

JEAN-PAUL BÉZIVIN

**Sur les diviseurs premiers des suites
récurrentes linéaires**

Annales de la faculté des sciences de Toulouse 5^e série, tome 8, n^o 1
(1986-1987), p. 61-73

http://www.numdam.org/item?id=AFST_1986-1987_5_8_1_61_0

© Université Paul Sabatier, 1986-1987, tous droits réservés.

L'accès aux archives de la revue « Annales de la faculté des sciences de Toulouse » (<http://picard.ups-tlse.fr/~annales/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

Sur les diviseurs premiers des suites récurrentes linéaires

JEAN PAUL BÉZIVIN ⁽¹⁾

RÉSUMÉ. — Dans cet article, nous nous intéressons à des minoration du plus grand facteur premier des termes d'une suite récurrente linéaire $u(n) = \sum_{k=1}^s a_k (b_k)^n$, avec a_k et b_k éléments de \mathbf{Z} . Nous donnons aussi une minoration pour la fonction $\varphi : \varphi(x) = \text{card} \{p \text{ premier}, p \leq x, u(n) \neq 0 \text{ et } p|u(n)\}$ dans le cas de suites binaires, i.e. $s = 2$.

ABSTRACT. — In this paper, we prove lower bounds for the greatest prime divisor of terms of linear recurrent sequences of the form $u(n) = \sum_{k=1}^s a_k (b_k)^n$ with $a_k, b_k \in \mathbf{Z}$. We prove also a lower bound for the function $\varphi : \varphi(x) = \text{card} \{p \text{ prime}, p \leq x, p|u(n) \text{ and } u(n) \neq 0\}$ in the case of binary sequences, i.e. $s = 2$.

§ I. Introduction

Dans cet article, nous nous intéressons aux diviseurs premiers de suites récurrentes linéaires du type

$$u(n) = \sum_{k=1}^s a_k b_k^n$$

où s est un entier plus grand que un, et a_k et b_k des éléments non nuls de \mathbf{Z} . On suppose dès le départ que l'ensemble des b_i a pour plus grand commun diviseur le nombre 1, ainsi que l'ensemble des a_i .

Il résulte d'un théorème général de G.POLYA que, si l'on note A l'ensemble des diviseurs premiers de la suite $u = (u(n))$, c'est-à-dire : $A = \{p \text{ premier}$

(1) Université Pierre et Marie Curie, Mathématiques, Tour 45-46, 4, place Jussieu, 75252 Paris Cedex 05

| il existe $n \in \mathbf{N}$ tel que $u(n) \neq 0$ et $p|u(n)$, l'ensemble A est infini, sauf dans le cas particulier où les deux sous-suites $u(2n)$ et $u(2n+1)$ sont de la forme $c d^n$, c et d étant deux éléments de \mathbf{Z} (voir [13]).

Nous supposons dans toute la suite que les valeurs absolues des b_i sont toutes distinctes, de façon à éviter ces cas particuliers. Le théorème de G.POLYA cité plus haut peut se généraliser de plusieurs façons.

Notons, pour $x \in \mathbf{Z}$, $P(x)$ le plus grand facteur premier de x si x est différent de 0 et ± 1 , avec la convention $P(0) = P(\pm 1) = 1$. Le théorème de G.POLYA peut alors se traduire en disant que, sauf en des cas très particuliers, on a $\limsup P(u(n)) = +\infty$. Ce point de vue a été très étudié, en particulier ces dernières années.

Les résultats les plus récents sur le sujet, sont, à la connaissance de l'auteur des estimations de C.L.STEWART ([7]).

Dans le cas général d'une suite récurrente à valeurs dans \mathbf{Z} et d'ordre s , s entier supérieur ou égal à deux, C.L.STEWART démontre que l'on a l'estimation suivante :

Pour tout réel ϵ , strictement compris entre zéro et un, on a, pourvu que l'entier naturel n soit assez grand, la minoration

$$P(u(n)) \geq (1 - \epsilon) \log(n).$$

Il est cependant fait, pour obtenir ce résultat, l'hypothèse que le polynôme caractéristique de la suite récurrente $u = (u(n))$ possède une unique racine de module maximal.

Dans le cas d'une suite récurrente d'ordre deux, on a des estimations plus précises, puisque C.L.STEWART démontre que l'on a

$$P(u(n)) \geq c \left(\frac{n}{\log n} \right)^{1/(d+1)}$$

pourvu que n soit assez grand, c étant une constante strictement positive effectivement calculable, et d le degré sur \mathbf{Q} d'une racine du polynôme caractéristique de la récurrence.

Enfin, dans le cas d'une récurrence binaire, on a des résultats valables pour presque tout entier n ; on a en effet, pour une suite récurrente binaire non dégénérée, la minoration

$$P(u(n)) \geq \epsilon(n)n \log(n)$$

sauf peut-être pour un ensemble de valeurs de n de densité asymptotique nulle; dans cette formule, $\epsilon(n)$ est une suite quelconque de réels positifs de limite nulle à l'infini.

Les preuves de ces résultats utilisent une version, due à M. WALDSCHMIDT, du théorème de BAKER sur des minorations de formes linéaires en logarithmes. On pourra voir la référence [6] pour un exposé de synthèse très intéressant sur ces résultats.

Le deuxième point de vue est de préciser l'ensemble A des diviseurs de la suite $u = (u(n))$ par des minorations de la fonction du réel positif x définie par $\varphi(x) = \text{card}\{p \in A | p \leq x\}$. Il y a, contrairement au premier point de vue, très peu de résultats semble-t-il sur ce sujet.

Des résultats de densité sur l'ensemble A sont connus pour des suites récurrentes binaires très particulières, et sont dûs à H. HASSE et J. LAGARIAS, voir [1]. La preuve de ces résultats nécessite l'emploi du théorème de densité de TCHEBOTAREF. On a aussi des résultats de densité, pour des suites binaires de la forme $u(n) = a^n - b$, avec a et b dans \mathbf{N} , voir [5], la preuve nécessitant la validité de l'hypothèse de Riemann pour les fonctions dzéta de DEDEKIND de certains corps Kummériens.

Dans cet article, nous nous servons d'une technique inaugurée par I.E. SHPARLINSKII ([4]) pour démontrer deux résultats relatifs à chacun des points de vue que nous venons d'indiquer. On notera que notre méthode de démonstration est totalement élémentaire.

§ II. Énoncés des résultats

Nous allons démontrer les résultats suivants :

THÉORÈME 1. — *Soit $u = (u(n))$ une suite récurrente de la forme $u(n) = \sum_{k=1}^s a_k b_k^n$, où les a_k et b_k sont les éléments de \mathbf{Z} non nuls, les b_k étant de valeurs absolues distinctes, avec $u(n) \neq 0 \forall n \in \mathbf{N}$. Soit $\epsilon(n)$ une fonction strictement positive, de limite nulle à l'infini. Alors on a $P(u(n)) \geq \epsilon(n)n^{1/3}$, sauf peut-être pour un ensemble d'indices n de densité arithmétique nulle.*

THÉORÈME 2. — *Soit u une suite récurrente binaire de la forme $u(n) = a_1 b_1^n + a_2 b_2^n$; on suppose que cette suite vérifie les hypothèses du théorème 1. On note $A = \{p \text{ premier}, \exists n \in \mathbf{N} p | u(n)\}$, et $\varphi(x) = \text{card}\{p \in A, p \leq x\}$. On a alors la minoration $\varphi(x) \geq c_7 \left(\frac{\log x}{\log \log x}\right)^{1/2}$, $c_7 > 0$, pourvu que x soit assez grand.*

Notons tout d'abord que, vu les hypothèses faites sur la suite $u(n) = \sum_1^s a_k b_k^n$, cette suite n'a qu'un nombre fini de zéros; quitte à considérer une suite décalée de la suite $u(n)$, c'est-à-dire une suite $v(n) = u(n + n_o)$ pour un $n_o \in \mathbf{N}$, on peut supposer que $u(n)$ est non nul pour tout n dans \mathbf{N} . On remarquera d'ailleurs qu'il est facile de montrer que, si la suite $u(n)$ s'annule pour n_o appartenant à \mathbf{N} , l'ensemble A des diviseurs de u est l'ensemble des nombres premiers à un nombre fini d'exceptions près.

Comme indiqué dans l'introduction, nous utilisons des idées dues à I.E. SHPARLINSKII ([4]).

Pour ce qui est du théorème 1, le résultat démontré ici est une amélioration de ceux démontrés dans [4], pour les suites plus particulières que nous examinons.

En ce qui concerne le théorème 2, des résultats de ce type ne sont pas considérés dans l'article [4]. Cependant, le lemme 1 de [4] permet de démontrer, dans un cadre plus général que celui présenté ici, des estimations analogues à celles du théorème 2. Nous n'avons pas pu nous procurer la démonstration du lemme 1 de [4], ce qui explique que nous nous restreignons à un cadre assez étroit.

§ III. Preuve du théorème 1

PROPOSITION 1. — Soit $u(n) = \sum_1^s a_k b_k^n$ une suite vérifiant les hypothèses du théorème 1, et p un nombre premier. Soit $N \geq 1, M \geq 1$ deux entiers. On note $B(p, M, N)$ le cardinal de l'ensemble des indices $n, 0 \leq n \leq N$ tels que $u(n) \equiv 0[p^M]$. Il existe alors des constantes c_1, c_2, c_3, c_4 strictement positives telles que l'on ait pour tout (p, N, M) l'inégalité :

$$B(p, M, N) \leq c_1 \frac{pN}{M \log p} + c_2 \frac{p^2}{\log p} + c_3 \log(N) + c_4$$

Preuve. — La proposition 1 résultera de la série de lemmes qui suivent.

Le lemme 1 est un énoncé qui donne, pour un polynôme f de $\mathbf{Z}[X]$, et un élément a de \mathbf{Z} , une majoration du nombre d'entiers distincts, proches p -adiquement de a , et tels que la valeur de f en ces points soit p -adiquement petite. Nous l'utiliserons en interprétant les congruences $u(n) \equiv 0[p^M]$ comme des congruences portant sur les valeurs de polynômes à coefficients dans \mathbf{Z} , construits à partir de la suite $u = (u(n))$.

Pour p entier premier rationnel, nous notons v_p la valuation p -adique, i.e. si b est un élément non nul de \mathbf{Z} , tel que $b = p^c d$, avec c appartenant à \mathbf{N} , et d un élément de \mathbf{Z} premier à p , on pose $v_p(b) = c$; par convention on a $v_p(0)$ égal à l'infini.

LEMME 1. — Soit p un nombre premier, f un polynôme de $\mathbf{Z}[X]$ non nul. Soient $M \geq 1$, $a \in \mathbf{Z}$ donnés, ainsi que K entiers distincts n_1, \dots, n_K . On suppose que :

- (i) $a \equiv n_i[p] \quad i = 1, 2, \dots, K$
- (ii) $f(n_j) \equiv O[p^M]$ pour $j = 1, 2, \dots, K$

On note

$$L = \max_k v_p \left(\prod_{j \neq k} (n_j - n_k) \right).$$

On a alors l'inégalité suivante :

$$v_p(f(a)) \geq \min(K, K - L + M - 1).$$

Preuve. — Ceci est le lemme 1 de [2], auquel nous renvoyons le lecteur.

LEMME 2. — Soit $u(n) = \sum_1^s a_k b_k^n$ une suite récurrente linéaire vérifiant les hypothèses du théorème 1, et p un entier premier tel que pour tous les b_k soient des unités p -adiques. Soient T, S, M trois entiers naturels avec S et M non nuls. On note E l'ensemble des entiers m tels que, avec $q = p - 1$ si p est impair, $q = 2$ si $p = 2$:

- a) $u(qm) = O[p^M]$
- b) $T + 1 \leq m \leq T + S$

Alors, si K est le cardinal de E , on a l'inégalité

$$v_p(u(0)) \geq \min \left(K, M - \frac{S - 1}{p - 1} \right).$$

Preuve. — Nous suivons le schéma de démonstration du lemme 2 de [2]. On suppose tout d'abord que p est impair.

Soit g une racine primitive modulo p^2 , de sorte que g est une racine primitive modulo p^k pour tout k . On définit les entiers c_k par $b_k \equiv g^{c_k} [p^{M'}], M' \geq M$. Soit $v(z) = \sum_1^s a_k g^{c_k z}$. On a clairement, pour tout

z dans \mathbb{N} , $u(z) \equiv v(z)[p^{M'}]$. En particulier, $u(0) \equiv v(0)[p^{M'}]$, de sorte que, si l'on a pris M' suffisamment grand, on a $v_p(u(0)) = v_p(v(0))$. (On rappelle que $u(0)$ est non nul).

Soit alors f le polynôme défini par $f(x) = \sum_1^s a_k X^{c_k}$. On va appliquer le lemme 1 avec $a = 1$, et n_1, \dots, n_k les éléments $g^{(p-1)m}$ avec m appartenant à E . Il nous faut trouver une majoration de

$$\max_{m \in E} v_p \left(\prod_{\substack{r \in E \\ r \neq m}} (g^{(p-1)r} - g^{(p-1)m}) \right).$$

On a $v_p(g^{(p-1)m} - g^{(p-1)r}) = 1 + v_p(r - m)$.

Le produit $\prod_{r \neq m} (r - m)$ est un diviseur de $(m - T - 1)! (T + S - m)!$, donc de $(S - 1)!$; on en déduit que $v_p(\prod_{r \neq m} (r - m)) \leq v_p((S - 1)!) \leq \frac{S-1}{p-1}$. On a donc, avec les notations du lemme 1, l'inégalité $L \leq K - 1 + \frac{S-1}{p-1}$, et par suite $K - L + M - 1 \geq M - \frac{S-1}{p-1}$, d'où le lemme dans le cas de p impair.

On suppose maintenant que p est égal à 2.

Comme les b_h sont tous impairs, on a $b_h^2 \equiv 1 [4]$. Il existe donc $c_k \in \mathbb{N}$ tels que $b_k^2 \equiv 5^{c_k} [2^{M'}]$, avec $M' \geq M$, choisi de façon qu'en notant $v(z) = \sum_1^s a_k 5^{c_k z}$ on ait $v_2(v(0)) = v_2(u(0))$.

On poursuit alors la démonstration comme dans le cas p impair.

LEMME 3. — Soit $u(n) = \sum_1^s a_k b_k^n$ vérifiant les hypothèses du théorème 1. Soit p un nombre premier, tel que tous les b_h soient des unités p -adiques. Soient M, N , deux entiers non nuls. On note $B(p, M, N)$ le cardinal de l'ensemble des indices n , $0 \leq n \leq N$ tels que $u(n) \equiv 0 [p^M]$. Il existe alors deux constantes c_1, c_2 , strictement positives telles que

$$B(p, M, N) \leq c_1 \frac{pN}{M \log(p)} + c_2 \frac{p^2}{\log(p)}.$$

Preuve. — On note, pour $0 \leq r \leq p - 2$, $v(n) = u(n + r)$, et nous allons appliquer le lemme 2 à la suite v . On suppose $p \neq 2$. Soient T, S deux entiers, et K le cardinal des entiers n de $[T + 1, T + S]$ tels que $v((p - 1)n) \equiv 0 [p^M]$. D'après le lemme 2, on a la relation $v_p(v(0)) = v_p(u(r)) \geq \min(K, M - \frac{S-1}{p-1})$. Donc si $M - \frac{S-1}{p-1} \geq K$, on a $K \leq v_p(u(r))$. Puisque $K \leq S$, il suffit d'avoir $S \leq M \frac{p-1}{p} + \frac{1}{p}$ pour avoir $K \leq v_p(u(r))$. Nous notons dans ce qui suit $[y]$ la partie entière du réel y .

Soit maintenant S un entier quelconque. On découpe alors l'intervalle $\{0, 1, \dots, S\}$ en des intervalles de longueur $[M \frac{p-1}{p} + \frac{1}{p}]$, sauf peut-être le dernier d'entre eux. Sur chacun de ces intervalles, le nombre d'indices n tels que $v((p-1)n) \equiv 0 \pmod{p^M}$ est majoré par $v_p(u(r))$.

Dans le cas général, le nombre de ces intervalles est majoré par $[\frac{S}{[M(1-1/p)+1/p]}] + 1$, quantité plus petite que $\frac{2pS}{M(p-1)} + 1$. Le nombre d'indices $n, 0 \leq n \leq S$, tels que $v((p-1)n) \equiv 0 \pmod{p^M}$ est donc majoré par $(2 \frac{pS}{M(p-1)} + 1)v_p(u(r))$.

L'ensemble des indices $n, 0 \leq n \leq N$, tels que $u(n) \equiv 0 \pmod{p^M}$ est la réunion des ensembles $W_r = \{k \mid (p-1)k + r \leq N \text{ et } u((p-1)k + r) \equiv 0 \pmod{p^M}\}$ où r varie entre 0 et $p-2$. Il est clair qu'un ensemble W_r est inclus dans $\{0, \dots, [\frac{N}{p-1}]\}$.

Le nombre des indices n tels que $0 \leq n \leq N$ vérifiant $u(n) \equiv 0 \pmod{p^M}$ est donc majoré par l'expression

$$\left(\frac{8N}{Mp} + 1\right) \left(\sum_{r=0}^{p-2} v_p(u(r))\right).$$

Il nous reste à majorer $\sum_{r=0}^{p-1} v_p(u(r))$; il existe une constante $c_2 > 1$ telle que, pour tout n entier, on ait $|u(n)| \leq c_2^{n+1}$. On en déduit $v_p(u(r)) \leq c_3 \frac{r+1}{\log(p)}$, d'où la majoration $\sum_{r=0}^{p-2} v_p(u(r)) \leq c_4 \frac{p^2}{\log(p)}$ avec $c_4 > 0$. Finalement, on a la majoration :

$$B(p, M, N) \leq c_1 \frac{pN}{M \log p} + c_2 \frac{p^2}{\log(p)} \quad c_1, c_2 \text{ strictement positives.}$$

On voit facilement que si $p = 2$, il existe une inégalité analogue.

LEMME 4. — Soit $u(n) = \sum_1^s a_k b_k^n$. On suppose que les hypothèses du théorème 1 sont vérifiées. Soit p un nombre premier qui divise au moins l'un des b_i . Soient M, N deux entiers non nuls. Avec les notations du lemme 3, il existe alors des constantes c_1, c_2, c_3, c_4 strictement positives telles que l'on ait :

$$B(p, M, N) \leq c_1 \frac{pN}{M \log(p)} + c_2 \frac{p^2}{\log(p)} + c_3 \log(N) + c_4.$$

Preuve. — Puisque le plus grand commun diviseur des $b_k, k = 1, 2, \dots, s$ est égal à un, le nombre premier p ne divise pas tous les b_k .

On peut toujours supposer que p ne divise pas b_1, \dots, b_t , $t \leq s - 1$, et p divise b_{t+1}, \dots, b_s . Soit

$$w(n) = \sum_1^t a_k b_k^n.$$

On a, pour tout n $w(n) \equiv u(n) [p^n]$. Soit $F = \{n \mid 0 \leq n \leq N, u(n) \equiv 0 [p^M]\}$. Si $N \geq M$, la partie de F formée des indices n $M \leq n \leq N$ est égale à l'ensemble $\{n \mid M \leq n \leq N \mid w(n) \equiv 0 [p^M]\}$, donc de cardinal majoré par une quantité de la forme $c'_1 \frac{p^N}{M \log(p)} + c'_2 \frac{p^2}{\log p}$, c'_1 et c'_2 étant deux quantités strictement positives indépendantes de p, M et N , par application du lemme 3.

Il reste donc à majorer le cardinal de l'ensemble $H = \{n \in F \mid 0 \leq n \leq M\}$, (ensemble qui est égal à F si $N \leq M$).

Soit L un entier fixé, et $G_L = \{n \mid \frac{L}{2} \leq n \leq L, w(n) \equiv 0 [p^n]\}$. G_L est inclus dans $\{n \mid 0 \leq n \leq L \mid w(n) \equiv 0 [p^{\lfloor L/2 \rfloor}]\}$, donc son cardinal est majoré, d'après le lemme 3, par

$$c''_1 \frac{pL}{L/2 \log p} + c'_2 \frac{p^2}{\log p} = c''_1 \frac{2p}{\log p} + c'_2 \frac{p^2}{\log p} \leq c_3,$$

avec c_3 une constante absolue, ne dépendant que de u ; on a utilisé là le fait que les p premiers divisant le produit des b_k sont en nombre fini.

L'ensemble H est inclus dans la réunion des G_L pour $L = M, M/2, \dots, M/2^k$; on a un ensemble d'intervalles du type G_L en nombre majoré par $c_4 \log(M + 1)$, $c_4 > 0$. Finalement, le cardinal de H est majoré par $c_5 \log(M + 1)$.

Maintenant, si H est vide, la majoration annoncée est bien sûr correcte; sinon, il existe $h \in \{0, 1, \dots, N\}$ tel que $u(h) \equiv 0 [p^M]$, ce qui entraîne $p^M \leq c_2^{h+1}$, d'où $M \log p \leq \log(c_2)(N + 1)$, i.e. $M \leq c_6 (N + 1)$, et finalement $\log(M + 1) \leq c_7 \log(N) + c_8$.

Il est clair que la réunion des résultats des lemmes 3 et 4 prouve la proposition 1.

PROPOSITION 2.— Soit U un ensemble fini de nombres premiers, dont on note le cardinal par r . Soient J et L deux entiers, avec $L > J$.

On note $E(U, J, L)$ l'ensemble des indices $n, J \leq n \leq L$, tels que tous les facteurs premiers de $u(n) = \sum_1^r a_k b_k^n$ appartiennent à U . On a alors la majoration :

$$\text{card}(E(U, 0, L)) \leq c_1 r \log(L) \left(\sum_{\ell \in U} \ell \right) + c_2 \log(L) \left(\sum_{\ell \in U} \frac{\ell^2}{\log(\ell)} \right) + c_3 r (\log L)^2.$$

Preuve. — Notons $U = \{\ell_1, \dots, \ell_r\}$. Pour $n \in E(U, J, L)$ on peut écrire $|u(n)| = \ell_1^{k_1(n)} \dots \ell_r^{k_r(n)}$ avec $k_i(n) \in \mathbb{N}$.

Pour $m = 1, 2, \dots, r$ on note $E_m(U, J, L)$ l'ensemble des indices n de $E(U, J, L)$ tels que $\ell_m^{k_m(n)}$ soit le plus grand des $\ell_i^{k_i(n)}$ $i = 1, 2, \dots, r$. On note M le plus petit des $k_m(n)$ quand n décrit $E_m(U, J, L)$ supposé non vide.

Pour n appartenant à $E_m(U, J, L)$ on a alors $u(n) \equiv 0[\ell_m^M]$. D'après la proposition 1, on a donc

$$\text{card}(E_m(U, J, L)) \leq c_1 \frac{\ell_m L}{M \log \ell_m} + c_2 \frac{\ell_m^2}{\log \ell_m} + c_3 \log(L) + c_4.$$

Maintenant, il existe n_o dans $E_m(U, J, L)$ tel que l'on ait $k_m(n_o) = M$. On a donc $\ell_1^{k_1(n_o)} \dots \ell_m^M \dots \ell_r^{k_r(n_o)} = |u(n_o)| \leq \ell_m^{Mr}$ puisque ℓ_m^M est le plus grand des $\ell_i^{k_i(n_o)}$.

D'autre part, $n_o \geq J$ et il existe une constante $c > 0$ telle que $|u(J)| \geq \exp[cJ]$. On a donc $\ell_m^{Mr} \geq \exp[cJ]$, d'où l'on déduit que $Mr \log(\ell_m) \geq cJ$ et finalement $M \log(\ell_m) \geq c \frac{J}{r}$. On trouve donc :

$$\text{card } E_m(U, J, L) \leq c'_1 \ell_m r \frac{L}{J} + c_2 \frac{\ell_m^2}{\log \ell_m} + c_3 \log(L) + c_4$$

En sommant pour $m = 1$ à r , il vient donc :

$$\text{card } E(U, J, L) \leq c'_1 r \frac{L}{J} \left(\sum_{m=1}^r \ell_m \right) + c_2 \sum_{m=1}^r \frac{\ell_m^2}{\log \ell_m} + c_3 r \log L + c_4 r.$$

On découpe maintenant l'intervalle $\{0, 1, \dots, L\}$ en intervalles de la forme $\left[\left[\frac{T}{2}, T \right], T \right]$; il y a au plus $c \log(L)$ intervalles de ce type, et $\text{card} \left(U, \left[\frac{T}{2}, T \right], T \right)$ est majoré par une expression

$$c''_1 r \left(\sum_1^r \ell_m \right) + c_2 \sum_1^r \frac{\ell_m^2}{\log \ell_m} + c_3 r \log(L) + c_4 r.$$

Au total, on a donc une majoration de $\text{card } E(U, O, L)$:

$$\text{card } E(U, 0, L) \leq c_1 \left(r \sum_1^r \ell_m \right) \log(L) \sum_1^r \frac{\ell_m^2}{\log \ell_m} + c_3 r (\log L)^2$$

(les constantes c_1, c_2, c_3 ne sont plus les mêmes que celles ainsi notées précédemment).

Preuve du théorème 1. – Dans la proposition 2, nous allons prendre pour ensemble U l'ensemble des r premiers nombres premiers. On a les estimations suivantes :

$$\sum_1^r \ell_m \leq c r^2 \log(r) \quad \text{et} \quad \sum_1^r \frac{\ell_m^2}{\log \ell_m} \leq c' r^3 \log r$$

avec $c > 0, c' > 0$.

On en déduit : $\text{card } E(U, 0, L) \leq c'' r^3 \log(r) (\log L)^2$ avec $c'' > 0$. Soit maintenant $\epsilon(L)$ une fonction strictement positive de L , de limite nulle quand L tend vers $+\infty$.

On note $B = \{n | P(u(n)) < \epsilon(n) n^{1/3}\}$. Soit L un entier assez grand, et $B_L = \{n \in B | n \leq L\}$. On définit la fonction $r(L)$ par $r(L) = \frac{L^{1/3}}{\log(L)} \sqrt{\epsilon(L)}$. On a $r(L) \log r(L) \sim \frac{1}{3} L^{1/3} \sqrt{\epsilon(L)}$, de sorte que, pourvu que L soit assez grand, $\epsilon(L) L^{1/3} \ll r(L) \log r(L)$.

Donc, si n appartient à B_L , le plus grand facteur de $u(n)$ est plus petit que le $r(L)$ -ième nombre premier. On a donc $B_L = \{n \in B | n \leq L\} \subset E(U_L, 0, L)$ avec $U_L = \{p_1, \dots, p_{r(L)}\}$.

On a $\text{card } E(U_L, 0, L) = o(L)$, donc finalement l'ensemble B est de densité arithmétique nulle. Finalement, on a bien $P(u(n)) \geq \epsilon(n) n^{1/3}$, sauf peut-être pour un ensemble d'indices de densité arithmétique nulle, ce qui démontre le théorème 1.

§ VI. Preuve du théorème 2

Nous aurons besoin de lemmes analogues à ceux démontrés dans la partie III, mais sous une forme plus précise, les résultats démontrés pour s quelconque ne permettant pas de démontrer une version du théorème 2 dans le cas général.

LEMME 5. — Soit $u(n) = a_1 b_1^n + a_2 b_2^n$, avec $(a_1, a_2) = 1$ et $(b_1, b_2) = 1$. Soit p un nombre premier. On note $B(p, M, N)$ le cardinal de l'ensemble des

indices n , $0 \leq n \leq N$, tels que $u(n) \equiv 0[p^M]$. Il existe c_1 et c_2 constantes strictement positives telles que $B(p, M, N) \leq c_1 \frac{N}{M \log(p)} + c_2$.

Preuve. — Supposons tout d'abord que p ne divise pas le produit $a_1 b_1 a_2 b_2$. Dans ce cas, la suite $u(n)$ est périodique modulo p^M ; soit τ_M le plus petit entier t tel que t soit non nul et $b_1^t \equiv b_1^t [p^M]$. On vérifie facilement que $u(n) \equiv 0[p^M]$ équivaut à $u(n + \tau_M) \equiv 0[p^M]$.

Par conséquent, $\{n \mid u(n) \equiv 0[p^M]\}$ est ou vide, ou de la forme $\{n_0 + k \tau_M, k \in \mathbb{N}\}$. Dans le dernier cas, on trouve que $B(p, M, N)$ est majoré par $\frac{N}{\tau_M} + 1$. D'autre part, on a $|b_1^{\tau_M} - b_2^{\tau_M}| \geq p^M$, d'où on déduit l'inégalité $\tau_M \geq c_1 M \log(p)$, d'où finalement $B(p, M, N) \leq c \frac{N}{M \log(p)} + 1$.

Si p divise le produit $a_1 a_2 b_1 b_2$, il y a, puisque par hypothèse a_1 et a_2 d'une part, et b_1 et b_2 d'autre part, sont premiers entre eux, deux cas de figure à permutations près de a_1, a_2 et b_1, b_2 :

- 1) p divise $a_1 b_1$, et ne divise ni a_2 , ni b_2
- 2) p divise a_1 et b_2 , et ne divise ni a_2 , ni b_1 .

Dans le premier cas, on voit que, pour tout entier M supérieur ou égal à un, l'ensemble $\{n \mid u(n) \equiv 0[p^M]\}$ est vide, ou réduit à $\{0\}$.

Dans le second cas, on note m la valuation p -adique de a_1 . Soit M un entier supérieur ou égal à $m + 1$. On voit facilement que $\{n \mid u(n) \equiv 0[p^M]\}$ est inclus dans $\{0, \dots, m\}$.

Il existe donc une constante M_0 , dépendant uniquement de la suite $u = (u(n))$, telle que $B(p, M, N)$ soit majoré indépendamment de p, M et N pourvu que p divise $a_1 a_2 b_1 b_2$ et que M soit plus grand que M_0 . Il en résulte encore qu'il existe, quand p divise $a_1 a_2 b_1 b_2$, une constante c strictement positive telle que l'on ait pour tout M et N

$$B(p, M, N) \leq c \frac{N}{M \log(p)} + 1$$

d'où le lemme.

Nous démontrons maintenant le théorème 2, en suivant le schéma de démonstration du théorème 1, dont on reprend les notations. Soit U un ensemble de nombres premiers, $U = \{\ell_1, \dots, \ell_r\}$. Avec les notations antérieures, on a :

$$\text{card } E_m(U, J, L) \leq c_1 \frac{L}{M \log \ell_m} + c_2 \leq c'_1 r \frac{L}{J} + c_2.$$

On a donc

$$\text{card } E(U, J, L) \leq c'_1 r^2 \frac{L}{J} + c_2 r \leq c_3 r^2 \frac{L}{J}.$$

Et enfin, on a

$$\text{card } E(U, 0, L) \leq c_4 r^2 \log(L).$$

Ce qui est intéressant dans cette estimation est que l'ensemble U n'intervient que par son cardinal r .

Prenons pour U l'ensemble des nombres premiers divisant l'un des $u(k)$, $0 \leq k \leq L$. On a alors $E(U, 0, L) = \{0, 1, \dots, L\}$, d'où $r^2 \geq c_5 \frac{L}{\log L}$, i.e. $r \geq c_6 \left(\frac{L}{\log L}\right)^{1/2}$.

Soit maintenant x un réel assez grand, et

$$A_x = \{p \in A \mid p \leq x\}.$$

Il existe $c > 0$ tel que pour tout n on ait $|u(n)| \leq c^{n+1}$. Soit $L = [c_2 \log x]$ $c_2 > 0$, choisi de façon que l'on ait $c^{c_2 \log x} \leq x$. Il est alors clair que si p divise l'un des $u(k)$ avec $k \leq L$, on a $p \leq x$. Donc $\{p \mid \exists k \leq L \quad p \mid u(k)\} \subset A_x$, de sorte que

$$\varphi(x) = \text{card } A_x \geq \text{card } \{p \mid \exists k \leq L \quad p \mid u(k)\} \geq c_6 \left(\frac{L}{\log L}\right)^{1/2}.$$

Finalement, on a pour x assez grand une inégalité du type $\varphi(x) \geq c_7 \left(\frac{\log x}{\log \log x}\right)^{1/2}$, ce qui démontre le théorème 2.

Notes : 1) Le Professeur C.L.STEWART nous a amicalement informé que, pour les suites binaires non dégénérées, il est possible de démontrer, avec les notations du théorème 2, $\varphi(x) \geq c_7 \log(x)$, en utilisant les méthodes de [7].

2) L'auteur remercie vivement le Referee pour ses nombreuses suggestions pour une meilleure rédaction de cet article.

Références

- [1] LAGARIAS (J.C.).— The set of prime dividing the Lucas numbers has density $2/3$, *Pacific Journal of Maths*, t. **118**, n°2, 1985, p. 449-461.
- [2] LEWIS (D.J.) and MONTGOMERY (H.L.).— On zeros of p -adic forms, *Michigan Math. Journal*, t. **30**, 1983, p. 83-87.
- [3] POLYA (G.).— Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen, *J. Reine Angew. Math.*, t. **151**, 1921, p. 1-31.

Sur les diviseurs premiers

- [4] SHPARLINSKII (I.E.).— On prime divisors of recursive sequences, *Izv. Vyssh. Uchebn. Zaved. Math* (4), t. 215, 1980, p. 101-103.
- [5] STEPHENS (P.J.).— Prime divisors of second order linear recurrences, I et II, *J. Number Theory*, t. 8, 1976, p. 313-345.
- [6] STEWART (C.L.).— On the Greatest prime factor of terms of a linear recurrence sequence, *Rocky Mountain J. of Maths.*, t. 15, n^o2, 1985, p. 599-608.
- [7] STEWART (C.L.).— On divisors of terms of linear recurrent sequences, *J. Reine angew Math.*, t. 333, 1982, p. 12-31.