Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Maurice Mignotte

Suites récurrentes linéaires

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 15, n° 2 (1973-1974), exp. n° G14, p. G1-G9

<http://www.numdam.org/item?id=SDPP_1973-1974__15_2_A9_0>

Séminaire DELANGE-PISOT-POITOU
(Groupe d'étude de théorie des nombres)
15e année, 1973/74, n° G14, 9 p.

6 mai 1974

SUITES RÉCURRENTES LINÉAIRES

par Maurice MIGNOTTE

RÉSUMÉ. - Les suites considérées sont à valeurs entières. Le calcul d'un nombre fini de termes d'une suite récurrente linéaire permet de savoir si elle admet une infinité de zéros. Dans certains cas, des méthodes p-adiques permettent de déterminer tous les zéros d'une suite récurrente. On donne ensuite une minoration effective, essentiellement la meilleure possible, du terme général des suites récurrentes d'un certain type. Pour une suite récurrente binaire (u_n), on donne aussi une minoration effective du plus grand diviseur premier de u_n. Le calcul du n-ième terme d'une suite récurrente linéaire peut être effectué en $O(\log n)$ opérations, ceci permet de savoir si un polynôme P à coefficients entiers se décompose en facteurs linéaires modulo p après $O(\log p)$ calculs.

I. Notations et préliminaires.

Une suite $\underset{\sim}{u} = (u_n)_{n\geq 0}$ de nombres est dite récurrente s'il existe un entier h, et des nombres $q_1, q_2, \ldots, q_h$ $(q_h \neq 0)$ tels que

$$u_{n+h} = q_1 u_{n+h-1} + \ldots + q_h u_n \text{ , si } n \geq 0 . \tag{1}$$

On ne considérera que le cas où les q_j sont des entiers, ainsi que les u_n. Si on pose

$$\mathcal{U}_n = \begin{pmatrix} u_n \\ u_{n+1} \\ \cdot \\ \cdot \\ \cdot \\ u_{n+h-1} \end{pmatrix} \text{ pour } n \geq 0 \text{ et } \mathcal{Q} = \begin{pmatrix} 0 & 1 & 0 & \ldots & . \\ 0 & 0 & 1 & 0 & \ldots \\ \ldots & & & & \\ \ldots & & & & \\ 0 & \ldots\ldots\ldots & & 0 & 1 \\ q_h & \ldots\ldots\ldots & & & q_1 \end{pmatrix},$$

la relation (1) s'écrit sous forme matricielle

$$\mathcal{U}_{n+1} = \mathcal{Q}\mathcal{U}_n = \mathcal{Q}^{n+1}\,\mathcal{U}_0 \text{ , pour } n \geq 0 . \tag{1}'$$

On associe à $\underset{\sim}{u}$ le polynôme

$$P(X) = X^h - q_1 X^{h-1} - q_2 X^{h-2} - \ldots - q_h = (X-\alpha_1)^{k_1} \ldots (X-\alpha_r)^{k_r} ,$$

où les α_i sont distincts. Sur la décomposition de Jordan de $\mathcal{Q}$, on voit qu'il existe des polynômes $R_1, \ldots, R_r$, de degrés respectivement majorés par $k_1 - 1, \ldots, k_r - 1$, tels que l'on ait

$$u_n = R_1(n)\,\alpha_1^n + \ldots + R_r(n)\,\alpha_r^n \text{ , si } n \geq 0 . \tag{2}$$

On dira qu'une suite $\underset{\sim}{u}$, vérifiant (1), est d'ordre au plus égal à h ; elle sera dite d'ordre h si elle ne vérifie aucune relation d'ordre plus petit, dans ce cas les polynômes $R_j(t)$, $j = 1, \ldots, r$, sont de degré $k_j - 1$.

Inversement, une suite $\underset{\sim}{u}$, définie par (2), vérifie la relation (1).

Si $\underset{\sim}{u}$ vérifie (1), et si on considère la suite $\underset{\sim}{v} = (v_n)_{n\geq 0}$ définie par

$$v_n = u_{nT+m}\ ,\quad n \geq 0\quad (\ T > 0\ ,\quad m \geq 0\ ,\ \text{entiers fixés}),$$

la relation (2) montre que l'on a

$$(3)\qquad v_n = \Sigma_{j=1}^{r}\ \alpha_j^m\ R_j(nT + m)(\alpha_j^T)^n\ ;$$

on en déduit que $\underset{\sim}{v}$ vérifie une relation de récurrence d'ordre $\leq h$ et que cette relation ne dépend que de T.

II. Applications de méthodes p-adiques.

1. Le théorème de Skolem-Mahler.

THÉORÈME 1. - *Soit* (u_n) *une suite récurrente à valeurs entières. Soit* E *l'ensemble des indices* n *tel que* u_n *soit nul. Alors* E *est égal à une union finie de progressions arithmétiques* (*).

Démonstration. - Soit $K = \underset{\sim}{Q}(\alpha_1\ ,\ \ldots\ ,\ \alpha_r)$, et soit $\mathfrak{p}$ un idéal premier de K tel que les α_j soient des $\mathfrak{p}$-unités.

Il est facile de voir que, pour tout $\varepsilon > 0$, il existe un entier T tel que

$$|\alpha_j^T - 1|_{\mathfrak{p}} < \varepsilon\ ,\quad j = 1\ ,\ \ldots\ ,\ r\ .$$

En particulier, il existe un entier T tel que les fonctions

$$f_m\ :\ x \longmapsto \Sigma\ R_j(xT + m)\ \alpha_j^m\ \exp((\log \alpha_j^T)x)\ ,\quad m = 0\ ,\ 1\ ,\ \ldots\ ,\ T - 1\ ,$$

soient définies et analytiques pour $x \in \underset{\sim}{Z}_p$ (p nombre premier au-dessous de $\mathfrak{p}$). Bien sûr, $u_{nT+m} = f_m(n)$.

Si la suite $\underset{\sim}{u}$ possède une infinité de zéros, il en est de même pour certaines des fonctions f_m. Or, les f_m sont des fonctions analytiques sur le compact $\underset{\sim}{Z}_p$, et, à moins d'être identiquement nulles, elles ne possèdent qu'un nombre fini de zéros. D'où la conclusion.

COROLLAIRE. - *Si* $\underset{\sim}{u}$ *admet une infinité de zéros, alors, pour tout* α_i, *il existe* α_j, $j \neq i$, *tel que* α_i/α_j *soit une racine de l'unité.*

Supposons que l'on ait $v_n = u_{nT+m} = 0$ pour tout n. La conclusion résulte alors facilement de la relation (3).

Le problème se pose de savoir décider si $\underset{\sim}{u}$ comporte ou non une infinité de zéros. Pour cela, remarquons d'abord que dans la démonstration du théorème 1, on peut déterminer de manière effective l'idéal $\mathfrak{p}$ et le nombre T ; il suffit, par exemple, de choisir $\mathfrak{p}$ au-dessus d'un nombre premier, qui ne divise pas q_h, discr P ; il existe alors une valeur convenable de T, égale à $p^f - 1$ avec

(*) Certaines de ces progressions arithmétiques peuvent être de raison nulle!

$f \leqslant h!$. On peut alors considérer les fonctions f_m . Il suffit ensuite de noter que f_m est identiquement nulle sur $\underset{\sim}{N}$ si, et seulement si, $f_m(i) = 0$ pour $i = 0 , \ldots , h - 1$. Pour montrer que cette condition est suffisante, on utilise le fait, évident, qu'une suite récurrente d'ordre $\leqslant h$, dont les h premières valeurs sont nulles, est identiquement nulle (on a vu au §I que la suite $v_n = f_m(n)$ vérifiait une relation de récurrence d'ordre $\leqslant h$). Il suffit donc de calculer les Th premières valeurs de $\underset{\sim}{u}$. Nous avons démontré le résultat suivant.

Complément. - Pour déterminer si une suite récurrente linéaire entière admet une infinité de zéros, il suffit de calculer ses N premières valeurs, pour un certain nombre N effectif.

2. Détermination des zéros des suites récurrentes.

Un exemple montrera concrètement comment on procède.

Considérons la suite récurrente, définie par

$$u_0 = u_1 = 0 , \quad u_2 = 1 , \quad u_{n+3} = 2u_{n+2} - 4u_{n+1} + 4_n \quad \text{si} \quad n \geqslant 0 .$$

On constate que l'on a

$$u_0 = u_1 = u_4 = u_6 = u_{13} = u_{52} = 0 .$$

Cet exemple, dû à J. BERSTEL, contredit une conjecture affirmant qu'une suite récurrente cubique à valeurs entières, qui n'a qu'un nombre fini de zéros, en a au plus 5 (voir [4]).

Montrons que les zéros trouvés plus haut sont les seuls. Choisissons $p = 53$. Modulo p , le polynôme $P = X^3 - 2X^2 + 4X - 4$ se décompose en facteurs linéaires distincts. Soient $\alpha_1 , \alpha_2 , \alpha_3$ les racines de P dans $\underset{\sim}{Q}_p$, ce sont des p-unités. Les inégalités $v_p(\alpha_i^{p-1} - 1) \geqslant 1$ montrent que les fonctions

$$n \longrightarrow u_{(p-1)n+m} , \quad m \in \{0 , 1 , \ldots , 51\} ,$$

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

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

on vérifie facilement que l'on a

$$(4) \qquad v_p(a_{k,m}) \geqslant i \quad \text{si} \quad k \geqslant i , \text{ pour } i = 1 , 2 , 3 .$$

On constate que

$$v_p(f_m(0)) = 0 \quad \text{si} \quad m \notin \{0 , 1 , 4 , 6 , 13\} ,$$

dans ce cas une égalité

$$f_m(x) = \sum_0^{\infty} a_{k,m} x^k = a_{0,m} + (\sum_{k=1}^{\infty} a_{k,m} x^k) = 0$$

est impossible pour $x \in \underset{\sim}{Z}_p$ puisque

$$0 = v_p(a_{0,m}) < 1 \leqslant v_p(\sum_{h=1}^{\infty} a_{k,m} x^k) .$$

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

$$v_p(f_m(1)) = 1 \quad \text{et} \quad f_m(0) = 0 ,$$

d'où (utiliser (4) avec $i = 2$)

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

Enfin, pour $m = 0$,

$$f_0(0) = f_0(1) = 0 , \quad v_p(f_0(2)) = 2 ,$$
$$f_0(x) = x(a_{1,m} + \sum_{k=2}^{\infty} a_{k,m}\, x^{k-1}) , \quad v_p(a_{1,m}) = 2 ;$$

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

Pour k entier, on pose

$$(X)_k = \prod_{0 \leqslant i < k} (X - i) .$$

Du fait que X^n est une combinaison linéaire à coefficients entiers des $(X)_i$, pour $i \leqslant n$, on voit qu'une série $\sum a_n x^n$ se met sous la forme $\sum b_n (x)_n$, où $v_p(b_n) \geqslant \min_{m \geqslant n} v_p(a_m)$. Si on applique ceci à f_0, on trouve

$$f_0(x) = b_2 (x)_2 + \sum_{k \geqslant 3} b_k (x)_k \quad , \text{ où } v_p(b_2) = 2 , \ v_p(b_3) \geqslant 3 \text{ si } k \geqslant 3$$
$$= b_2\, x(x-1)(1 + g(x)) \text{ , où } v_p(g(x)) > 1 \text{ si } x \in Z_p .$$

Ce qui montre que, pour $x \in Z_p$, les seuls zéros de f_0 sont 0 et 1. D'où le résultat annoncé.

Nous aurions aussi pu utiliser brutalement le résultat suivant.

THÉORÈME de Strassman. - Soit $f(x) = \sum_0^{\infty} a_k x^k$, $a_k \in K_p$, une série convergente sur $\mathcal{O}_p$, anneau des entiers de K_p, non identiquement nulle. Alors, le nombre de zéros de f dans $\mathcal{O}_p$ est majoré par

$$N = \max\{k \ ; \ v_p(a_k) \text{ est minimal}\} .$$

On en trouvera une démonstration dans [4]. Dans tous les cas, ce théorème permet de majorer le nombre de zéros de u, si ce nombre est fini.

III. Applications des travaux de Baker.

1. Minoration du terme général.

THÉORÈME 2. - *Soit u une suite récurrente à valeurs entières telle que le polynôme P associé possède au plus trois racines de module maximal et que ces racines $\alpha_1, \dots, \alpha_\ell$ $(\ell \leqslant 3)$ soient simples. Alors, il existe des constantes effectives C_1, C_2, C_3 telles que si*

$$u_n = R_1 \alpha_1^n + \dots + R_\ell \alpha_\ell^n + R_{\ell+1}(n)\, \alpha_{\ell+1}^n + \dots + R_r(n)\, \alpha_r^n , \quad (R_1, \dots, R_\ell \text{ sont constantes})$$

et

$$u'_n = R_1 \alpha_1^n + \ldots + R_\ell \alpha_\ell^n ,$$

on ait

$$|u_n| \geq C_1 |\alpha_1|^n n^{-C_2} \text{ si } u'_n \neq 0 \text{ et } n \geq C_3 .$$

Démonstration. - D'après les hypothèses, il existe $\lambda > 0$ tel que l'on ait

$$u_n = u'_n + O(|\alpha_1|^n e^{-\lambda n}) .$$

Par conséquent, il suffit de démontrer l'existence des constantes effectives C'_1 , C'_2 et C'_3 telles que

$$(u'_n \neq 0) \Rightarrow (|u'_n| \geq C'_1 |\alpha_1|^n n^{-C'_2} \text{ si } n \geq C'_3) .$$

On supposera $R_1 \neq 0$. Le cas $R_2 = R_3 = 0$ est évident. Quitte à diviser par $|\alpha_1|^{-n}$, on se ramène à l'étude d'une expression du type

$$x_n = a_1 y_1^n + \overline{a}_1 \overline{y}_1^n + a_3 \; ; \; a_1, y_1 \text{ algébriques}, \; a_1 \neq 0 , \; |y_1| = 1 , \; a_3 = 0 \text{ ou } 1 .$$

Il est clair qu'il suffit de considérer le cas $a_3 \leq 2|a_1|$. Posons alors

$$u_1 = |a_1| e^{i\psi} , \; y_1 = e^{i\theta} , \; a_3 |a_1|^{-1} = -2 \cos \varphi \; ; \; \theta , \varphi , \psi \in]-\pi , \pi] .$$

On a

$$(*) \qquad |x_n| = 4|a_1| \left|\sin\left(\frac{n\theta + \psi + \varphi}{2}\right) \sin\left(\frac{n\theta + \psi - \varphi}{2}\right)\right| .$$

En distinguant les cas $\varphi = 0$ et $\varphi \neq 0$, on voit qu'il existe deux constantes effectives C_4 et C_5 positives telles que

$$0 < |x_n| < \eta < C_4 \Rightarrow 0 < \min_{|m| \leq n, \varepsilon = \pm 1} |n\theta + m\pi + \psi + \varepsilon\varphi| < C_5 \eta^{\frac{1}{2}} .$$

On est ramené à l'étude d'une forme linéaire en logarithmes de nombres algébriques. Le résultat résulte du théorème ci-dessous.

THÉORÈME de Baker [1]. - Soient $\beta_1 , \ldots , \beta_n$ des nombres algébriques fixés. Il existe une constante C effective, telle que, pour tout $\delta \in]0 , \frac{1}{2}[$, les inégalités

$$0 < |b_1 \log \beta_1 + \ldots + b_{k-1} \log \beta_{k-1} - \log \beta_k| < \delta^{-C} e^{-\delta B}$$

n'ont pas de solutions entières $b_1 , \ldots , b_{k-1}$ de module au plus égal à B .

(En fait, BAKER démontre un résultat beaucoup plus fort.)

Dans le cas présent, il suffit de remarquer qu'en posant $\delta = C/B$, ce qui est possible si $B > 2C$, on obtient

$$|b_1 \log \beta_1 + \ldots + \log \beta_k| > \left(\frac{C}{e}\right)^C B^{-C} \text{ si } B > 2C \text{ et } |b_1 \log \beta_1 - \ldots - \log \beta_k| \neq 0 .$$

D'où la conclusion.

Examinons quelques conséquences du théorème 2. Si u'_n a au moins trois zéros, alors (*) montre que $y_1 = \alpha_2/\alpha_1$ est une racine de l'unité ; on en déduit une

nouvelle démonstration du théorème de Skolem-Mahler dans le cas où les hypothèses du théorème 2 sont vérifiées. De plus, le théorème 2 permet de déterminer tous les zéros de $\underset{\sim}{u}$. Dans le cas où $|\alpha_1| > 1$ (si $|\alpha_1| = 1$, α_1 est une racine de l'unité, voir théorème 3 plus loin, la suite $\underset{\sim}{u}$ est périodique), $|u_n|$ tend vers l'infini et on peut déterminer toutes les solutions n de l'équation $u_n = a$, a fixé.

Il semble difficile de démontrer le théorème 2 dans le cas général. On peut par contre l'étendre à quelques cas particuliers. Par exemple, si $\ell = 4$ et $u'_n = \alpha_1^n + \overline{\alpha}_1^{-n} + \alpha_3^n + \overline{\alpha}_3^{-n}$, on a

$$u'_n = 2|\alpha_1|^n \,|\cos n\theta_1 + \cos n\theta_2| = 4|\alpha_1|^n \cos(n\,\frac{\theta_1 + \theta_2}{2}) \cos(n\,\frac{\theta_1 - \theta_2}{2}) ,$$

et on peut alors raisonner de manière analogue à ce qui précède.

2. Minoration du plus grand diviseur premier (récurrences binaires).

Soit $\underset{\sim}{u}$ une suite récurrente binaire dont le terme général est donné par la formule

$$u_n = a\alpha^n + b\beta^n = a\alpha^n(1 - c\gamma^n) .$$

Soit $\mathfrak{p}$ un idéal premier de K tel que a, α et c soient des unités $\mathfrak{p}$-adiques. On a alors

$$|u_n|_{\mathfrak{p}} = |1 - c\gamma^n|_{\mathfrak{p}} .$$

Supposons de plus $|1 - c|_{\mathfrak{p}}$ assez petit. Pour $\varepsilon > 0$ assez petit, on a

$$0 < |u_n|_{\mathfrak{p}} \leq \varepsilon \Rightarrow |\log c + n \log \gamma|_{\mathfrak{p}} \leq \varepsilon ,$$

où les logarithmes sont définis sur $K_{\mathfrak{p}}$. On peut alors appliquer l'analogue p-adique des travaux de Baker (voir par exemple l'article de SPRINDŽUK [7]).

Ceci permet, sous les hypothèses précédentes, de minorer effectivement $|u_n|_{\mathfrak{p}}$. En fait, ceci peut être obtenu pour tout $\mathfrak{p}$. Les minorations obtenues montrent que le plus grand facteur premier de u_n tend vers l'infini et que, si $p_1, \ldots, p_\ell$ sont des nombres premiers fixés, et si on désigne par U_n le plus grand diviseur de u_n de la forme $p_1^{i_1} \ldots p_\ell^{i_\ell}$, alors $\log U_n = o(\log |u_n|)$ si γ n'est pas une racine de l'unité, les inégalités obtenues étant effectives. Nous espérons revenir de manière plus précise sur cette question une autre fois.

IV. Applications des suites récurrentes.

1. Un lemme de Kronecker.

THÉORÈME 3 (KRONECKER). - *Soit α un entier algébrique dont les conjugués $\alpha_1 = \alpha, \ldots \alpha_d$ sont tous de module 1. Alors α est une racine de l'unité.*

Démonstration. - Posons

$$u_n = \mathrm{Tr}(\alpha^n) = \alpha_1^n + \ldots + \alpha_d^n \text{ , pour } n \geq 0 .$$

La suite $\underset{\sim}{u}$ est à valeurs entières, bornée ; donc ultimement périodique. Clairement, $|\mathrm{Norm}(\alpha)| = 1$, donc $\underset{\sim}{u}$ vérifie une relation de récurrence du type

$$u_{n+d} = q_1 u_{n+d-1} + \ldots \pm u_n \text{ si } n \geq 0 .$$

Elle est donc purement périodique. Soit T sa période. On a

$$u_T = \alpha_1^T + \ldots + \alpha_d^T = u_0 = d , \quad |\alpha_i| = 1 \text{ pour } i = 1 , \ldots , d .$$

Donc $\alpha_1^T = 1$.

2. Décomposition de polynômes modulo p .

Soit $P(X) = X^d + a_1 X^{d-1} + \ldots + a_d$ un polynôme à coefficients entiers. Soit p un nombre premier. On cherche à déterminer le comportement de P modulo p ; $\overline{P}$ désignera le polynôme réduit modulo p .

On peut supposer $p \nmid a_d$. Soient $\alpha_1 , \ldots , \alpha_r$ les racines de $\overline{P}$ dans une extension de $\underset{\sim}{F}_p$. On pose $K = \underset{\sim}{F}_p(\alpha_1 , \ldots , \alpha_r)$. On se propose de calculer $[K : \underset{\sim}{F}_p]$ avec le minimum d'opérations possible. Les calculs qui suivent seront effectués dans K . On considère les suites récurrentes vérifiant

$$(5) \qquad u_{n+d} = - a_1 u_{n+d-1} - \ldots - a_d u_n \text{ si } n \geq 0 \qquad (u_n \in K) .$$

Si $\underset{\sim}{w}$ désigne la solution de (5) vérifiant les conditions initiales

$$w_0 = \ldots = w_{d-2} = 0 , \quad w_{d-1} = 1$$

alors, toute solution $\underset{\sim}{u}$ de (5) est de la forme

$$u_n = c_0 w_n + c_1 w_{n+1} + \ldots + c_{d-1} w_{n+d-1} , \quad c_i \in K .$$

En particulier, si α désigne l'un quelconque des α_i , on a

$$\alpha^n = b_0 w_n + b_1 w_{n+1} + \ldots + b_{d-1} w_{n+d-1} , \quad n \geq 0 .$$

La suite $\underset{\sim}{w}$ est purement périodique, soit D sa période. La relation précédente montre que les α_i vérifient

$$(6) \qquad \alpha_i^D = 1 , \quad i = 1 , \ldots , r .$$

Pour simplifier, supposons que p ne divise pas le discriminant de P ; les α_i sont alors au nombre de d , et $\underset{\sim}{w}$ est de la forme

$$w_n = \beta_1 \alpha_1^n + \ldots + \beta_d \alpha_d^n ,$$

ce qui prouve que, dans ce cas, D divise le p. p. c. m. des ordres des α_i . Ce résultat, joint à (6), montre que D est égal au p. p. c. m. des ordres des α_i . De plus, si $[K : \underset{\sim}{F}_p] = f$, f est le plus petit entier tel que D divise $p^f - 1$. La détermination de D permet donc de calculer f . Ainsi f est le plus petit des entiers qui vérifient

$$w_{p^f-1} = w_{p^f} = \dots = w_{p^{f+d-2}} = 0 \ , \quad w_{p^{f+d-1}} = 1 \ .$$

L'entier d étant fixé, ainsi que P , pour déterminer f , pour p variable, il suffit de calculer un nombre constant de termes de $\underset{\sim}{w}$ (on a $f \mid d!$). La relation (1)' montre que le calcul de w_n revient à celui d'une puissance n-ième d'une certaine matrice, ce qui nécessite $O(\log n)$ opérations. On a donc montré que la détermination de f nécessite $O(\log p)$ opérations. Récapitulons les résultats obtenus.

THÉORÈME 4. - Soit $(u_n)_{n\geq 0}$ une suite récurrente linéaire. On peut calculer une valeur particulière u_n en $O(\log n)$ opérations.

THÉORÈME 5. - Soit P un polynôme unitaire à coefficients entiers. Pour p premier, $p \nmid P(0)\,\mathrm{discr}(P)$; soit K l'extension de F_p la plus petite dans laquelle P se décompose en facteurs linéaires. Alors on peut déterminer le degré de K sur $\underset{\sim}{F}_p$ en $O(\log p)$ opérations.

Ce théorème contient évidemment le résultat suivant.

COROLLAIRE. - Soient P et p comme ci-dessus. On peut savoir si P a toutes ses racines dans $\underset{\sim}{F}_p$ après $O(\log p)$ opérations.

On notera la puissance de ce résultat par rapport au calcul banal de

$$P(0) \ , \ P(1) \ , \ \dots \ , \ P(p-1) \ .$$

Dans le cas où P est de degré 3 , soit L l'extension de $\underset{\sim}{Q}$ engendrée par l'une des racines de P . On supposera L non galoisienne. On montre dans ce cas que la décomposition d'un idéal (p) dans L sous la forme $(p) = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3$ correspond à la représentation simultanée de p par certaines formes quadratiques. Cette vérification nécessite $O(p^{1/2})$ calculs au lieu des $O(\log p)$ opérations du corollaire.

Notes. - Il est clair que, partout, on aurait pu remplacer l'hypothèse u_n entier par u_n algébrique. On trouvera des détails supplémentaires sur le complément au théorème 1 dans [3]. Une forme plus faible du théorème 2 paraîtra en [6]. Les résultats, prouvés ou annoncés en II.1 et II.2, sont des généralisations effectives de résultats de K. MAHLER [5] sur les suites récurrentes binaires.

Pour le théorème 4, voir [2] (où des méthodes pratiques de calcul plus précises sont mises en évidence). Le théorème 5 peut être d'une utilité pratique réelle pour calculer des tables donnant le comportement de l'idéal (p) dans un corps de nombres.

BIBLIOGRAPHIE

[1] BAKER (A.). - A sharpening of the bounds for linear forms in logarithms, II., Acta Arithm., Warszawa, t. 24, p. 33-36.

[2] BERSTEL (J.). - Sur le calcul des termes d'une suite récurrente linéaire, Exposé fait à l'I. R. I. A. (Rocquencourt) en mars 1974.

[3] BERSTEL (J.) et MIGNOTTE (M.). - Problèmes décidables sur les suites récurrentes linéaires (en préparation).

[4] LEWIS (D. J.). - Diophantine equations : p-adic methods, "Studies in number theory", p. 23-75. - Englewood Cliffs, Prentice-Hall, 1969.

[5] MAHLER (K.). - A remark on recursive sequences, J. math. Sc., t. 1, 1966, p. 12-17.

[6] MIGNOTTE (M.). - A note on linear recursive sequences, J. Austr. math. Soc. (à paraître).

[7] SPRINDŽUK (V. G.). - On rational approximations to algebraic numbers [en russe], Izv. Akad. Nauk SSSR, Ser. Mat., t. 35, 1971, p. 991-1007 ; [en anglais], Mathematics of the USSR-Izvestija, t. 5, 1971, p. 1003-1019.

(Texte reçu le 8 mai 1974)

Maurice MIGNOTTE
Département de Mathematiques
Centre scientifique et polytechnique
Place du 8 mai 1945
93206 SAINT DENIS