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: B. ÉTUDE ARITHMÉTIQUE
DOI: https://doi.org/10.5169/seals-87887

ramènent le problème de la recherche de conditions nécessaires et suffisantes pour l'existence du Q.D.-schéma à celui de la distribution des zéros dans les s.r.l. $H_{j,n}$. (Ce problème — relativement à une s.r.l. arbitraire — a été étudié en [6].)

B. ÉTUDE ARITHMÉTIQUE

> La théorie des suites récurrentes est une mine inépuisable qui renferme toutes les propriétés des nombres; en calculant les termes consécutifs de telles suites, en décomposant ceux-ci en facteurs, en recherchant par l'expérimentation les lois de l'apparition et de la reproduction des nombres premiers, on fera progresser d'une manière systématique l'étude des propriétés des nombres et de leurs applications dans toutes les branches des Mathématiques.
>
> Edouard LUCAS *(Théorie des Nombres)*

I. MÉTHODES ÉLÉMENTAIRES

1. *Propriétés de périodicité*

Le premier résultat de ce type est dû à Lagrange, la proposition suivante est essentiellement due à Carmichael.

PROPOSITION. *Soit* ξ *une suite à valeurs dans un anneau* $\mathscr{A}$ *et vérifiant la relation de récurrence linéaire (à coefficients dans* $\mathscr{A}$*)*

$$\xi_{n+k} = a_{k-1}\,\xi_{n+k-1} + a_{k-2}\,\xi_{n+k-2} + \ldots + a_0\,\xi_n, n \geqslant 0\,.$$

On suppose que ξ *ne prend qu'un nombre fini de valeurs; alors* ξ *est ultimement périodique. De plus, lorsque* a_0 *n'est pas un diviseur de zéro, la suite* ξ *est purement périodique.*

Considérons la suite $(\xi_n, \xi_{n+1}, \ldots, \xi_{n+k-1})_{n\geqslant 0}$ des k-uples de valeurs successives de ξ. Si ξ ne prend qu'un nombre fini de valeurs alors ces k-uples ne prennent aussi qu'un nombre fini de valeurs, il existe donc $n_0 \geqslant 0$ et $t > 0$ tels que

$$(\xi_n, \xi_{n+1}, \ldots, \xi_{n+k-1}) = (\xi_{n+1+t}, \ldots, \xi_{n+t+k-1}) \quad \text{pour} \quad n = n_0\,.$$

Grâce à la relation de récurrence cette égalité reste vraie pour tout $n \geqslant n_0$ et on a donc $\xi_{n+t} = \xi_n$ pour $n \geqslant n_0$. C'est la première assertion.

Supposons en outre a_0 non diviseur de zéro et que n_0 a été choisi minimal. Si on a $n_0 \geqslant 1$ alors la relation de récurrence montre que

$a_0(\xi_{n_0-1}-\xi_{n_0+t-1}) = 0$, ce qui implique $\xi_{n_0-1} = \xi_{n_0+t-1}$, formule qui contredit la minimalité de n_0. On a donc $n_0 = 0$, autrement dit la suite ξ est bien purement périodique. □

On peut en déduire une démonstration du théorème de Kronecker.

COROLLAIRE. *Soit* θ *un entier algébrique non nul dont tous les conjugués sont de module au plus* 1, *alors* θ *est une racine de l'unité.*

Soient $\theta_1 = \theta, \theta_2, ..., \theta_d$ les conjugués de θ et $X^d - a_{d-1}X^{d-1} - ... - a_0$ son polynôme minimal sur $\mathbf{Z}$. Pour n entier $\geqslant 0$ posons $\xi_n = \theta_1^n + \theta_2^n + ... + \theta_d^n$. Alors la suite (ξ_n) vérifie

$$\xi_{n+d} = a_{d-1}\xi_{n+d-1} + ... + a_0\xi_n, \quad n \geqslant 0,$$

de plus les ξ_n sont des entiers de l'intervalle $[-d, +d]$. Enfin a_0 est non nul, la proposition implique donc que (ξ_n) est purement périodique. Soit t la période, on a $\xi_t = \xi_0$; soit $\theta_1^t + ... + \theta_d^t = d$, et comme $|\theta_i| \leqslant 1$ pour $i = 1, ..., d$, $\theta^t = 1$. □

Le cas particulier de la proposition 1 le plus intéressant est celui où $\mathscr{A} = \mathbf{F}_p(=\mathbf{Z}/p\mathbf{Z})$, p étant (comme toujours !) un nombre premier. Considérons donc une série s.r.l. ξ à valeurs dans $\mathbf{F}_p$ et vérifiant

$$\xi_{n+k} = a_{k-1}\xi_{n+k-1} + ... + a_0\xi_n, \quad n \geqslant 0 \ (a_0, ..., a_{k-1} \in \mathbf{F}_p).$$

Soit $L = \mathbf{F}_{p^d}$ la plus petite extension de $\mathbf{F}_p$ dans laquelle le polynôme $G = X^k - a_{k-1}X^{k-1} - ... - a_0$ se décompose en facteurs linéaires. Alors ξ est ultimement périodique (purement périodique si $a_0 \neq 0$) et sa période est un diviseur de $p(p^d-1)$, ce qu'on voit en utilisant les formules (3) et (4) de A.I.2 [d'une part les ρ_j appartiennent à L^* et vérifient donc $\rho_j^{p^d-1} = 1$, d'autre part les coefficients du binôme modulo p admettent p comme période]; en outre si G n'a que des racines simples alors la période divise $p^d - 1$. Le cas des suites récurrentes linéaires binaires est très simple. L'entier d ne peut alors prendre que les valeurs 1 ou 2. Plus précisément, si ξ vérifie

$$\xi_{n+2} = a_1\xi_{n+1} + a_0\xi_n, \quad n \geqslant 0, \quad a_0, a_1 \in \mathbf{F}_p, \quad a_0 \neq 0,$$

posons $\Delta = a_1^2 + 4a_0$ et supposons p impair. Le symbole de Legendre permet de caractériser les cas $d = 1$ ou 2: on a

$$d = 2 \quad \text{si et seulement si} \quad \left(\frac{\Delta}{p}\right) = -1 .$$

Ainsi, on a les trois possibilités suivantes:

(i) Δ est un résidu quadratique modulo p, alors la période t divise $p-1$,

(ii) Δ n'est pas un résidu quadratique modulo p, alors t divise p^2-1,

(iii) $\Delta = 0$, alors t divise $p(p-1)$.

On peut raffiner l'assertion (ii) de la manière suivante. Supposons $\left(\frac{\Delta}{p}\right) = -1$. Soient ρ_1 et ρ_2 les racines du polynôme $X^2 - a_1X - a_0$ dans le corps $\mathbf{F}_{p^2}$ et soit σ l'automorphisme de Frobenius de ce corps $(\sigma(\alpha)=\alpha^p)$. On a d'une part

$$\xi_n = \alpha_1\rho_1^n + \alpha_2\rho_2^n , \quad \alpha_1, \alpha_2 \in L ,$$

et d'autre part

$$\rho_1^p = \rho_2 , \ \rho_2^p = \rho_1 \quad \text{et} \quad \rho_1\rho_2 = -a_0 .$$

D'où

$$\rho_1^{p+1} = \rho_2^{p+1} = \rho_1\rho_2 = -a_0 ,$$

ce qui prouve l'assertion suivante.

(ii)′ Soit e l'ordre de $-a_0$ dans le corps $\mathbf{F}_p$, alors si Δ n'est pas résidu quadratique modulo p, la période divise $e(p+1)$.

Exemple 1: Reprenons la suite de Fibonacci. On a alors,

$$F_{n+2} = F_{n+1} + F_n , \quad \Delta = 5 , \quad e = 2$$

et les trois cas précédents sont

(i) $p = 5k \pm 1$, la période divise $p-1$,

(ii) $p = 5k \pm 2$, la période divise $2(p+1)$ (c'est encore vrai pour $p = 2$)

(iii) $p = 5$, la période est égale à 20.

On en déduit aussitôt les propriétés de divisibilité suivantes:

si $p = 5k \pm 1$ alors p divise F_n lorsque $p-1$ divise n,

si $p = 5k \pm 2$ alors p divise F_n lorsque $p+1$ divise n,

[en effet, $F_n = \dfrac{\rho_1^n - \rho_2^n}{\rho_1 - \rho_2}$ donc $F_{p+1} = \dfrac{\rho_1\rho_2 - \rho_1\rho_2}{\rho_1 - \rho_2} = 0$],

enfin si $p = 5$ on vérifie directement que 5 divise F_n si et seulement si 5 divise n.

Exemple 2: Le critère de Lucas peut être obtenu comme corollaire de l'étude précédente. Soit $\omega = \dfrac{1+\sqrt{5}}{2}$ le nombre d'or. On considère la suite d'entiers $r_m = \omega^{2^m} + \omega^{-2^m}$, $m = 1, 2, 3, \ldots$, ainsi $r_m = 3, 7, 47, \ldots$, et on peut calculer aisément les r_m grâce à la relation évidente $r_{m+1} = r_m^2 - 2$. En fait si (L_n) est la s.r.l. — dite de Lucas — définie par $L_0 = 2$, $L_1 = 1$, $L_{n+2} = L_{n+1} + L_n$ pour $n \geqslant 0$, on a $r_m = L_{2^m}$. On a alors le critère de primalité suivant.

PROPOSITION 2. *Soit p un nombre premier de la forme $4n + 3$ et soit $M = M_p = 2^p - 1$, le $p^{ième}$ nombre de Mersenne. Alors M est premier si, et seulement si, $r_{p-1} \equiv 0 \pmod M$.*

Supposons d'abord M premier, $M = 8 \cdot 16^n - 1 \equiv 2 \pmod 5$, donc $\omega^{M+1} \equiv -1 \pmod M$, ce qui implique bien

$$r_{p-1} = (\omega^{M+1} + 1)\,\omega^{-2^{p-1}} \equiv 0 \pmod M .$$

Inversement, supposons $r_{p-1} \equiv 0 \pmod M$. On a alors

(*) $\omega^{2^p} \equiv -1 \pmod M$ [comme deux lignes plus haut]

donc

(**) $\omega^{2^{p+1}} \equiv 1 \pmod M$.

Supposons que M se décompose sous la forme

$$M = \Pi\, p_i \cdot \Pi\, q_j$$

où les p_i sont des nombres premiers de la forme $5a \pm 1$ et les q_j sont des nombres premiers de la forme $5a \pm 2$, et on a

$$\omega^{p_i - 1} \equiv 1 \pmod{p_i}, \qquad \omega^{2(q_j+1)} \equiv 1 \pmod{q_j} .$$

Comme les congruences (*) et (**) sont valables pour tout diviseur de M, on voit que l'ordre de ω modulo chaque diviseur premier de M est exactement 2^{p+1}. Donc les p_i et les q_j sont respectivement de la forme

$$p_i = 2^{p+1} h_i + 1 \quad \text{et} \quad q_j = 2^p k_j - 1 .$$

Le premier cas est impossible puisqu'on aurait $p_i > M$; le second cas n'est possible que pour $k_j = 1$ et on a donc $M = q_j$, M est bien premier! □

Ce test s'applique par exemple pour $p = 7$ et montre que 127 est premier, de la même manière (mais après plus de calculs!) on peut montrer que M_{127} est aussi premier.

D'autres tests de primalité sur les nombres de Mersenne et de Fermat figurent dans l'ouvrage de Sierpinski [56], chap. X.

2. *L'équation de Pell-Fermat*

Soit Γ une « conique » définie sur $\mathbf{Z}$, elle peut alors être caractérisée par une équation à coefficients entiers de la forme

$$ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0.$$

En multipliant cette équation par a, on a la forme équivalente (si $a \neq 0$)

$$(ax+by+d)^2 + (ac-b^2)y^2 + 2(ac-bd)y + af - d^2 = 0.$$

Si $a = 0$ et $c \neq 0$ on obtient une écriture analogue.

Si $a = c = 0$ alors b est non nul (sinon Γ est une droite) et en posant $x' = x + y$, $y' = x - y$ on peut mettre l'équation de Γ sous la forme

$$2bx'^2 - 2by'^2 + 2(d+e)x' + 2(d-e)y' + f = 0,$$

ce qui nous ramène au cas précédent.

Ainsi, par un changement convenable de coordonnées, on peut se limiter à l'étude de l'équation

$$x'^2 + c'y'^2 + 2d'y' + f' = 0;$$

— pour $c' > 0$, Γ est une ellipse qui, bien entendu, n'a qu'un nombre fini de coordonnées entières (que l'on peut calculer facilement),

— pour $c' = 0$, Γ est une parabole, nous n'étudierons pas ce cas (on peut encore déterminer facilement les points entiers de Γ),

— pour $c' < 0$, Γ est une hyperbole et par un nouveau changement de coordonnées on peut mettre l'équation sous la forme

$$(E) \qquad X^2 - DY^2 = k, \quad \text{avec} \quad D > 0.$$

Nous excluons encore le cas trivial où k est nul. Nous sommes donc ramenés à l'étude de cette équation, dite de Pell-Fermat. Si $D = u^2$ est le carré d'un entier on a la décomposition

$$(X-uY)(X+uY) = k$$

et Γ n'a qu'un nombre fini de points que l'on trouve de manière évidente. On supposera donc désormais que D n'est pas un carré.

La théorie de l'équation de Pell-Fermat est bien connue. On montre (cf. par exemple Borevitch et Schafarevitch [10], chap. II, § 5, Th. 1) qu'il existe un nombre fini de solutions $(x^{(1)}, y^{(1)}), \ldots, (x^{(k)}, y^{(k)})$ qui peuvent être calculées effectivement, telles que toute solution (x, y) vérifie

$$x + \sqrt{D}\, y = (x^{(i)} + \sqrt{D}\, y^{(i)})\, \varepsilon^s,$$

où $1 \leqslant i \leqslant k$, $s \in \mathbf{Z}$, et ε est l'unité fondamentale de l'anneau $\mathbf{Z}[\sqrt{D}]$ dont la norme est égale à 1.

On a donc les formules

$$x = x_s^{(i)} = \frac{1}{2}\left((x^{(i)} + \sqrt{D}\, y^{(i)})\, \varepsilon^s + (x^{(i)} - \sqrt{D}\, y^{(i)})\, \varepsilon^{-s}\right)$$

et

$$y = y_s^{(i)} = \frac{1}{2}\left((x^{(i)} + \sqrt{D}\, y^{(i)})\, \varepsilon^s - (x^{(i)} - \sqrt{D}\, y^{(i)})\, \varepsilon^{-s}\right).$$

Ceci montre qu'il existe un nombre fini de suites récurrentes binaires $\xi^{(1)}, \ldots, \xi^{(k)}, \eta^{(1)}, \ldots, \eta^{(k)}$ admettant toutes $X^2 - (\varepsilon + \varepsilon^{-1})X - 1$ comme échelle telles que les solutions de l'équation (E) soient exactement les couples $(\xi_n^{(i)}, \eta_n^{(i)})$, $1 \leqslant i \leqslant k$ et $n \geqslant 0$.

Exemple 1 : Considérons l'équation

$$X^2 - 5Y^2 = 1, \quad \text{avec } X \text{ et } Y \text{ positifs}.$$

On sait que l'unité fondamentale du corps $\mathbf{Q}(\sqrt{5})$ est le nombre d'or $\omega = \dfrac{1+\sqrt{5}}{2}$, de conjugué $\dfrac{1-\sqrt{5}}{2} = -\omega^{-1}$. D'autre part l'anneau des entiers de ce corps est principal, donc si x, y est une solution avec $x > 0$ et $y \geqslant 0$, il existe $n \geqslant 0$ tel que

$$x + \sqrt{5}\, y = \pm\left(\frac{1 \pm \sqrt{5}}{2}\right)^{2n}.$$

On voit aussitôt que les deux signes doivent être $+$, donc

$$x + \sqrt{5}\, y = \left(\frac{1+\sqrt{5}}{2}\right)^{2n} = \left(\frac{3+\sqrt{5}}{2}\right)^{n}.$$

Ensuite, on constate que n doit être multiple de trois, soit

$$x + \sqrt{5}\, y = (9+4\sqrt{5})^s, \quad s \geqslant 0.$$

Les solutions sont donc $(x_s, y_s) = (1, 0), (9, 4), (161, 72), \ldots$ et elles vérifient

$$x_{s+2} = 18x_{s+1} - x_s, \quad y_{s+2} = 18y_{s+1} - y_s \quad \text{pour} \quad s \geqslant 0.$$

On peut exprimer ces nombres en fonction des nombres de Fibonacci et de Lucas,

$$x_s = \frac{1}{2} L_{3s}, \quad y_s = \frac{1}{2} F_{3s}.$$

[On a plus généralement $L_n^2 - 5\, F_n^2 = (-1)^n 4$ pour tout $n \geqslant 0$].

Exemple 2: Considérons l'équation $\dfrac{x(x+1)}{2} = 3 \cdot 2^k - 5$ où x et k sont inconnus (et entiers!). Posons $X = 2x + 1$; l'équation devient

$$X^2 - 3 \cdot 2^n = -39, \quad \text{où} \quad n = k + 3.$$

Si $n = 2m + 1$ est impair, posons $y = 2^m$, alors

$$X^2 - 6y^2 = -39,$$

mais comme $\left(\dfrac{6}{13}\right) = -1$, l'équation n'a pas de solution. Donc n est pair, disons $n = 2m$. Posons encore $y = 2^m$, alors

$$X^2 - 3y^2 = -39.$$

Donc $X = 3z$ et

$$y^2 - 3z^2 = 13.$$

On peut montrer (cf. [42]) que les solutions $y \geqslant 0$ sont les valeurs de la suite (y_s) définie par

$$y_0 = 4, \quad y_1 = 11, \quad y_s = 4y_{s-1} - y_{s-2}, \quad s \in \mathbf{Z}.$$

Donc $\ldots y_{-2} = 16,\ y_{-1} = 5,\ y_0 = 4,\ y_1 = 11,\ y_2 = 40 \ldots$ et on constate que pour les petites valeurs de $|s|$ seuls y_0 et y_{-2} sont des puissances de 2 qui correspondent aux deux solutions de l'équation initiale

$$x = 1, \quad k = 1: \frac{1(1+1)}{2} = 3 \cdot 2 - 5,$$

et

$$x = 13\,, \quad k = 5 : \frac{13(13+1)}{2} = 3 \cdot 2^5 - 5\,.$$

Nous allons montrer que ce sont les seules. D'abord ce sont les seules pour $k \leqslant 6$. Supposons que l'équation ait une solution avec $k \geqslant 7$ (i.e. $m \geqslant 5$) alors $y = y_t = 2^m$. On vérifie sans peine que ceci impose $t \equiv 6 \bmod 16$ (regarder y_s modulo 32). On considère enfin (y_s) modulo 31, cette suite est de période 32 (on a $\left(\frac{3}{31}\right) = -1$) et

$$t \equiv 6 \bmod 16 \Rightarrow y_t \equiv \pm 7 \bmod 31\,.$$

Mais, modulo 31, les puissances de 2 sont 1, 2, 4, 8 et 16. Donc l'équation considérée n'a que les deux solutions notées précédemment.

La méthode appliquée ici est un cas particulier d'un algorithme général présenté en [42] et qui s'applique à toutes les équations diophantiennes de la forme $f(x) = c \cdot a^n$, où f est un polynôme du second degré; c'est ainsi que l'on peut obtenir une nouvelle démonstration du fait que l'équation de Ramanujan-Nagell $x^2 + 7 = 2^n$ sont obtenues pour $n = 3, 4, 5, 7, 15$ (on considère des congruences modulo 7681, voir [43]).

Exemple 3: Nous allons montrer que les seuls carrés de la suite de Lucas 2, 1, 3, 4, 7 ... sont 1 et 4 et que les seuls carrés de la suite de Fibonacci 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233 ... sont 0, 1 et 144. Ce résultat est dû à Cohn [20] (voir aussi le chapitre 8 du livre de Mordell [48]).

Si $\omega = \dfrac{1+\sqrt{5}}{2}$ et $\omega' = \dfrac{1-\sqrt{5}}{2}$, on sait déjà que

$$F_n = \frac{\omega^n - \omega'^n}{\sqrt{5}} \quad \text{et} \quad L_n = \omega^n + \omega'^n\,,$$

ce qui permet d'étendre la définition de ces suites à $n \leqslant 0$. Modulo 4, les deux suites sont de période 6

n	0	1	2	3	4	5	6	7	. .
F_n mod 4	0	1	1	2	3	1	0	1	. .
L_n mod 4	2	1	3	0	3	3	2	1	. .

comme on le voit sur cette table.

De la relation $L_n^2 - 5F_n^2 = 4(-1)^n$ et de la table on déduit que

$$(F_n, L_n) = 1 \quad \text{si} \quad n \not\equiv 0 \pmod 3,$$
$$(F_n, L_n) = 2 \quad \text{si} \quad n \equiv 0 \pmod 3.$$

Démontrons d'abord l'assertion sur L_n.

Si $n = 2m$ est pair la formule $L_{2m} = L_m^2 - 2$ montre que L_n ne peut être un carré.

Supposons donc n impair. Il suffit de considérer le cas $n > 0$, et même $n \geqslant 5$ ($L_1 = 1$ et $L_3 = 4$ sont des carrés). On peut écrire $n = c + 2 \cdot t\,k$ avec $t = 3^r$, $k > 0$, $k \equiv \pm 2 \pmod 6$ et $c = 1$ ou 3. Et les formules

$$\begin{aligned} 2L_{m+2k} &= 5F_m L_{2k} + L_m L_{2k} \\ &= 5F_m F_k L_k + L_m(L_k - 2) \\ &\equiv -2v_m \pmod{L_k} \end{aligned}$$

jointes au fait que L_k est impair montrent que

$$L_n = L_{c+2tk} \equiv -L_c \equiv -1, -4 \pmod{L_k}.$$

Si L_n est un carré $\left(\dfrac{-1}{L_k}\right) = +1$ mais comme $L_k \equiv 3 \pmod 4$ c'est impossible.

Passons maintenant aux nombres de Fibonacci F_n.

Si $n \equiv 1 \pmod 4$, supposons $n \neq 1$ (sinon $F_n = 1$ est un carré). Comme plus haut écrivons $n = 1 + 2\,t\,k$ avec $t = 3^r$, $k \equiv \pm 2$ modulo 6. Les formules

$$\begin{aligned} 2F_{m+2k} &= F_n L_{2k} + F_{2k} L_n \\ &= F_n(L_k^2 - 2) + F_k L_k L_n \\ &\equiv -2F_n \pmod{L_k} \end{aligned}$$

et le fait que L_k est impair, impliquent

$$L_n \equiv -1 \pmod{L_k},$$

et comme nous l'avons déjà vu cette congruence est impossible. Donc $n = 1$ et $F_n = 1$.

Si $n \equiv 3 \pmod 4$, le changement de n en $-n$ nous ramène au cas précédent.

Si $n = 2n$ est pair alors $F_{2m} = F_m L_m = x^2$ et on peut supposer $m > 0$.

— 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 (ξ_n) une suite récurrente linéaire à valeurs entières. Alors l'ensemble des indices n tels que ξ_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 ξ_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 ω_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 (ξ_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* (ξ_n) *admet une infinité de zéros, alors, si* ξ_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* ω_j *des nombres algébriques non nuls; pour tout* i *il existe un indice* $j \neq i$ *tel que* ω_i/ω_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 ρ_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 (ξ_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 (ξ_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 ξ_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 (ξ_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 (ξ_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 ω_1, ω_2 et ω_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 (ξ_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 (ξ_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. (ξ_n) a une racine simple ω_k alors la 0-multiplicité de (ξ) est majorée par la multiplicité d'une s.r.l. (η_n) de rang $m - 1$, m étant le rang de (ξ_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 (ξ_n) est égale à la — P_m — multiplicité de (η_n).

On dira que (ξ_n) est *dégénérée* lorsqu'il existe α tel que son α-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 (ξ_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 (ξ_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* α *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* α *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* ξ_n *admet un dénominateur non divisible par* p,

(ii) Ξ *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 (ξ_{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 (ξ_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 ω_1 et ω_2 sont de même module. Considérons en effet le cas le plus simple où (ξ_n) est réelle et donnée par $\xi_n = \omega_1^n + \omega_2^n$.

Si ω_1 et ω_2 sont réels alors $\omega_2 = -\omega_1$, et on a $\xi_n = 2\,\omega_1^n$ si n est pair et $\xi_n = 0$ sinon. Par contre si ω_1 n'est pas réel, $\omega_2 = \bar{\omega}_1$ et on peut écrire $\omega_1 = \rho\, e^{i\theta}$, $\omega_2 = \rho\, e^{-i\theta}$ avec ρ réel > 0; alors

$$\xi_n = 2\,\rho^n \cos(n\,\theta), \quad \text{avec} \quad 0 < \theta < \pi .$$

Pour minorer ξ_n dans ce cas il faut minorer la quantité

$$\operatorname*{Min}_{k \in \mathbf{Z}} \left| n\theta - \left(k + \frac{1}{2}\right)\pi \right| .$$

Le cas $\theta = \dfrac{\pi}{2}$ correspond à une suite dégénérée, nous l'excluons. Ainsi, dans le cas non dégénéré, on aboutit à un problème d'approximation diophantienne.

Si f est une fonction de $\mathbf{N}$ dans lui-même qui croît arbitrairement vite, on peut trouver θ tel que, pour une infinité de valeurs de n, il existe k entier avec $\left| n\theta - \left(k + \dfrac{1}{2}\right)\pi \right| < 1/f(n)$. Pour obtenir une minoration non triviale de $|\,\xi_n\,|$ il est donc nécessaire de faire des hypothèses sur l'approximation du quotient θ/π par des rationnels.

Depuis les travaux de Gel'fond, on sait que de telles hypothèses sont vérifiées lorsque $\cos\theta$ est un nombre algébrique, donc en particulier lorsque ω_1 et ω_2 sont algébriques. Nous nous limiterons donc à l'étude des s.r.l. à valeurs algébriques.

Définissons s par

$$|\,\omega_1\,| = \ldots = |\,\omega_s\,| > |\,\omega_{s+1}\,|,$$

et posons $r_j = 1 + \deg(P_j)$ pour $j = 1, \ldots, k$.

La première minoration effective a été obtenue — pour les s.r.l. binaires — par A. Schinzel [55]. Un théorème plus général a été ensuite publié en [38], où on montre que sous les hypothèses $s \leqslant 3$ et $r_1 = \ldots = r_s = 1$, il existe des constantes effectives c et n_0 telles que, pour $n \geqslant n_0$,

$$|\,\xi_n\,| \geqslant |\,\omega_1\,|^n\, n^{-c}, \quad \text{pourvu que} \quad \sum_{j=1}^{s} P_j\,.\,\omega_j^n \neq 0 .$$

La démonstration est une application directe des estimations de A. Baker sur les formes linéaires de logarithmes de nombres algébriques [4].

Depuis ces résultats ont été étendus en [45], où le résultat suivant est démontré.

THÉORÈME. *Supposons* $s \leqslant 3$ *et qu'au moins un des nombres* ω_i/ω_j, $1 \leqslant i < j \leqslant s$ *ne soit pas une racine de l'unité. Alors il existe des constantes effectivement calculables* $C_1 > 0$ *et* $C_2 > 0$ *qui ne dépendent que de* (ξ_n) *telles que l'on ait*

$$|\xi_n| \geqslant |\omega_1|^n \exp(-C_1(\operatorname{Log} n)^2),$$

pour $n \geqslant C_2$.

La preuve repose aussi sur les minorations de Baker. Pour $s \leqslant 3$, on peut donc déterminer effectivement toutes les solutions de l'équation $\xi_n = \alpha$ pour α fixé.

Si on se limite à l'équation $\xi_n = 0$, on montre dans le même article que les indices n peuvent être déterminés effectivement sous les hypothèses: $s = 4$, $|\omega_1| > 1$ et aucun des ω_i/ω_j, $1 \leqslant i < j \leqslant 4$, n'est une racine de l'unité.

Dans le cas général, la question suivante est ouverte.

PROBLÈME. Etant donné une s.r.l. entière (ξ_n), existe-t-il un algorithme permettant de trouver tous les indices n tels que $\xi_n = 0$?

Nous énonçons la conjecture suivante.

CONJECTURE. Il existe un entier positif k tel que, si $\xi^{(1)}, \ldots, \xi^{(k)}$ sont k suites récurrentes linéaires entières quelconques, la propriété

$$\exists (n_1, n_2, \ldots, n_k), \quad \xi^{(1)}_{n_1} + \ldots + \xi^{(k)}_{n_k} = 0$$

soit indécidable.

Sous certaines hypothèses (voir [45] th. 3), on peut aussi minorer $|\xi_m - \xi_n|$ de manière effective et donc alors — en principe — déterminer les répétitions de la suite (voir [44] pour un exemple).

2. *L'équation* $\xi_m = \eta_n$

En utilisant encore une estimation sur les formes linéaires de logarithmes, on peut montrer (cf. [41]) le résultat suivant.

THÉORÈME. *Soient* (ξ_m) *et* (η_n) *deux suites récurrentes linéaires à valeurs algébriques données par*

$$\xi_m = P_1(m)\,\omega_1^m + \ldots + P_h(m)\,\omega_h^m, \quad P_1 \neq 0,$$

et

$$\eta_n = Q_1(n)\,\rho_1^n + \ldots + Q_k(n)\,\rho_k^n, \quad Q_1 \neq 0.$$

On suppose

$$|\omega_1| > |\omega_2| \geqslant \ldots, \quad |\rho_1| > |\rho_2| \geqslant \ldots, \quad |\omega_1| > 1, \quad |\rho_1| > 1.$$

Alors,

(i) *il existe un entier* N_1, *effectivement calculable, tel que pour* $m+n \geqslant N_1$ *la relation* $\xi_m = \eta_n$ *implique*

$$(*) \qquad P_1(m)\,\omega_1^m = Q_1(n)\,\rho_1^n;$$

(ii) *il existe un entier* N_2, *effectivement calculable, tel que si l'équation* (*) *admet une solution vérifiant* $m+n \geqslant N_1$, *alors* ω_1 *et* ρ_1 *sont multiplicativement dépendants;*

(iii) *soit* Z *l'ensemble des couples* (m, n) *tels que* $\xi_m = \eta_n$, *alors:*

(a) *si* P_1 *et* Q_1 *sont de même degré,* Z *est égal à l'union d'un ensemble fini et d'une union finie de progressions arithmétiques,*

(b) *si les degrés de* P_1 *et* Q_1 *sont distincts et si* Z *est infini, cet ensemble n'est pas du type précédent et on a même*

$$\lim \mathrm{Log}(m_{k+1}/m_k) > 0, \quad \textit{si} \quad (m_k, n_k)$$

désigne la suite des points de Z, *ordonnée par valeurs croissantes de* m.

On peut noter que la preuve de (ii) est élémentaire et que le cas (b) peut se produire: exemple, $\xi_m = 2^m$ et $\eta_n = n\,2^n$. De plus, on sait décider si deux nombres algébriques sont multiplicativement indépendants ou non, donc — sous les hypothèses du théorème — on sait décider si Z est fini ou non. En supposant en outre que les $|\omega_i|$ d'une part, et les $|\rho_j|$ d'autre part, sont distincts on peut même déterminer effectivement Z.

Le cas de l'équation $\xi_m = \xi_n$, pour une s.r.l. binaire, a été traité grâce à une méthode analogue par J. C. Parmani et T. N. Shorey [49].

3. *Sur le plus grand diviseur premier de* ξ_n

Cette question fait l'objet du long article de C. L. Stewart [58], le lecteur désirant plus de détails pourra consulter ce travail. Bien entendu, nous supposons que (ξ_n) est une s.r.l. à valeurs entières. Dans l'écriture

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

nous supposons de plus qu'aucun des quotients ω_i/ω_j, $i \neq j$, n'est une racine de l'unité. Enfin le plus grand diviseur d'un entier a sera noté $P(a)$ (avec la convention $P(0) = P(\pm 1) = 1$).

En 1921, Polya a montré que lim sup $P(\xi_n) = \infty$. Grâce à une généralisation p-adique du théorème de Thue-Siegel-Roth-Schmidt (généralisation due à Schlickewei), récemment R. van der Poorten et Schlickewei ont montré [53] qu'en fait $P(\xi_n)$ tend vers l'infini, une preuve indépendante mais voisine a été donné par Evertse [24]. A ce jour, ces preuves sont ineffectives.

Grâce à la théorie des formes linéaires de logarithmes, Stewart a démontré le résultat suivant (cf. [57]).

THÉORÈME. *Si on a* $|\omega_1| > |\omega_2| \geqslant \ldots |\omega_k|$ *alors, pour tout* $\varepsilon > 0$, *il existe une constante effective* $N = N(\varepsilon, \omega_1, \ldots, \omega_k, P_1, \ldots, P_k)$ *telle que, pour* $n \geqslant N$, *on ait*

$$P(\xi_n) > (1-\varepsilon) \operatorname{Log} n$$

lorsque $\xi_n \neq P_1(n)\, \omega_1^n$.

Des résultats plus forts ont été démontrés pour les s.r.l. binaires, en particulier par C. L. Stewart et T. Shorey; voir [58] pour plus d'information.

BIBLIOGRAPHIE

[1] ABE, E. *Hopf algebras.* Cambridge Univ. Press, 1980.

[2] AMICE, Y. *Les nombres p-adiques.* Paris, P.U.F., 1975.

[3] BACHMANN, P. *Niedere Zahlentheorie.* Zweiter teil, Leipzig, Teubner, 1910.

[4] BAKER, A. A sharpening of the bounds for linear forms in logarithms, II. *Acta Arithm. 24* (1973), 33-36.

[5] BERSTEL, J. *Transductions and context-free languages.* Stuttgart, Teubner, 1979.

[6] BERSTEL, J. et M. MIGNOTTE. Deux propriétés décidables des suites récurrentes linéaires. *Bull. Soc. Math. France 104* (1976), 175-184.

[7] BERSTEL, J. et REUTENAUER. *Les séries rationnelles et leurs langages.* Paris, Masson, 1984.

[8] BEUKERS, F. The multiplicity of binary recurrences. *Compositio Math. 40* (1980), 251-267.

[9] BEUKERS, F. and R. TIJDEMAN. On the multiplicity of binary complex recurrences. *Compositio Math. 51* (1984), 193-213.

[10] BOREVITCH, S. I. et I. R. SCHAFAREVITCH. *Théorie des nombres.* Paris, Gauthier-Villars, 1967.

[11] BOURBAKI, N. *Eléments de mathématiques. Algèbre, chap. 5.* Paris, Herman, 1959.

[12] CERLIENCO, L. e F. PIRAS. Risultante, m.c.m. e M.C.D. di due polinomi col metodo delle s.r.l. *Rend. Sem. Fac. Sci., Univ. Cagliari 50* (1980), 711-717.