèses mais pas $a_{0,m} = \xi_m$].

Pour $m = 1, 4, 6, 13$, on a

$$f_m(0) = 0\,, \quad 53 \mid f_m(1) \quad \text{mais} \quad f_m(1) \not\equiv 0 \pmod{53^2}$$

et, en utilisant la propriété (*) pour $i = 2$, on voit que

$$f_m(x) = x(a_{1,m} + \sum_{k \geqslant 2} a_{k,m}\, x^{k-1}) \neq 0 \quad \text{si} \quad x \in \mathbf{Z}_p^*\,.$$

Enfin, pour $m = 0$, on a (en oubliant l'indice zéro)

$$f(0) = f(1) = 0\,, \quad f(2) \equiv 0 \pmod{p^2} \quad \text{et} \quad f(2) \not\equiv 0 \pmod{p^3}\,,$$

$$f(x) = x(a_1 + \sum_{k \geqslant 2} a_k\, x^{k-1}) \quad \text{avec} \quad p^2 \mid a_1 \quad \text{mais} \quad a_1 \not\equiv 0 \pmod{p^3};$$

mais ici la méthode précédente ne s'applique plus, nous avons besoin d'un outil plus puissant.

Pour $k$ entier positif, posons

$$(X)_k = X(X-1)\ldots(X-k+1)\,, \quad \text{et en particulier} \quad (X)_0 = 1\,.$$

Du fait que $X^n$ est une combinaison linéaire à coefficients entiers des $(X)_i$ pour $0 \leqslant i \leqslant n$, on voit qu'une série $\Sigma\, a_n\, X^n$ peut se mettre sous forme $\Sigma\, b_n \,.\, (X)_n$ avec $p^j \mid b_n$ si $p^j \mid a_m$ pour tout $m \geqslant n$. Si on applique ceci à l'exemple de $f_0$, on trouve

$$f(x) = f_0(x) = b_2 \,.\, (x)_2 + \sum_{k \geqslant 3} b_k \,.\, (x)_k\,,$$

où $p^2 \mid b_2$, $b_2 \not\equiv 0 \pmod{p^3}$ et $p^3 \mid b_k$ si $k \geqslant 3$ (utiliser (*) avec $i=3$). Donc $f$ s'écrit

$$f(x) = b_2\, x(x-1)\,(1+g(x)) \quad \text{avec} \quad p \mid g(x) \quad \text{si} \quad x \in \mathbf{Z}_p\,.$$

Ceci montre que, pour $z$ parcourant $\mathbf{Z}_p$, les seuls zéros de $f_0$ sont 0 et 1. D'où le résultat annoncé.

Pour d'autres détails sur cet exemple voir [37] et [44].

3. *Multiplicités de suites récurrentes linéaires*

Ce sujet a été traité très en détail par R. Tijdeman dans son exposé [60], ce qui nous permet d'être relativement brefs.

Nous ne considérerons ici que des suites à valeurs dans un anneau $\mathscr{A}$ contenu dans le corps des complexes. Pour un élément $a$ de cet anneau, la *a-multiplicité* de la suite $(\xi_n)$ est le nombre d'indices $n$ pour lesquels

$\xi_n = a$; la *multiplicité* est la borne supérieure de ses $a$-multiplicités lorsque $a$ parcourt $\mathscr{A}$. Lorsque $(\xi_n)$ est une s.r.l. de rang $m$, sa multiplicité est égale à la 0-multiplicité d'une s.r.l. de rang au plus $m + 1$ [ceci résulte de l'exemple de A.II]. Inversement, si $\mathscr{A}$ est un corps et si le polynôme caractéristique d'une s.r.l. $(\xi_n)$ a une racine simple $\omega_k$ alors la 0-multiplicité de $(\xi)$ est majorée par la multiplicité d'une s.r.l. $(\eta_n)$ de rang $m - 1$, $m$ étant le rang de $(\xi_n)$; en effet on a alors

$$\xi_n = P_1(n)\,\omega_1^n + \ldots + P_{k-1}(n)\,\omega_{k-1}^n + P_k\,\omega_k^n,\ P_k \text{ constant},$$

et il suffit de poser

$$\eta_m = P_1(n)\,(\omega_1/\omega_k)^n + \ldots + P_{k-1}(n)\,(\omega_1/\omega_{k-1})^n,$$

et la 0-multiplicité de $(\xi_n)$ est égale à la — $P_m$ — multiplicité de $(\eta_n)$.

On dira que $(\xi_n)$ est *dégénérée* lorsqu'il existe $\alpha$ tel que son $\alpha$-multiplicité soit infinie. Cette définition diffère de celle de [60] où la suite est dite dégénérée ssi sa 0-multiplicité est infinie. D'après le paragraphe précédent, on sait tester si une s.r.l. est dégénérée ou non.

Le problème de la multiplicité a surtout été étudié pour le premier cas non trivial, celui des s.r.l. binaires non dégénérées et à valeurs entières. M. Ward, qui a écrit plusieurs dizaines d'articles sur les suites récurrentes linéaires, avait conjecturé dans les années trente que la multiplicité d'une telle suite ne dépasse pas 5.

Après des travaux de Skolem, Chowla, Dunton, Lewis, Laxton... Kubota a prouvé cette conjecture, et même montré que la multiplicité d'une telle suite n'excède jamais 4, voir [31]. Nous avons placé l'étude de la multiplicité d'une s.r.l. dans le chapitre relatif aux méthodes $p$-adiques, en effet la preuve de Kubota utilise de manière essentielle la méthode de Skolem, mais elle est trop compliquée pour que nous puissions en donner une idée ici. Les résultats de Kubota ont ensuite été améliorés par Beukers [8] qui a montré que la somme de la $a$-multiplicité et de la $(-a)$-multiplicité d'une suite récurrente binaire entière non dégénérée est au plus 3 sauf dans le cas de la suite

$$\xi_{n+2} = \xi_{n+1} - 2\,\xi_n, \qquad \xi_0 = \xi_1 = 1$$

où cette somme vaut 5 ($\xi_0 = \xi_1 = 1$ et $\xi_2 = \xi_4 = \xi_{12} = -1$)

et dans quatre autres cas (explicites) où cette somme vaut 4. L'exemple de la suite $(\xi_n)$ définie par

$$\xi_0 = \xi_1 = 1, \qquad \xi_{n+2} = -\xi_{n+1} + N\,\xi_n \quad (\text{donc } \xi_3 = 1),$$

avec $N$ entier quelconque montre qu'il existe une infinité de suites récurrentes linéaires entières et non dégénérées dont la multiplicité est égale à trois.

Notons une conjecture énoncée en [60] par R. Tijdeman.

CONJECTURE. Si $(\xi_n)$ est une s.r.l. binaire entière non dégénérée et si $\xi_s = \xi_t$ avec $r < s < t$ alors la différence $t - r$ est bornée par une constante absolue.

Récemment Beukers et Tijdeman ont démontré des résultats généraux sur la multiplicité des s.r.l. binaires à valeurs complexes, voir [9], leur article contient en particulier le très joli résultat suivant.

THÉORÈME. *Soit* $\alpha$ *un nombre complexe de module* $\geqslant 2$ *et soit* $L$ *une droite du plan complexe qui ne passe pas par l'origine. Alors, au plus sept puissances entières de* $\alpha$ *sont sur* $L$.

Ce travail n'utilise pas l'analyse $p$-adique mais les polynômes hypergéométriques, méthode qui remonte à Thue et Siegel.

4. *Critères de rationalité*

La partie A conduit au critère de rationalité suivant: Une série formelle

$$\Xi(t) = \sum_{n \geqslant 0} \xi_n t^n$$

à coefficients dans un corps $\mathscr{K}$ représente une fraction rationnelle si, et seulement si, il existe $k$ tel que, pour $N$ assez grand, le déterminant de Hankel d'ordre $N$ associé à la suite $(\xi_{n+k})_{n \geqslant 0}$ est nul.

Grâce à cette caractérisation, Dwork a considérablement généralisé un résultat de Borel et obtenu un théorème qui, dans le cas rationnel, s'énonce ainsi.

THÉORÈME. *Soit une série formelle à coefficients rationnels*

$$\Xi(t) = \sum_{n \geqslant 0} \xi_n t^n .$$

*S'il existe un ensemble fini* $S$ *de nombres premiers tels que*

(i) *pour* $p \notin S$, *chaque* $\xi_n$ *admet un dénominateur non divisible par* $p$,

(ii) $\Xi$ *définit une fonction méromorphe dans un disque de* $\mathbf{C}$ *de rayon* $R_0$,

(iii) *pour* $p \in S$, $f$ *définit dans* $\mathbf{C}_p$ *une fonction méromorphe dans un disque ouvert du centre* 0 *et de rayon* $R_p$,

(iv) *on a* $R_0 \cdot \prod_{p \in S} R_p \geqslant 1$,

*alors $f$ est une fonction rationnelle.* (Le corps $\mathbf{C}_p$ est le complété de la clôture algébrique de $\mathbf{Q}_p$).

Le théorème de Borel correspond au cas où $S$ est vide. Le principe de la démonstration du théorème ci-dessous est le suivant. On considère, pour $k$ assez grand, le déterminant du Hankel $H_N$ d'ordre $N$ de la suite $(\xi_{n+k})$ et on majore $|H_N|_v$ pour toutes les places $v$ du corps $\mathbf{Q}$:

— Si $v$ est ultramétrique et n'appartient pas à $S$, alors trivialement

$$|H_N|_v \leqslant 1 .$$

— Si $v \in S$ on utilise les inégalités de Cauchy dans $\mathbf{C}_p$.

— Si $v$ est la valeur absolue ordinaire, on utilise les inégalités de Cauchy dans $\mathbf{C}$.

Pour $k$ et $N$ assez grands, on aboutit à l'estimation

$$\prod_v |H_N|_v < 1 ,$$

qui implique $H_N = 0$. D'où la conclusion.

Une démonstration détaillée figure en [2], ainsi que celle du théorème de Polya-Bertrandias, qui généralise le théorème précédent.

## III. Méthodes transcendantes

### 1. *Minoration de* $|\xi_n|$

Grâce au théorème de Roth-Ridout, K. Mahler [35] avait obtenu une minoration non effective de $|\xi_n|$ pour une s.r.l. binaire. Les méthodes transcendantes conduisent à des résultats effectifs.

Soit $(\xi_n)$ une s.r.l. donnée par

$$\xi_n = P_1(n)\,\omega_1^n + \ldots + P_k(n)\,\omega_k^n \quad \text{pour} \quad n \geqslant 0 , \quad \omega_1, \ldots, \omega_k \in \mathbf{C} \text{ distincts} .$$

On peut supposer $|\omega_1| \geqslant |\omega_2| \geqslant \ldots \geqslant |\omega_k|$. Lorsque $|\omega_1| > |\omega_2|$ on a trivialement

$$|\xi_n| \sim |P_1(n)|\,|\omega_1|^n$$

donc $|\xi_n| \geqslant \frac{1}{2} P_1(n)\,|\omega_1|^n$ pour $n \geqslant n_0$ (effectif).

Minorer $|\xi_n|$ n'est plus aussi facile lorsque $\omega_1$ et $\omega_2$ sont de même module. Considérons en effet le cas le plus simple où $(\xi_n)$ est réelle et donnée par $\xi_n = \omega_1^n + \omega_2^n$.