I. MÉTHODES ÉLÉMENTAIRES

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **33 (1987)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **24.05.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

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* $\mathscr{A}$*)*

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

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 $(\xi_n, \xi_{n+1}, \dots, \xi_{n+k-1})_{n\geqslant 0}$ 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

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

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

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

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

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

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

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

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

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

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,

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

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 $p^{\text{ième}}$ nombre de Mersenne. Alors M est premier si, et seulement si, $r_{p-1} \equiv 0 \pmod M$.*

Supposons d'abord M premier, $M = 8 \,.\, 16^n - 1 \equiv 2 \pmod 5$, 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

et

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

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 $f(x) = c\,.\,a^n$, 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 $L_n^2 - 5\,F_n^2 = 4(-1)^n$ 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 $n = c + 2\,.\,t\,k$ avec $t = 3^r$, $k > 0$, $k \equiv \pm 2 \pmod 6$ et $c = 1$ ou 3. Et les formules

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

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

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

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 $F_m = 2\,y^2$ et $L_m = 2\,z^2$. Si m est impair on a $z^4 - 5\,y^4 = -1$, ce qui est impossible modulo 8. Si $m = 2\,m'$ alors $F_{m'}\,L_{m'} = 2\,y^2$. Si m' est impair on a $F_{m'} = 2\,t^2$ 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 $n = 3\,.\,2^s\,s \geqslant 3$ 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 $F_{24} = 2\,y^2$ puis $L_{12} = 2\,z^2$, 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)

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

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 $\mathfrak{P}$).