Collect. Math. **38** (1987), 37–55

DIVISEURS PREMIERS DE SUITES RÉCURRENTES NON LINÉAIRES

Jean-Paul Bezivin

ABSTRACT. Let P be a polynomial with rational integer coefficients, and $u(n)$, $n \in \mathbb{N}$, a linear recurrent sequence of rational integers. Define a sequence $a(n)$ of rational integers by its first term and the (non-linear in general) recurrence formula $a(n+1) = P(a(n)) + u(n)$.

We say that the non zero rational integer m is a divisor of the sequence $a(n)$ if m divides some non-zero term of the sequence.

In this paper, we characterize the sequences $a(n)$ with only a finite number of prime divisors.

I. Introduction

Soit $u(n)$ une suite récurrente linéaire d'éléments de $\mathbb{Q}$, c'est-à-dire une suite $u(n)$ vérifiant une relation de récurrence du type

$$u(n+s) + a_{s-1}\,u(n+s-1) + \ldots + a_0\,u(n) = 0, \qquad n \in \mathbb{N}. \tag{1}$$

Les a_i, $i = 0, 1, \ldots, s-1$, étant des éléments fixés de $\mathbb{Q}$.

Soit P un polynôme non nul de $\mathbb{Q}[x]$, et b un élément de $\mathbb{Z}$ fixé.

On se donne une suite $a(n)$ d'éléments de $\mathbb{Z}$, vérifiant les conditions suivantes:

$$\text{i) } a(0) = b \qquad \text{ii) } a(n+1) = P(a(n)) + u(n), \qquad n \in \mathbb{N}. \tag{2}$$

Soit m un entier rationnel non nul, on dira que m est un diviseur de la suite $a(n)$, si m divise un élément non nul de la suite $a(n)$.

Le problème que nous voulons étudier dans cet article est celui de caractériser les suites $a(n)$ vérifiant (2), qui ne possèdent qu'un nombre fini de diviseurs premiers.

A la connaissance de l'auteur, il n'y a que peu d'articles étudiant les diviseurs premiers d'une suite vérifiant une récurrence non linéaire du type (2); le problème correspondant, dans le cas d'une suite récurrente linéaire a été résolu par G. Polya, en 1921 (voir plus loin).

On peut cependant citer deux articles de R. W. K. Odoni. Dans le premier de ces articles, [6], cet auteur étudie l'ensemble $\mathcal{P}$ des diviseurs premiers de la suite $W(n)$ vérifiant:

$$W(1) = 2 \quad \text{et} \quad W(n+1) = W(n)^2 - W(n) + 1.$$

Il démontre le résultat suivant:

Théorème 1. *On a*

$$\text{card}[\mathcal{P} \cap [1, x]] = O\left(x(\log(x)^{-1})(\log\log\log(x))^{-1}\right)$$

quand x tend vers $+\infty$.

Autrement dit, la densité de l'ensemble des diviseurs premiers de la suite $W(n)$ est nulle.

Dans le second article, [5], R. W. K. Odoni généralise le théorème 1 sous la forme suivante:

Théorème 2. *Pour presque tout polynôme unitaire P de $\mathbb{Z}[X]$, de degré supérieur ou égal à deux, les diviseurs premiers de la suite $a(n+1) = P(a(n))$ forment un ensemble de densité nulle, pour tout choix de $a(0) \neq 0$ dans $\mathbb{Z}$.*

Nous allons démontrer dans cet article que, sauf cas très exceptionnel, une suite vérifiant $a(n+1) = P(a(n)) + u(n)$ a une infinité de diviseurs premiers.

II. Formulation des résultats

Notons tout d'abord que si le polynôme P est constant ou de degré 1, la suite $a(n)$ est une suite récurrente linéaire à partir d'un certain rang.

Dans ce cas particulier, le problème posé est résolu par un théorème de G. Polya:

Théorème 3. (G. Polya, [7]) *Soit $a(n)$ une suite récurrente linéaire d'éléments de $\mathbb{Z}$. On suppose que l'ensemble des diviseurs premiers des éléments non nuls de la suite*

$a(n)$ est un ensemble fini. Il existe alors un entier T, non nul, et des rationnels c_r, b_r, $r = 0, 1, \ldots, T-1$, tels que l'on ait pour tout $r = 0, 1, \ldots, T-1$, et tout k dans $\mathbf{N}$ la relation

$$a(kT + r) = c_r \ (b_r)^k. \tag{3}$$

Il est clair que toute suite vérifiant (3) a un ensemble fini de diviseurs premiers.

Nous supposerons désormais que le polynôme P est de degré supérieur ou égal à deux.

Il nous sera nécessaire, pour nos démonstrations, de faire des hypothèses restrictives sur la suite récurrente $u(n)$.

On sait qu'une telle suite peut se représenter sous la forme

$$u(n) = \sum_{i=1}^{m} Q_i(n)\, b_i^n, \qquad n \in \mathbf{N}. \tag{4}$$

Dans cette expression, les b_i, $i = 1, \ldots, m$, sont des éléments non nuls d'une clôture algébrique $\bar{\mathbf{Q}}$ de $\mathbf{Q}$, et les Q_i des polynômes non nuls de $\bar{\mathbf{Q}}[X]$. Nous dirons que les b_i, $i = 1, \ldots, m$, sont les fréquences de la suite récurrente linéaire $u(n)$.

Dans toute la suite, nous ferons les hypothèses suivantes sur la suite $u = u(n)$:

(H) *Si la suite $u = u(n)$ n'est pas constante, alors les polynômes Q_i, $i = 1, \ldots, m$, sont constants, et la fréquence b_1 est dominante, c'est-à-dire que l'on a $|b_1| > 1$ et, pour tout $i = 2, \ldots, m$, $|b_1| > |b_i|$.*

Sous ces hypothèses, nous allons démontrer les résultats suivants:

Théorème 4. *La suite $a(n)$, $n \in \mathbf{N}$, n'a qu'un nombre fini de diviseurs premiers que dans les deux cas suivants:*

a) *Le polynôme $P(X)$ est un monôme, et la suite $u(n)$ est nulle.*

b) *La suite $a(n)$ est une suite récurrente linéaire à partir d'un certain rang (et est alors de la forme (3) du théorème 3, à partir d'un certain rang).*

Dans les résultats qui nous serviront à démontrer le théorème 4 se trouvent les propositions suivantes, qui nous semblent avoir leur intérêt popre:

Proposition 1. *Soit $u(n)$ une suite récurrente linéaire d'éléments de $\mathbf{Z}$. On suppose que $u(n)$ n'est pas constante, et vérifie l'hypothèse* (H). *Soit t un entier naturel supérieur ou égal à deux, et $a(n)$, $b(n)$, deux suites d'entiers. On suppose que:*

(i) *$a(n)^t + b(n) = u(n)$ pour tout n dans $\mathbf{N}$.*

(ii) *On a*

$$b(n) = O\left(|b_1|^{(t-2)n/t}\right)$$

si n tend vers l'infini (b_1 est la fréquence dominante de la suite $u(n)$).

Dans ces conditions, il existe une suite $d(n)$, ne prenant que les valeurs ± 1, telle que la suite $d(n)\,a(n)$ soit récurrente linéaire à partir d'un certain rang et la suite $b(n)$ est elle-même récurrente linéaire à partir d'un certain rang.

REMARQUE 1. On notera que dire qu'une suite $v(n)$ est récurrente linéaire à partir d'un certain rang est équivalent à dire que la série formelle $\sum v(n)\,x^n$ représente une fraction rationnelle.

REMARQUE 2. La proposition 1 est une légère amélioration d'un résultat de C. Pisot (voir [2]). On trouvera dans [9] des résultats plus récents sur cette question.

Proposition 2. *On suppose que la suite récurrente linéaire $u(n)$ est non constante et vérifie* (H). *Soit s un entier, et P un polynôme à $s+1$ variables, à coefficients dans $\mathbb{Q}$. On suppose que $P(X_0, \ldots, X_s)$ est de la forme:*

$$P(X_0, \ldots, X_s) = X_0^t + Q(X_0, \ldots, X_s), \tag{5}$$

le nombre entier t étant supérieur ou égal à deux, et le polynôme Q de degré total inférieur ou égal à $t-2$. Soit $a(n)$ une suite d'éléments de $\mathbb{Z}$ vérifiant:

$$P(a(n), \ldots, a(n+s)) = u(n) \qquad \text{pour tout } n \text{ dans } \mathbb{Z}.$$

On suppose que la série formelle $\sum a(n)\,x^n$ a un rayon de convergence non nul dans $\mathbb{C}$.

Alors il existe une suite $d(n)$ ne prenant que les valeurs ± 1, telle que la série $\sum a(n)\,x^n$ soit une fraction rationnelle.

REMARQUE 3. Bien entendu, dans certains cas, on peut améliorer le résultat de la proposition 2. Tout d'abord, il résulte de la démonstration de la proposition 1 que si t est un entier impair, on peut prendre $d(n)$ égal à un pour tout n. Dans ce cas, la série $\sum a(n)\,x^n$ est donc rationnelle.

Quand t est pair, l'exemple de $Q = 0$, montre que la présence du terme $d(n)$ est en général nécessaire; pour certains cas particuliers, comme celui de $a(n+1) = a(n)^4 + u(n)$, on déduit facilement de la proposition 2 que la suite $a(n)$ est récurrente linéaire à partir d'un certain rang.

REMARQUE 4. L'hypothèse faite sur le rayon de convergence de la série $\sum a(n)\,x^n$ est nécessaire, comme le montre l'exemple de $a(0) = 2$, $a(n+1) = a(n)^3 + 2^n + 3^n$, on vérifie aisément que $a(n) \geq 2^{2^n}$, donc la série $\sum a(n)\,x^n$ a un rayon de convergence nul.

REMARQUE 5. On notera enfin que la conjecture, due à C. Pisot, que le résultat de la proposition 1 est encore vrai si $a(n)^t = u(n)$, (i.e. $b(n) = 0$), sans hypothèses particulières sur la suite $u(n)$ (elle peut donc ne pas avoir de fréquence dominante unique), n'est toujours pas demontré (voir [9]).

III. Résultats préliminaires

Nous aurons besoin des résultats suivants:

Théorème 5. ([3], [10]) *Soit* $\mathbf{K}$ *un corps de caractéristique nulle, et* T *un sous-groupe de type fini du groupe multiplicatif de* $\mathbf{K}$. *Soit* s *un entier naturel non nul. Alors il existe seulement un nombre fini de points* $\underline{x} = (x_0, \ldots, x_s)$ *dans* $P_s(\mathbf{K})$, *tels que les trois propriétés suivantes soient vérifiées:*

a) pour tout i, $0 \leq i \leq s$, x_i *appartient à* T.

b) $x_0 + x_1 + \cdots + x_s = 0$.

c) Pour toute partie non vide et propre $(i_0, i_1, \ldots, i_t)$ *de* $\{0, 1, \ldots, s\}$, *on a* $x_{i_0} + \cdots + x_{i_t}$ *non nul.*

Théorème 6. (Critère de rationalité de Borel, voir [1], p. 170). *Soit*

$$f(x) = \sum_{n \geq 0} a(n)\,x^n$$

une série formelle de $\mathbb{Z}[[x]]$. *On suppose que le rayon de méromorphie de* f *est strictement supérieur à un. Alors* f *est le développement de Taylor à l'origine d'une fraction rationnelle.*

Théorème 7. *On suppose que les séries formelles* $\sum c(h)\,x^h$ *et* $\sum b(h)\,x^h$ *appartenant à* $\mathbb{C}[[x]]$ *sont les développements de Taylor à l'origine de fractions rationnelles, avec* $b(h) \neq 0$ *pour tout* h *assez grand. Si les quotients*

$$\frac{c(h)}{b(h)} = a(h)$$

(définis pour tout h assez grand) appartiennent à un anneau A de type fini sur $\mathbb{Z}$ pour tout h assez grand, alors $\sum a(h)\,x^h$ est le développement de Taylor d'une fraction rationnelle.

Ce résultat avait été conjecturé par C. Pisot et a été démontré par A. J. Van der Poorten. Pour la démonstration, voir [11] et [8].

Théorème 8. *Soit $\sum a(n)\,x^n$ une série formelle à coefficients dans $\mathbb{C}$, représentant le développement de Taylor à l'origine d'une fraction rationnelle. Il existe alors un entier naturel T non nul, tel que l'on ait, pour tout $r = 0, \ldots, T-1$, l'alternative suivante*

i) la suite $a(kT+r)$ est nulle à partir d'un certain rang.

ii) la suite $a(kT+r)$ est non nulle à partir d'un certain rang.

Preuve. Ceci est le théorème de Skolem-Lech-Mahler, voir [4].

IV. Preuve des propositions 1 et 2

Preuve de la proposition 1.

Par hypothèse, on peut écrire

$$u(n) = c_1\,b_1^n + O((e_1\,|b_1|)^n),$$

le nombre réel e_1 appartenant à l'intervalle $]0,1[$, et c_1, b_1 appartenant à $\bar{\mathbb{Q}}$ (cf. l'hypothèse (H)).

D'autre part, on a

$$b(n) = O\left(|b_1|^{(t-2)\,n/t}\right) ;$$

on en conclut facilement que si t est un entier pair, c_1 et b_1 sont deux réels positifs. On écrit alors:

$$a(n)^t = u(n) - b(n) = c_1\,b_1^n\,\left[1 + c_1^{-1}b_1^{-n}(u(n) - c_1\,b_1^n) + c_1^{-1}b(n)\right].$$

Il existe alors une suite d'entiers $d(n)$, ne prenant que les valeurs ± 1, telle qu'on ait:

$$d(n)\,a(n) = c_1^{1/t}b_1^{n/t}\sqrt[t]{1 + c_1^{-1}b_1^{-n}(u(n) - c_1\,b_1^n) + c_1^{-1}b_1^{-n}b(n)} \tag{6}$$

où $c_1^{1/t}$ et $b_1^{1/t}$ désignent les racines réelles positives t–ième de c_1 et b_1 respectivement.

Dans le cas où t est impair, on peut prendre $d(n) = 1$ pour tout n, en prenant alors pour $c_1^{1/t}$ et $b_1^{1/t}$ les racines réelles t–ièmes de c_1 et b_1.

Soit h un entier, assez grand, que l'on choisira plus loin. On écrit le développement de $\sqrt[t]{1+x}$ en $x = 0$:

$$\sqrt[t]{1+x} = 1 + v_1 x + \cdots + v_h x^h + g(x) \tag{7}$$

avec, pour $|x|$ assez petit, l'inégalité

$$|g(x)| \leq c_2 |x|^{h+1},$$

c_2 étant une constante positive.

Posons

$$w(n) = c_1^{-1} b_1^{-n} (u(n) - c_1 b_1^n) + c_1^{-1} b_1^{-n} b(n).$$

On a

$$u(n) - c_1 b_1^n = O((e_1 |b_1|)^n)$$

avec $e_1 \in]0,1[$, et

$$b(n) = O\left(|b_1|^{(t-2)n/t}\right).$$

On en déduit donc que l'on a $|w(n)| \leq c_3 e_2^n$, $c_3 > 0$, e_2 appartenant à $]0,1[$. En particulier, $w(n)$ tend vers zéro si n tend vers l'infini. Par suite, on peut écrire, pour n assez grand:

$$d(n)\, a(n) = c_1^{1/t} b_1^{n/t} \left[1 + v_1 w(n) + \cdots + v_h w(n)^h\right] + c_1^{1/t} b_1^{1/t} g(w(n)). \tag{8}$$

Nous allons regarder de plus près chacun des termes de la formule (8).

On commence par $c_1^{1/t} b_1^{1/t} g(w(n))$. Ce terme est majoré en valeur absolue par une expression de la forme:

$$\left|c_1^{1/t} b_1^{1/t} g(w(n))\right| \leq c_4 |b_1|^{n/t} |w(n)|^{k+1} \leq c_4 c_3^{h+1} \left[|b_1|^{1/t} e_1^{h+1}\right]^n.$$

Nous choisissons h de façon que la quantité $|b_1|^{1/t} e_1^{h+1}$ soit strictement inférieure à un.

Ce choix de h étant fait, on regarde maintenant un terme de la forme:

$$v_i\, c_1^{1/t} b_1^{n/t} (w(n))^i.$$

Cette expression est combinaison linéaire de termes de la forme:

$$b_1^{n/t} b_1^{-nl} (u(n) - c_1 b_1^n)^l\, b_1^{-kn} (b(n))^k. \tag{9}$$

L'expression (9) est majorée par

$$c_6 |b_1|^{n/t} |b_1|^{-nl} e_1^{nl} |b_1|^{-kn} |b_1|^{(t-2)\,k/t},$$

ou encore:

$$c_6 e_1^{nl} |b_1|^{(1-2k)n/t}.$$

On voit donc que, dès que k est non nul, l'expression (9) est majorée par une expression de la forme $c e^n$ avec c positif et e appartenant à $]0,1[$.

Soit e_4 le maximum de ces quantités e et de

$$e_3 = |b_1|^{1/t} e_2^{h+1}.$$

On peut alors écrire:

$$v_i c_1^{1/t} b_1^{n/t} (w(n))^i = v_i c_1^{1/t} b_1^{n/t} c_1^{-i} b_1^{-ni} (u(n) - c_1 b_1^n)^i + O(e_4^n)$$

pour $i = 1, \ldots, h$.

On a donc:

$$d(n)\, a(n) = R(n) + O(e_4^n) = R(n) + J(n), \tag{10}$$

formule dans laquelle $R(n)$ est la suite récurrente linéaire

$$R(n) = 1 + \sum_{i=1}^{h} v_i c_1^{1/t} b_1^{n/t} c_1^{-i} b_1^{-ni} (u(n) - c_1 b_1^n)^i .$$

La série formelle $f(x) = \sum d(n)\, a(n)\, x^n$ est donc la somme de la fraction rationnelle $\sum R(n)\, x^n$, et de la série $\sum J(n)\, x^n$. Cette dernière est analytique dans le disque de centre l'origine, et de rayon $1/e_4$ de $\mathbb{C}$; le critère de Borel s'applique, et montre que f est une fraction rationnelle, ce qui démontre la proposition 1.

Preuve de la proposition 2.

Nous allons démontrer que, en posant $b(n) = Q(a(n), \ldots, a(n+s))$, on peut appliquer la proposition 1.

Par hypothèse, la série formelle $\sum a(n)\, x^n$ a un rayon de convergence non nul.

Soit R ce rayon de convergence. Si R est strictement supérieur à un, la série $\sum a(n)\, x^n$ est un polynôme, et il n'y a rien à démontrer.

Nous supposons donc $R \leq 1$ dans la suite.

Soit ϵ un réel strictement positif. Il existe un réel c_5 positif, tel que l'on ait pour tout entier n l'inégalité

$$|a(n)| \leq c_5 \left(R^{-1} + \epsilon\right)^n, \qquad n \in \mathbf{N}.$$

D'après l'hypothèse faite sur le degré de $Q(X_0, \ldots, X_s)$, on voit qu'il existe c_6 constante positive telle que

$$|b(n)| = |Q(a(n), \ldots, a(n+s))| \leq c_6 \left(R^{-1} + \epsilon\right)^{(t-2)n}, \qquad n \in \mathbf{N}.$$

Il existe d'autre part, vu l'hypothèse (H), une constante c_7 positive telle que

$$|u(n)| \leq c_7 |b_1|^n, \qquad n \in \mathbf{N}.$$

Finalement, on obtient l'inégalité:

$$|a(n)|^t \leq c_6 \left(R^{-1} + \epsilon\right)^{(t-2)n} + c_7 |b_1|^n \leq c_8 (c_9)^n \qquad n \in \mathbf{N} \tag{11}$$

avec

$$c_9 = \max\left(\left(R^{-1} + \epsilon\right)^{t-2}, |b_1|\right).$$

Par conséquent:

$$R^{-t} \leq c_9 = \max\left(\left(R^{-1} + \epsilon\right)^{t-2}, |b_1|\right). \tag{12}$$

En faisant tendre ϵ vers zéro dans (12), on obtient

$$R^{-t} \leq \max\left(R^{-(t-2)}, |b_1|\right);$$

en tenant compte de $R \leq 1$, on obtient $R^{-1} \leq |b_1|^{1/t}$; il en résulte que $\left(R^{-1}\right)^{t-2} < |b_1|$. On choisit alors ϵ dans (12) de façon que l'on ait encore $\left(R^{-1} + \epsilon\right)^{t-2} < |b_1|$; la formule (11) montre alors que

$$|a(n)| \leq c_{10} |b_1|^{n/t}, \qquad n \in \mathbf{N}, \qquad c_{10} \text{ constante positive.}$$

En reportant cette majoration dans l'expression de $b(n) = Q(a(n), \ldots, a(n+s))$, on voit que l'on a:

$$|b(n)| \leq c_{11} |b_1|^{(t-2)n/t}, \qquad n \in \mathbf{N}, \qquad c_{11} \text{ constante positive.}$$

Cette dernière relation permet d'appliquer la proposition 1, et démontre le résultat.

V. Preuve du théorème 4

Notons tout d'abord que quitte à modifier légèrement la suite récurrente $u(n)$, on peut supposer que le polynôme P n'a pas de terme constant.

Nous allons considérer séparément les trois cas suivants:

A) la suite u est constante.

B) la suite u est non constante, et le degré de P est au moins trois.

C) la suite u est non constante, et le degré de P est égal à deux.

A) Etude du cas où la suite $u(n)$ est constante.

Soit S l'ensemble fini formé des nombres premiers qui divisent un terme non nul de la suite $a(n)$, et T le sous-groupe multiplicatif du groupe multiplicatif de $\mathbf{Q}$, engendré par ± 1, les éléments de S, et les coefficients non nuls du polynôme P, ainsi que la valeur constante de la suite u. Il est clair que T est un groupe de type fini.

On écrit:

$$P(X) = c_s X^s + \cdots + c_1 X, \qquad u(n) = c_0, \qquad n \in \mathbf{N}.$$

On a donc l'égalité suivante:

$$a(n+1) - c_s\, a(n)^s + \cdots + c_1\, a(n) - c_0 = 0, \qquad n \in \mathbf{N}. \tag{13}$$

Si l'on note

$$x_0(n) = a(n+1), \quad x_1(n) = -c_s\, a(n)^s, \quad \ldots \quad , x_s(n) = -c_0,$$

on voit donc que les hypothèses du théorème 4, à l'exception du c) et du fait que les $x_i(n)$ peuvent être nuls, sont satisfaites.

On voit facilement que, pour tout indice n, tel que $a(n+1)$ soit non nul, on peut trouver une partie I de $\{0, 1, \ldots, s\}$, contenant 0, et telle que:

i) $\sum_{i \in I} x_i(n) = 0$.

ii) pour toute partie propre J de I on a $\sum_{i \in J} x_i(n) \neq 0$.

Comme l'ensemble de telles parties I est fini, on déduit du théorème 5 qu'il existe un ensemble A fini, d'éléments de $\bar{\mathbf{Q}}$, tel que, pour tout entier n on a l'alternative suivante:

i) $a(n+1) = 0$.

ii) $a(n+1) = w(a(n))^l$, w appartenant à A, et l à $\{0, 1, \ldots, s\}$.

Nous supposons d'abord que l'ensemble des valeurs prises par la suite $a(n)$ est infini. Les indices n tels que $a(n+1)$ soit nul sont tels que $P(a(n)) + c_0 = 0$; il n'y a donc qu'un nombre fini de valeurs $a(n)$ correspondantes.

Il existe donc un couple w, l tel que, pour une partie infinie de l'ensemble des $a(n)$, on ait l'égalité $a(n+1) = w(a(n))^l$.

Par suite, $w(a(n))^l - P(a(n)) - c_0 = 0$ pour ces valeurs. On a donc $P(X) + c_0 = w X^l$, ce qui correspond au cas a) du théorème 4.

On suppose maintenant que l'ensemble des valeurs $a(n)$ est fini.

Il existe alors un couple N, K d'entiers, avec K non nul, et $a(N+K) = a(N)$. On voit alors facilement que, pour tout entier n dans $\mathbf{N}$, n supérieur ou égal à N, on a $a(n+K) = a(n)$.

La série $\sum a(n)\, x^n$ est donc une fraction rationnelle, c'est le cas b) du théorème 4.

B) Nous supposerons maintenant la suite u non constante (elle a donc une fréquence dominante b_1), et le degré du polynôme P supérieur ou égal à trois.

La suite $u(n)$ a une expression de la forme

$$a(n) = d_1\, b_1^n + \cdots + d_m\, b_m^n,$$

d_1 et b_1 étant réels, avec $|b_1| > 1$ et $|b_1| > |b_i|$, $i = 2, \ldots, m$.

On a donc la relation:

$$a(n+1) - c_s\, a(n)^s - \cdots - c_1\, a(n) - d_1\, b_1^n - \cdots - d_m\, b_m^n \tag{14}$$

pour tout n dans $\mathbf{N}$.

On applique alors le théorème 5 comme on l'a vu précédemment, pour démontrer qu'il existe une partie finie A dans $\bar{\mathbf{Q}}$, telle que pour tout entier n, on ait l'une des relations suivantes:

a) $a(n+1) = 0$.

b) $a(n+1) = W\, a(n)^l$, W appartenant à A, l à $\{1, 2, \ldots, s\}$.

c) $a(n+1) = W\, d_i\, b_i^n$, W appartenant à A, i à $\{1, 2, \ldots, m\}$.

Dans le cas a), on a $P(a(n)) = -u(n)$.

Dans le cas b), on a $W\,a(n)^l - P(a(n)) = u(n)$.

Il en résulte, puisque la suite $|u(n)|$ tend vers $+\infty$ quand n tend vers $+\infty$, que le polynôme $W\,X^l - P(X)$ est non constant, sauf si l'ensemble des indices n tels que $a(n+1) = W(a(n))^l$ est un ensemble fini.

Dans le cas c), on a $P(a(n)) = -u(n) - W\,d_i\,b_i^n$.

Finalement, on voit qu'il existe une famille F_1 de polynômes non constants, et une famille F_2 de suites récurrentes linéaires, telles que, pour tout n assez grand, on ait

$$Q(a(n)) = S(n),$$

où le polynôme Q appartient à F_1 et la suite récurrente linéaire $S(n)$ à F_2.

On en déduit qu'il existe deux constantes c_{12} et c_{13} telles que l'on ait:

$$|a(n)| \leq c_{12}\,(c_{13})^n, \tag{15}$$

n appartenant à $\mathbf{N}$.

En considérant une suite $a(n) = d_2(\tilde{a}(n) + d_1)$, avec d_1 appartenant à $\mathbf{Q}$, et d_2 à $\mathbf{N}$, on peut supposer que le polynôme P n'a pas de terme en X^{s-1}, et que $\tilde{a}(n)$ soit à valeurs dans $\mathbf{Z}$.

Puisque s =degré de P est supérieur ou égal à trois, la proposition 2 s'applique alors, et montre qu'il existe une suite $d(n)$, ne prenant que les valeurs ± 1, et telle que $d(n)\,\tilde{a}(n)$ soit récurrente linéaire à partir d'un certain rang.

Si l'entier s est impair, on peut prendre $d(n) = 1$ pour tout n; par suite, $\tilde{a}(n)$ est récurrente à partir d'un certain rang, donc aussi $a(n)$.

Il suffit, dans le cas où s est un entier pair, de démontrer que la suite $d(n)$ est une suite récurrente linéaire à partir d'un certain rang (elle sera donc périodique) pour pouvoir conclure.

Ceci résultera du lemme suivant:

Lemme. *Soit P un polynôme de $\mathbf{Q}[X]$, de degré supérieur ou égal à deux, et $u(n)$ une suite récurrente linéaire d'éléments de $\mathbf{Z}$, ayant une fréquence dominante, et $a(n)$ une suite d'entiers telle que l'on ait*

$$a(n+1) = P(a(n)) + u(n)$$

pour tout n.

On suppose qu'il existe une suite d'entiers $d(n)$, ne prenant que les valeurs ± 1, et une suite récurrente linéaire $v(n)$, ayant une fréquence dominante, telle que $a(n) = d(n)\,v(n)$ pour tout entier n assez grand.

Alors $a(n)$ est une suite récurrente linéaire pour n assez grand.

Preuve. On peut écrire:

$$P(X) = c_s\,X^s + \cdots + c_1\,X,$$

d'où on déduit

$$P(a(n)) = V_1(n) + d(n)\,V_2(n),$$

avec

$$V_1(n) = \sum_{i \text{ pair}} c_i\,(v(n))^i \quad \text{et} \quad V_2(n) = \sum_{i \text{ impair}} c_i\,(v(n))^i.$$

Ces deux suites $V_1(n)$ et $V_2(n)$ sont récurrentes linéaires, et l'on a

$$a(n+1) = V_1(n) + u(n) + d(n)\,V_2(n). \tag{16}$$

Si la suite V_2 est la suite nulle, on a donc démontré que la suite $a(n+1)$, (et donc $a(n)$) est récurrente linéaire à partir d'un certain rang.

Si la suite $V_2(n)$ n'est pas nulle, il résulte de son expression qu'elle a, comme $v(n)$, une fréquence dominante.

D'autre part, la suite $v(n+1)/V_2(n)$ tend vers une limite finie, éventuellement nulle.

On déduit de (16) la relation, pour n assez grand:

$$d(n) = \frac{a(n+1)}{V_2(n)} - \frac{V_1(n)+u(n)}{V_2(n)} = d(n+1)\,\frac{v(n+1)}{V_2(n)} - \frac{V_1(n)+u(n)}{V_2(n)}\,. \tag{17}$$

En faisant apparaître la racine dominante de $V_2(n)$, et en écrivant

$$V_2(n) = \tilde{c}_1\,\tilde{b}_1^n\,(1 + O(\theta_1^n))$$

avec θ_1 appartenant à $]0,1[$ on montre facilement que l'on peut écrire alors:

$$-\frac{V_1(n)+u(n)}{V_2(n)} = R_1(n) + O(\theta_2^n)$$

pour θ_2 appartenant à $]0,1[$.

Soit w la limite de $v(n+1)/V_2(n)$. On a donc:

$$w\,d(n+1) - d(n) = R_1(n) + o(1), \tag{18}$$

$R_1(n)$ étant une suite récurrente linéaire.

Il existe donc des w_i, $i = 0, 1, \ldots, q$, tels que l'on ait la relation:

$$\sum_{i=0}^{q} w_i\, d(n+i) = o(1)$$

(les w_i n'étant pas tous nuls).

Mais la suite $\sum_{i=0}^{q} w_i\, d(n+i)$ prend un nombre fini de valeurs; comme elle tend vers zéro quand n tend vers l'infini, elle est nulle à partir d'un certain rang. Par conséquent, la suite $d(n)$ est une suite récurrente linéaire, ce qui démontre le lemme.

L'application du lemme au cas de la suite $d(n)\,\tilde{a}(n)$ est immédiate, puisqu'il résulte de la démonstration de la proposition 1 que cette suite récurrente linéaire a une fréquence dominante, et ceci termine la démonstration du cas B) du théorème 4.

C) Nous passons maintenant au cas de $s = 2$, u étant une suite non constante.

On peut donc écrire

$$a(n+1) = \tilde{c}_1\, a(n)^2 + \tilde{c}_1\, a(n) + u(n)$$

ou encore:

$$a(n)^2 = v(n) + c'_1\, a(n) + c'_2\, a(n+1)$$

avec c'_2 non nul.

En procédant comme dans la démonstration de la proposition 1, on voit facilement que l'on peut écrire, avec $d(n)$ appartenant à ± 1 pour tout entier n:

$$d(n)\,a(n) = R_2(n) + \frac{c'_1\, a(n) + c'_2\, a(n+1)}{2\sqrt{c_1}\,\left(\sqrt{b_1}\right)^n} + O\left(e_5^n\right) \tag{19}$$

avec e_5 appartenant à $]0,1[$.

(Il s'est donc introduit le terme

$$\frac{c'_1\, a(n) + c'_2\, a(n+1)}{2\sqrt{c'_1}\,\left(\sqrt{b_1}\right)^n}$$

en plus).

On a de plus

$$R_2(n) = \sqrt{c'_1}\ \left(\sqrt{b_1}\right)^n + O\left(\left(e_6\sqrt{b'_1}\right)^n\right)$$

avec e_6 appartenant à]0,1[.

On tire facilement de (19) la formule suivante:

$$d(n)\,a(n) = R_2(n) + \frac{c'_1}{2}\,d(n) + \frac{c'_2}{2}\,\sqrt{b_1}\,d(n+1) + O(e_7^n) \tag{20}$$

avec e_7 appartenant à]0,1[.

La suite $R_2(n)$ est une suite récurrente linéaire d'éléments de $\bar{\mathbf{Q}}$. Il existe donc des éléments t_i dans $\mathbf{Z}$, non tous nuls, tels que l'on ait pour tout n assez grand la relation:

$$\sum_{i=0}^{m} t_i\,R_2(n+i) = 0.$$

On en déduit que

$$\sum_{i=0}^{m} t_i\,d(n+i)\,a(n+i) = \frac{c'_2}{2}\sum_{i=0}^{m} t_i\,d(n+i) + \frac{c'_2}{2}\,\sqrt{b_1}\sum_{i=0}^{m} t_i\,d(n+i+1) + O\left(e_7^n\right).$$

Il existe un entier l dans $\mathbf{N}^*$ tel que $lc'_1/2$ et $lc'_2/2$ soient tous les deux dans $\mathbf{Z}$.

Posons

$$h(n) = l\left(\sum_{i=0}^{m} t_i\,d(n+i)\ a(n+i)\right) - l\,\frac{c'_1}{2}\sum_{i=0}^{m} t_i\,d(n+i)$$

et

$$c(n) = \frac{l\,c'_2}{2}\sum_{i=0}^{m} t_i\,d(n+i+1).$$

On a alors: $h(n)$ appartient à $\mathbf{Z}$ pour tout n, ainsi que $c(n)$, et:

$$h(n) = \sqrt{b_1}\,c(n) + O\left(e_7^n\right).$$

Comme $d(n)$ appartient à ± 1 pour tout entier n, la suite $c(n)$ prend un nombre fini de valeurs.

Nous allons distinguer plusieurs cas.

Tout d'abord, si la suite $c(n)$ est nulle à partir d'un certain rang, on a la relation $\sum t_i\, d(n+i+1) = 0$ pour n assez grand; ceci prouve que $d(n)$ est une suite récurrente linéaire; d'après l'égalité:

$$a(n) = d(n)\, R(n) + \frac{c'_1}{2} + \frac{c'_2}{2}\, \sqrt{b_1}\, d(n)\, d(n+1) + O\,(e_7^n)\,,$$

et le théorème de Borel, la suite $a(n)$ est une suite récurrente linéaire à partir d'un certain rang, d'où le résultat.

S'il existe maintenant une infinité de valeurs n telles que $c(n) = c$ non nul, on a pour ces valeurs $h(n) = \sqrt{b_1}\, c + O(e_7^n)$; tenant compte du fait que $h(n)$ est élément de $\mathbb{Z}$ pour tout n, on voit que ceci implique que $\sqrt{b_1}$ est élément de $\mathbb{Q}$.

On peut alors choisir l de façon que $\sqrt{b_1}\, c(n)$ soit à valeurs entières; le théorème de Borel nous indique alors que la suite

$$d(n)\, a(n) - \frac{c'_1}{2}\, d(n) - \frac{c'_2}{2}\, \sqrt{b_1}\, d(n+1)$$

est récurrente linéaire à partir d'un certain rang.

On a donc:

$$d(n)\, a(n) = R_3(n) + e(n),$$

avec $R_3(n)$ suite récurrente linéaire et

$$e(n) = \frac{c'_1}{2}\, d(n) + \frac{c'_2}{2}\, \sqrt{b_1}\, d(n+1).$$

Nous reprenons avec cette expression pour $d(n)\, a(n)$ la formule de départ, à savoir

$$a(n)^2 = v(n) + c'_2\, a(n) + c'_2\, a(n+1).$$

Après quelques calculs, on trouve:

$$R_3^2(n) - v(n) - \frac{{c'_1}^2 + 2\, c'_2\, c'_1 - b_1\, {c'_2}^2}{4} =$$

$$c'_2\, d(n+1) \left(R_3(n+1) - \sqrt{b_1}\, R_3(n) + \frac{c'_3 \sqrt{b_1}}{2}\, d(n+2) \right).$$

Ou encore:

$$A(n) = d(n+1)\,(B(n) + p\, d(n+2)). \tag{21}$$

$A(n)$ et $B(n)$ étant deux suites récurrentes linéaires, et p la constante $c_2' \sqrt{b_1}/2$, qui est non nulle.

En élevant (21) au carré, et tenant compte de $d(n+1) = \pm 1$, on a:

$$A(n)^2 = B(n)^2 + p^2 + 2p\,B(n)\,d(n+2). \tag{22}$$

Si la suite $B(n)$ est non nulle à partir d'un certain rang, on trouve que la suite $d(n+2)$ d'éléments de $\{\pm 1\}$, est quotient de deux suites récurrentes linéaires.

D'après le théorème 7, la suite $d(n+2)$ est donc une suite récurrente linéaire.

Il en est donc de même de la suite $a(n)$, ce qui termine la démonstration dans ce cas.

Si maintenant la suite $B(n)$ a une infinité de zéros entiers, le théorème 8 nous affirme qu'il existe un entier non nul d_0, tel que, pour tout r dans $\{0, 1, \ldots, d_0 - 1\}$, la suite $B(k\,d_0 + r)$ soit nulle à partir d'un certain rang, ou non nulle à partir d'un certain rang.

On suppose d'abord que la suite $B(n)$ n'est pas nulle à partir d'un certain rang.

Dans ce cas, il existe un r_0 dans $\{0, 1, \ldots, d_0 - 1\}$, tel que $B(k\,d_0 + r)$ soit non nul à partir d'un certain rang.

La formule (22) montre alors que la suite $d(k\,d_0 + r_0 + 2)$ est récurrente linéaire à partir d'un certain rang.

Nous allons démontrer par récurrence que, pour tout entier l dans $\mathbf{N}$, la suite $d(k\,d_0 + r_0 + l + 2)$ est récurrente linéaire pour k assez grand. C'est vrai pour $l = 0$. Si cette propriété est vrai pour $l - 1$, et si $B(k\,d_0 + r_0 + l)$ est non nul à partir d'un certain rang, la suite $d(k\,d_0 + r_0 + l + 2)$ est récurrente linéaire à partir d'un certain rang.

Si par contre $B(k\,d_0 + r_0 + l)$ est nulle à partir d'un certain rang, la formule (21) montre que la suite $d(k\,d_0 + r_0 + l + 1)\,d(k\,d_0 + r_0 + l + 2)$ est récurrente linéaire à partir d'un certain rang.

Par hypothèse de récurence, il en est de même de $d(k\,d_0 + r_0 + l + 1)$, donc aussi de $d(k\,d_0 + r_0 + l + 2)$.

Finalement, toutes les suites $d(k\,d_0 + r)$, $r \in \{0, 1, \ldots, d_0 - 1\}$ sont récurrentes linéaires à partir d'un certain rang, donc il en est de même de la suite $d(n)$.

Il ne nous reste qu'un seul cas à examiner: le cas où la suite $B(n)$ est nulle à partir dún certain rang.

La formule (22) donne alors que la suite $d(n+1)\,d(n+2)$ est récurrente linéaire à partir d'un certain rang, et à valeurs dans $\{\pm 1\}$.

Par suite, $d(n+1)\,d(n+2)$ est périodique; soit T une période, on a donc pour tout n assez grand

$$d(n+T+1)\,d(n+T+2) = d(n+1)\,d(n+2).$$

Donc:

$$\frac{d(n+T+2)}{d(n+2)} = \frac{d(n+1)}{d(n+T+1)} = \frac{d(n+T+1)}{d(n+1)}\,.$$

La suite $d(n+T+1)/d(n+1)$ est donc constante pour n assez grand; ceci prouve que $d(n)$ est une suite récurrente linéaire, et termine la démonstration.

Références

[1] Y. Amice, *Les nombres p–adiques*, Presses Universitaires de France, 1973.

[2] B. Benzaghou, Algèbres de Hadamard, *Bull. Soc. Math. France* **98** (1970), 209–252.

[3] J. H. Evertse, On sums of S–units and linear recurrences, *Compositio Math.* **52** (1984), 225–245.

[4] K. Mahler, On the Taylor coefficients of rational functions, *Proc. Camb. Phil. Soc.* **52** (1956), 39–48.

[5] R. K. W. Odoni, The Galois theory of iterates and composite polynomials, *Proc. London Math. Soc.* (3) **51** (1985), 385–414.

[6] R. K. W. Odoni, On the prime divisors of the sequence $w_{n+1} = 1 + w_1 \cdots w_n$, *J. London Math. Soc.* (2) **32** (1985), 1–11.

[7] G. Polya, Arithmetische Eigenschaften der Reihenenwicklungen rationaler Funktionen, *J. Reine und Angew. Math.* **151** (1921), 1–31.

[8] R. Rumely, Notes on Van der Poorten's proof of the Hadamard quotient theorem, I and II, Preprint.

[9] R. Rumely and A. J. Van der Poorten, A note on the Hadamard k–th root of a rational function, Preprint.

[10] H. P. Schlickewei and A. J. Van der Poorten, The growth condition for recurrent sequences, Macquarie Math. reports 82–0041, Northride Australia, 1972.

[11] A. J. Van der Poorten, Hadamard operations on rational functions, Groupe d'étude ultramétrique 1982–1983, exposé 4.

Received 6/NOV/87

Jean-Paul Bezivin
Université Paris VI, Mathématiques
4, Place Jussieu 75252 Paris CEDEX
FRANCE