REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE DE JIJEL
FACULTE DES SCIENCES
DEPARTEMENT DE MATHEMATIQUES

Série :

MEMOIRE

Présenté en vue d'obtenir le diplôme de

MAGISTER

Spécialité Mathématiques

Option Analyse

Thème

L'analyse p-adique et les suites linéaires récurrentes

Par

KERKATOU MESSAOUD

Soutenu le :.../.../2008 Devant le jury :

Président :	A. Aibeche	Prof. Univ. Sétif
Rapporteur :	T. Zerzaihi	MC. Univ. Jijel
Examinateurs :	M. Yarou	MC. Univ. Jijel
	D. Azzam. Laouir	MC. Univ. Jijel
	W. Chikouche	D. Univ. Jijel

Laboratoire de Mathématiques Pures et Appliquées (LMPA)

Remerciements

Mes remerciements vont tout d'abord à Dieu le tout puissant pour la santé et la volonté qu'il m'a accordées pour terminer ce mémoire.

Je remercie vivement monsieur **T. Zerzaihi**, *Maître de conférences et chef de département à l'université de Jijel d'avoir voulu proposer et assurer la direction de ce mémoire, pour sa disponibilité et ses conseils judicieux tout au long de ce travail.*

J'exprime ma gratitude la plus sincère à monsieur **A. Aibeche**, *professeur à l'université de Sétif, pour avoir accepter d'être le président du jury de cette thèse, j'en suis honoré.*

Mes remerciements vont également à monsieur **M. Yrou**, *Maître de conférences à l'université de Jijel, à madame* **D. Azzem-Laouir**, *Maître de conférences à l'université de Jijel, à madame* **W. Chikouche**, *docteur à l'université de Jijel, je tiens à leurs exprimer mes remerciements d'avoir bien voulu accepter d'évaluer ce travail.*

Je ne saurais oublier l'ensemble des collègues de Magister, avec une pensée particulière à Mr **M. Kecies** *qui est toujours considéré comme bras de fer pour toute l'équipe de recherche.*

Qu'il me soit permis de saluer enfin **Mr A. Ahrieche**, *docteur en physique théorique pour son aide précieuse afin d'achever ce travail. Merci à tous les membres du département de Mathématiques de l'université de Jijel et à tous ceux qui ont pris part de près ou de loin à la réalisation de ce travail.*

Dédicace

Je dédie ce travail

A mes chers parents

A mes frères

Ahcène

Noureddine

Azzouz

Et Farid.

A mes sœurs

Razika

Sabrina

Et Sihem.

A mes amis

Fayçal

Hassan

Messaoud

Ahcène,...

Et à tous ceux qui me sont chers.

Table des matières

Introduction Générale

L'étude des suites linéaires récurrentes est d'intétêt majeur. leur âge, leur richesse ainsi que la diversité de leurs champs d'application font des suites linéaires récurrentes un sujet tellement vaste et si riche en résultats qu'il faudrait plusieurs ouvrages, en plus de ce qui existent déja, pour faire le tour de toutes leurs propriétés. Les suites linéaires récurrentes constituent une partie fondamentale de la théorie des nombres pour plusieurs années. En outre, ces suites apparaissent partout en mathématiques et en informatique. Par exemple, la théorie des séries entières représentant les fonctions rationnelles ; les nombres générateurs pseudo-aléatoires, les suites automatiques et les automates cellulaires. Les solutions de certaines classes d'équations diophantiènnes et de quelques problèmes combinatoires forment des suites linéaires récurrentes. Une grande variété de séries de puissances, par exemple les fonctions zéta de variétés algébriques sur des corps finis, les fonctions zéta dynamiques, les fonctions génératrices provenant de la théorie des groupes, les séries de Hilbert dans une algèbre commutative et les séries de Poincaré sont toutes connues d'être rationnelles dans de nombreux cas. Les coéfficients de la série representant ces fonctions sont des suites linéaires récurrentes, et donc tant de puissants résultats de la présente étude peuvent être appliqués. Les suites linéaires récurrentes participent également à la preuve du dixième problème de Hilbert sur $\mathbb{Z}$. Elles apparaissent encore dans plusieurs parties de la mathématique appliquée et d'informatique. Plusieurs systèmes de polynômes ortogonaux, y compris les polynômes de Tchebychev, les polynômes de Dickson satisfont des relations de récurrences sous forme de suites linéaires récurrentes. En théorie d'approximation, en cryptographie et en analyse des séries temporelles, les suites linéaires récurrentes jouent un rôle fondamental.

Un second outil intéressant pour simplifier l'étude des suites linéaires récurrentes est l'analyse p-adique. Un analyse construi sur un corps de nombres p-adiques $\mathbb{Q}_p$ muni d'une norme dite ultramétrique notée $\|.\|_p$. La principale motivation ayant donné naissance aux corps des nombres p-adiques était de pouvoir utiliser les téchniques des séries entières dans la théorie des nombres, mais leur utilité dépasse maintenant largement ce cadre.

L'application de l'analyse p-adique dans les suites linéaires récurrentes qui nous intéresse dans ce travail est portée sur un célèbre problème dit de "multiplicité". Un problème qui consiste à déterminer le nombre d'itérations d'un élément d'une suite linéaire récurrente. La plupart des résultats concernant ce problème utilisent des arguments p-adiques ; en particulier les propriétés des normes p-adiques (non-archimédiènnes), le théorème de Strassman appelé souvent "théorème de préparation p-adique de weierstrass" qui consiste à borner le nombre de solutions d'une équation à variable p-adique.

La première motivation du problème de multiplicité remonte aux années trentaine. C'est Morgan ward, le premier qui a conjecturé que la multiplicité d'une suite linéaire récurrente entière non dégénérée d'ordre deux est au plus cinq. Cette conjecture a été démontrée par K. K. Kubota [20] en 1977. En utilisant des mhétodes algébriques F. Beukers [5] et Tijdeman [30] ont amélioré cette borne en prouvant que pour un rationnel d, on a $m(d) + m(-d) \leq 3$.

Récemment, plusieurs auteurs se sont intéressés à établir des bornes supérieures de la multiplicité d'une suite récurrente linéaire d'ordre t comme fonction dépendant seulement de t et $d = [\mathbb{k} : \mathbb{Q}]$ où d est le dégré du corps algébrique contenant les termes de la suite. Citons par exemple Schmidt [28] qui a établit la borne $m(a_n) \leq \exp\exp\exp(3t\log t)$ en 1999. Beukers et Tijdeman [7] ont établit la borne $m(a_n) \leq 100\max\{d, 300\}$. Pour les suites récurrentes linéaires d'ordre trois, Beukers [6] a montré que la zéro-multiplicité ne dépasse pas 6.

Dans ce travail on va aborder une étude approfondie du problème de multiplicité des suites récurrentes linéaires d'ordre deux, du fait de la diversité de leurs champs d'application. La présence de carrés parfaits dans les suites de Fibonacci et Lucas constitue en fait un cas particulier du problème de multiplicité, pour cela le dernier chapitre y consacrée.

Ce mémoire est réparti en quatre chapitres. Dans le premier, on a donné les différentes notions de bases qui s'avèrent indispensables pour le reste de ce travail, en particulier les corps de nombres algébriques et p-adiques, le théorème de Strassman. Le deuxième chapitre est consacré à l'étude du problème de multiplicité. Afin d'établir une comparaison entre les méthodes p-adiques et algébriques utilisées ; on a premièrement étudié ce problème en s'appuyant sur des arguments p-adiques, puis on a abordé dans une deuxième partie ce problème d'un point de vue algébrique. En fait, la méthode algébrique est plus éfficace que celle utilisant les arguments p-adiques. En effet ; étant donnée une suite récurrente linéaire entière d'ordre deux définie par :

$$a_{n+2} = Ma_{n+1} - Na_n$$

avec $|a_0|+|a_1| \neq 0$ et un rationnel d, en s'inspirant de l'étude p-adique, on peut montrer que $m(a_n) \leq 5$ où $m(a_n)$ désigne la multiplicité de la suite$\{a_n\}_{n\geq 0}$, et dans le cas particulier si $(M,N)=1$, on constatera que $m(a_n) \leq 4$, cependant la méthode algébrique améliore cette borne, en prouvant que $m(d)+m(-d) \leq 3$.

Au toisième chapitre, on cherche à déterminer une formule explicite du terme général d'une suite récurrente linéaire d'ordre quelconque. Cette formule ressemble bien à une série de puissances généralisées. En effet, si $\{u_n\}$ est une suite récurrente linéaire d'ordre t définie par les valeurs initiales $u_0, u_1, ..., u_{t-1}$ et la relation de récurrence :

$$u_{n+t} = c_1 u_{n+t-1} + c_2 u_{n+t-2} + ... + c_t u_n, \forall n \geq 0$$

Alors, en désignant par $(\alpha_i)_{\overline{i=1,k}}$ les racines du polynôme caractéristique,

$$x^t - c_1 x^{t-1} - ... - c_t$$

où chaque α_i est de multiplicité r_i, le terme général u_n s'écrit sous la forme :

$$u_n = \sum_{i=1}^{k} p_i(n)\,\alpha_i^n$$

où chaque $p_i(n)$ est un polynôme de dégré au plus égal à $r_i - 1$. En utilisant cette dernière formule l'étude de la multiplicité se ramène à l'étude de quelques équations diophantiènnes de la forme : $x^n+y^n+z^n+... = d$. La dernière partie de ce chapitre est une simple démonstration du célèbre théorème de Skolem-Mahler-Lech [18], un théorème qui détermine la structure générale de l'ensemble des zéros d'une suite récurrente linéaire $\{u_n\}_{n\geq 0}$ comme réunion d'un ensemble fini et d'un nombre fini de progressions arithmétiques.

Comme application du problème de multiplicité, on a étudié dans le quatrième chapitre un autre problème concernant la présence de carrés parfaits dans les suites de Fibonacci et Lucas. Dans cette étude, on a confirmé que les seuls carrés parfaits dans une suite de Fibonacci sont :$F_0 = 0, F_{-1} = F_1 = F_2 = 1$ et $F_{12} = 144$, dans celle de Lucas vérifiant :

$$L_{n+2} = PL_{n+1} - QL_n$$

avec $(P,Q) = (1,-1)$ et $L_0 = 2, L_1 = 1$, les seuls carrés parfaits sonts : $L_1 = 1$ et $L_3 = 4$. Pour les suites de Lucas généralisées $\{x_n\}_{n\geq 0}$ définies par :

$$x_{n+2} = Px_{n+1} - Qx_n$$

avec P, Q impairs, premiers entre eux et vérifiant $P^2 - 4Q > 0$, on a établi une méthode de recherche éfficace qui suit les étapes suivantes :

-On commence à chercher des entiers b tels que : $x_{n+12} \equiv x_n \pmod{b}$.

Soit donc I l'ensemble des indices a, $0 \leq a < 12$ tels que x_a soit un carré modulo tous ces entiers b.

-Ainsi, si x_a est un carré, et si pour tout $j \geq 1$, x_a est premier à un diviseur premier $p_j \equiv -1 \pmod{4}$ de $V_{3.2^j}$ où $\{V_n\}_{n\geq 0}$ est la suite de Lucas du deuxième type, alors aucun $x_{a+12n}(n \neq 0)$ n'est un carré.

-Sinon, i.e., si x_a est un carré modulo les entiers b, mais un non-carré, dans ce cas x_{a+12n} peut être un carré et on commence par tester x_a modulo les diviseurs premiers de V_6. On distingue les cas suivants :

A) S'il existe un diviseur premier $p \equiv 1 \pmod{4}$, et si x_a est un non-carré modulo p, alors aucun x_{a+12n} n'est un carré. Sinon, on a les trois sous-cas suivants :

B.1)Il y a deux diviseurs premiers $p, p' \equiv -1 \pmod{4}$ de V_6 tels que $\left(\frac{x_a}{p}\right)$ et $\left(\frac{x_a}{p'}\right)$ sont opposés. Alors aucun x_{a+12n} n'est un carré.

B.2) x_a est un carré modulo tous les diviseurs premiers $p \equiv -1 \pmod{4}$ de V_6. Alors on teste x_a encore, cette fois modulo les diviseurs premiers de V_{12}.

B.3) x_a est un non-carré modulo tous les diviseurs premiers $p \equiv -1 \pmod{4}$ de V_6, on teste alors x_{a+12} ou x_{a-12} modulo les diviseurs premiers de V_{12}. Et ainsi de suite : on effectue des tests modulo les diviseurs premiers de $V_6, V_{12}, V_{24}, \ldots$ jusqu'à ce qu'on se trouve dans une bonne situation A) ou B.1) (ou jusqu'à ce qu'un carré inattendu soit découvert). Enfin une conclusion générale regroupe et résume tous les résultats des différents chapitres.

Chapitre 1

Notions fondamentales

Le but de ce chapitre est d'exposer les différents concepts et notions indispensables à l'étude des autres chapitres qui viennent ultérieurement. Dans la première partie, on va étudier les nombres p-adiques, en passant en revue toutes ses propriétés spécifiques, en particulier celles qui les diffèrent des nombres réels. Dans une deuxième partie, on va introduire un nouveau corps très riche et plus large par ses applications aussi bien en analyse qu'en algèbre, à savoir le corps des nombres algébriques. La trosième partie constitue une introduction succinte au suites linéaires récurrentes; tout en s'intéressant à des cas particuliers qui servent de modèles pour l'étude entamée dans les deux autres chapitres.

1.1 Corps de nombres p-adiques

Dans $\mathbb{R}$, on sait bien que la série $\sum_{n\geq 0} x^n$ ne converge que pour les x tels que $|x| < 1$. La présente partie consiste à introduire un nouveau corps dit de *nombres $p-adiques$*, que l'on munit d'une norme ultramétrique de telle sorte qu'on peut le considérer comme une complétion de $\mathbb{Q}$ par rapport à cette norme et que la série $\sum_{n\geq 0} x^n$ sera convergente pour toutes les valeurs de x.

Définition 1.1.1 *Soit $\Bbbk$ un corps muni d'une norme $\|.\|$. On dit que la norme $\|.\|$ est ultramétrique (non-archimédienne), si on a*

$$\forall\ x,\ y \in \Bbbk : \|x+y\| \leq \max\{\|x\|, \|y\|\}$$

* *Tout corps muni d'une norme non-archimédienne s'appelle corps ultamétrique.*

Remarque 1.1.2 *Si $d_{\|.\|}$ est la distance induite par la norme $\|.\|$, alors la relation précédente peut s'écrire comme suit*

$$\forall\ x,\ y,\ z \in \Bbbk : d_{\|.\|}(x,z) \leq \max\left\{d_{\|.\|}(x,y), d_{\|.\|}(y,z)\right\}$$

Proposition 1.1.3 *Soit $(\Bbbk, \|.\|)$ un corps valué; alors $\Bbbk$ est un corps ultramétrique si et seulement si*

$$\forall\ n \in \mathbb{N} : \|n\| \leq 1$$

Preuve. Supposons que $\Bbbk$ est ultramétrique et montrons par récurrence que

$$\forall\ n \in \mathbb{N} : \|n\| \leq 1$$

* Pour $n = 1$; on a $\|1\| = 1 \leq 1$.

* Supposons que $\|i\| \leq 1$ pour tout $i \leq n$ et montrons que $\|n+1\| \leq 1$. On a

$$\begin{aligned} \|n+1\| &\leq \max\{\|n\|, \|1\|\} = 1 \\ &\Rightarrow \|n+1\| \leq 1 \end{aligned}$$

Inversement : Supposons que l'on ait : $\forall\ n \in \mathbb{N} : \|n\| \leq 1$ et montrons que $\Bbbk$ est ultramétrique. ie.,

$$\forall\ x,\ y \in \Bbbk : \|x+y\| \leq \max\{\|x\|, \|y\|\}$$

* Si $y = 0$, alors

$$\|x+y\| = \|x\| \leq \max\{\|x\|, 0\}$$

* Si $y \neq 0$, il suffit de démontrer que

$$\forall\ x,\ y \in \Bbbk : \left\|\frac{x}{y} + 1\right\| \leq \max\left\{\left\|\frac{x}{y}\right\|, \|1\| = 1\right\}$$

ie.,

$$\forall\ x \in \mathbb{Q} : \|x+1\| \leq \max\{\|x\|, \|1\|\}$$

On a

$$\begin{aligned} \|x+1\|^n &= \|(x+1)^n\| \\ &= \left\|\sum_{k=0}^{n} C_n^k\ x^k\right\| \leq \sum_{k=0}^{n} \left\|C_n^k\right\| \cdot \|x^k\| \\ &\leq \sum_{k=0}^{n} \|x^k\| \ \text{ puisque } C_n^k \in \mathbb{N} \end{aligned}$$

* Si $\|x\| \leq 1$; alors $\|x\|^n \leq 1$, $\forall\, n \in \mathbb{N}$ et si $\|x\| > 1$; on a $\max\{\|x\|^n, 1\} = \|x\|^n$. On en conclut que

$$\|x+1\|^n \leq \sum_{k=0}^{n} \max\{\|x\|^n, 1\}$$

$$\Rightarrow \|x+1\|^n \leq (n+1)\max\{\|x\|^n, 1\}$$

$$\Rightarrow \|x+1\| \leq \sqrt[n]{n+1}\max\{\|x\|, \|1\|\}$$

$$\Rightarrow \|x+1\| \leq \max\{\|x\|, \|1\|\}$$

$$\Rightarrow \|.\| \text{ est une norme non archimédienne}$$

■

Définition 1.1.4 *(valuation p-adique)*
Soit p un nombre premier et soit $x \in \mathbb{N}^*$. On appelle valuation p-adique de x notée $V_p(x)$ le plus grand exposant de p tel que $p^{V_p(x)}$ divise x.
$V_p : \mathbb{N}^* \longrightarrow \mathbb{Z}_+$
$x \longmapsto V_p(x) = \max\{r \in \mathbb{Z}_+ : p^r/x\}$
* *On écrit*

$$x = p^{V_p(x)}.x' \text{ avec } (p, x') = 1$$

Remarque 1.1.5 1) *On pose par convention $V_p(0) = +\infty$.*
2) *Si $x = \frac{a}{b} \in \mathbb{Q}^*$; alors*

$$V_p(x) = V_p(a) - V_p(b)$$

Preuve. En effet

$$\frac{a}{b} \in \mathbb{Q}^* \Rightarrow (a,b) \in \mathbb{Z}^{*2}$$

$$\Longrightarrow \begin{cases} a = a_1.p^{V_p(a)}, (a_1, p) = 1 \\ b = b_1.p^{V_p(b)}, (b_1, p) = 1 \end{cases}$$

$$\Rightarrow \frac{a}{b} = \frac{a_1.p^{V_p(a)}}{b_1.p^{V_p(b)}} = \frac{a_1}{b_1}.p^{V_p(a)-V_p(b)} \text{ avec } (a_1, b_1, p) = 1$$

On en déduit que

$$V_p(x) = V_p(\frac{a}{b}) = V_p(a) - V_p(b)$$

■

Proposition 1.1.6 *Si $x, y \in \mathbb{Q}$. Alors la valuation V_p satisfait*

$$\begin{cases} 1) V_p(x.y) = V_p(x) + V_p(y) \\ 2) V_p(x+y) \geq \min\{V_p(x), V_p(y)\} \end{cases}$$

Preuve.

1) Soient $\begin{cases} x = p^{V_p(x)}.x' \\ y = p^{V_p(y)}.y' \end{cases}$ avec $\begin{cases} p \nmid x' \Rightarrow x' \neq k_1.p \\ p \nmid y' \Rightarrow y' \neq k_2.p \end{cases}$. Alors

$$x'.y' \neq k.p \ (k \in \mathbb{Z})$$

$$\Rightarrow x.y = x'.y'.p^{V_p(x)+V_p(y)} \text{ avec } p \nmid x'.y'$$

Ce qui donne

$$V_p(x.y) = V_p(x) + V_p(y)$$

2) Soient $x = p^r \frac{a}{b}$ et $y = p^s \frac{c}{d}$. Supposons que $r \leq s$; alors on a

$$\begin{aligned} V_p(x+y) &= V_p\left(p^r \frac{a}{b} + p^s \frac{c}{d}\right) \\ &= V_p\left(p^r \left[\frac{a}{b} + p^{s-r}\frac{c}{d}\right]\right) \\ &= V_p\left(p^r \left[\frac{da + p^{s-r}cb}{bd}\right]\right) \end{aligned}$$

Avec $p \nmid bd$. Donc

$$\begin{aligned} V_p(x+y) &= V_p(p^r) + V_p\left(\left[\frac{da + p^{s-r}cb}{bd}\right]\right) \geq r \\ &= \min\{V_p(x), V_p(y)\} \end{aligned}$$

ie.,

$$V_p(x+y) \geq \min\{V_p(x), V_p(y)\}$$

■

Exemple 1.1.7

$$V_p(n!) = \frac{n}{p-1} \text{ quand } n \longrightarrow \infty$$

En effet. On a

$$V_p(n!) = \frac{n - S_P(n)}{p-1} = \sum_{k \geq 1} \left[\frac{n}{k}\right]$$

où $S_P(n)$ *est la somme des chiffres de l'écriture de* n *dans la base* p *et* $\left[\frac{n}{k}\right]$ *est la partie entière de* $\frac{n}{k}$. *Donc*

$$\begin{aligned} V_p(n!) &\leq \frac{n}{p}\sum_{k\geq 1}\frac{1}{p^k} \\ &\leq \frac{n}{p}\frac{1}{1-\frac{1}{p}} \\ &\leq \frac{n}{p-1} \end{aligned}$$

$$\Rightarrow V_p(n!) \leq \frac{n}{p-1} \qquad (*)$$

D'autre part, on a

$$\begin{aligned} V_p(n!) &\geq \sum_{k=0}^{n}\frac{n}{p^k} - m \\ &\geq \frac{n}{p}\frac{1-\left(\frac{1}{p}\right)^m}{1-\left(\frac{1}{p}\right)} - m \\ &\geq \frac{n}{p-1} - \frac{np^{-m}}{p-1} - m \end{aligned}$$

Alors, on prend m *tel que* $p^m \leq n \leq p^{m+1}$ *; et d'après* $(*)$ *on aura*

$$\begin{aligned} \left|\frac{V_p(n!)}{n} - \frac{1}{p-1}\right| &\leq \frac{p^{-m}}{p-1} + \frac{m}{n} \\ &\leq p^{-m}\left(\frac{1}{p-1} + m\right) \longrightarrow 0 \text{ quand } m \longrightarrow +\infty \end{aligned}$$

On en déduit que, si $n, m \longrightarrow \infty$ *; alors*

$$\lim_{n\longrightarrow\infty}\frac{V_p(n!)}{n} = \frac{1}{p-1}$$

Enfin, on conclut que

$$V_p(n!) = \frac{n}{p-1} \text{ quand } n \longrightarrow +\infty$$

Définition 1.1.8 ***(norme p-adique)*** *Soit* p *un nombre premier. La norme p-adique de* x *notée* $\|x\|_p$ *est une application de* $\mathbb{Q}$ *vers* $\mathbb{R}_+$ *définie comme suit,*

$$\|.\|_p : \mathbb{Q} \longrightarrow \mathbb{R}_+$$

$$x \longmapsto \|x\|_p = \begin{cases} p^{-V_p(x)}, \text{ si } x \neq 0 \\ 0, \text{ si } x = 0 \end{cases}$$

Proposition 1.1.9 $\|.\|_p$ *est une norme ultramétrique sur* $\mathbb{Q}$.

Preuve. Il suffit de prouver l'inégalité triangulaire forte

$$\forall\, x, y \in \mathbb{Q} : \|x+y\|_p \leq \max\left\{\|x\|_p, \|y\|_p\right\}$$

* Si $x = 0$ ou $y = 0$, la dernière inégalité est triviale. Supposons que $x, y \neq 0$. Soient $x = \frac{a}{b}$, $y = \frac{c}{d}$. On a

$$x + y = \frac{ad+bc}{bd}$$

$$\Longrightarrow V_p(x+y) = V_p(ad+bc) - V_p(b) - V_p(d)$$

$$\begin{aligned} &= \min\left\{V_p(a) - V_p(b), V_p(c) - V_p(d)\right\} \\ &= \min\left\{V_p(x), V_p(y)\right\} \end{aligned}$$

On en déduit que

$$\begin{aligned} \|x+y\|_p = p^{-V_p(x+y)} &\leq \max\left\{p^{-V_p(x)},\ p^{-V_p(y)}\right\} \\ &= \max\left\{\|x\|_p, \|y\|_p\right\} \end{aligned}$$

Alors $\|.\|_p$ est une norme non archimédienne.

* L'application $\|.\|_p$ est appelée norme p-adique (valeur absolue p-adique). La distance sur $\mathbb{Q}$ induite par la norme p-adique $\|.\|_p$ est notée par d_p et définie par

$$d_p(x,y) = \|x-y\|_p$$

■

Exemple 1.1.10 *Pour la distance usuelle, on a* $|10-3| = 7$. *Tandis que pour la norme* $5-$*adique on a*

$$\|10-3\|_5 = \|7\|_5$$

Or $7 = 2 + 1.5$

$$\Rightarrow V_5(7) = 0$$

$$\Rightarrow \|7\|_5 = 5^{-0} = 1$$

Propriété importante : *La norme p-adique* $\|.\|_p$ *prend des valeurs discrètes, et on a*

$$\|\mathbb{Q}\|_p = \{0,\ p^n\ ;\ n \in \mathbb{Z}\}$$

* *Désignons maintenant par* $\|.\|_\infty$ *la valeur absolue usuelle sur* $\mathbb{Q}$. *Il est clair que* $\|.\|_\infty$ *est une norme archimédienne, et donc* $\mathbb{Z}$ *n'est pas bornée pour la distance usuelle* $d_{\|.\|_\infty}$ *sur* $\mathbb{R}$.

* *Si p est premier, tout entier n s'écrit sous la forme $n = p^r.m$ où $p \nmid m$ et r est la valuation p-adique de n. Donc*

$$\forall\, n \in \mathbb{Z} : \|n\|_p \leq p^{-r} \leq 1$$

Alors $\mathbb{Z}$ est bornée pour toute valeur absolue p-adique $\|.\|_p$.

Théorème 1.1.11 (***d'Ostowski***) *Toute valeur absulue non triviale $|.|$ sur $\mathbb{Q}$ est équivalente, soit à la valeur absolue usuelle $\|.\|_\infty$ soit à une valeur absolue p-adique $\|.\|_p$.*

Preuve. voir [19]. ■

Corollaire 1.1.12 *Deux valeurs absolues p-adiques $\|.\|_{p_1}$, $\|.\|_{p_2}$ sont équivalentes si et seulement si $p_1 = p_2$.*

1.1.1 Les nombres p-adiques

On sait que $\mathbb{R}$ est la complétion de $\mathbb{Q}$ par rapport la valeur absolue usuelle, et dans ce cas les éléments de $\mathbb{R}$ sont les classes d'équivalences des suites de Cauchy de $\mathbb{Q}$. La même procédure se fait pour une valeur absolue ultramétrique $\|.\|_p$. La complétion de $\mathbb{Q}$ par rapport cette valeur absolue $\|.\|_p$ donne un corps ultramétrique appelé corps des *nombres $p-adiques$* et se note $\mathbb{Q}_p$. Ainsi les éléments de $\mathbb{Q}_p$ sont les classes d'équivalences des suites de Cauchy dans $\mathbb{Q}$, muni de la relation suivante,

$$(a_n)\ R\ (b_n) \iff \lim_{n\longrightarrow\infty} \|a_n - b_n\|_p = 0$$

Remarque 1.1.13 *La valeur absolue $\|.\|_p$ peut être prolonger de $\mathbb{Q}$ sur tout $\mathbb{Q}_p$ de la façon suivante :*
Soit $x \in \mathbb{Q}_p$ et $(x_n)_{n\in\mathbb{N}}$ une suite de Cauchy dans $\mathbb{Q}$ de limite x pour la distance p-adique $d_{\|.\|_p}$; alors

$$\|x\|_p = \lim_{n\longrightarrow\infty} \|x_n\|_p$$

ie.,

$$\forall\, x \in \mathbb{Q}_p, \exists\, x_n \in \mathbb{Q} : x = \lim_{n\longrightarrow\infty} x_n$$

Proposition 1.1.14 $\left(\mathbb{Q}_p,\ \|.\|_p\right)$ *est un corps complet ultramétrique.*

1.1.2 Développement p-adique et séries de Hensel

On va montrer que tout élément a de $\mathbb{Q}_p$ admet une représentation canonique unique. Pour cela, on a besoin du lemme suivant.

Lemme 1.1.15 *Si $x \in \mathbb{Q}$ avec $\|x\|_p \leq 1$, alors*

$$\forall\, n \in \mathbb{N}\ ,\ \exists\, \alpha \in \mathbb{Z} : \|\alpha - x\|_p \leq p^{-n}$$

Preuve. Soient p un nombre premier et $x = \frac{a}{b}$ tels que : $(a,b) = (p,b) = 1$. On a

$$\begin{aligned} \|x\|_p &= p^{-V_p(x)} \leq 1 \\ &\Longrightarrow p^{-V_p(\frac{a}{b})} \leq 1 \\ &\Longrightarrow p^{V_p(b)-V_p(a)} \leq 1 \\ &\Longrightarrow \frac{p^{V_p(b)}}{p^{V_p(a)}} \leq 1 \end{aligned}$$

Et puisque $(p,b) = 1 \Rightarrow (p^n, b) = 1, \forall\, n \in \mathbb{N} \overset{\text{Bezout}}{\Longrightarrow} \exists\, m_1, m_2 \in \mathbb{Z} : m_1 b + m_2 p^n = 1$. Posons $\alpha = a.m_1$, alors $\alpha \in \mathbb{Z}$ et on a

$$\begin{aligned} \|\alpha - x\|_p &= \left\|\alpha - \frac{a}{b}\right\|_p \\ &= \left\|\frac{a}{b}\right\|_p . \|(m_1 b - 1)\|_p \\ &\leq \|(m_1 b - 1)\|_p = \|m_2 p^n\|_p \\ &\leq p^{-n} \end{aligned}$$

■

Théorème 1.1.16 *Si la classe d'équivalence $a \in \mathbb{Q}_p$ vérifie la condition $\|a\|_p \leq 1$. Alors elle possède un seul représentant $(a_n)_n$ qui satisfait*

$$\begin{cases} a_n \in \mathbb{Z},\ 0 \leq a_n < p^n \\ a_{n+1} \equiv a_n (\text{mod } p^{n+1}) \end{cases}$$

Preuve. Soit $a \in \mathbb{Q}_p$ tel que $\|a\|_p \leq 1$. D'après le lemme précédent, on a

$$\exists\, \alpha_0 \in \mathbb{Z} : \|\alpha_0 - a\|_p < 1 \text{ avec } 0 \leq \alpha_0 < p$$

On sait aussi que

$$\|\alpha_0 - a\|_p < \frac{1}{p}$$

$$\Longrightarrow \left(\frac{a-\alpha_0}{p}\right) \in \mathbb{Q}_p$$

Encore une fois, on applique le lemme précédent, pour trouver $\alpha_1 \in \mathbb{Z}$ tel que

$$\|a-(\alpha_0+\alpha_1 p)\|_p < p^{-1}\,;\, 0 \leq \alpha_1 < p$$

* Par itération, on obtient une suite d'entiers $(\alpha_n)_n$ telle que

$$\|a-(\alpha_0+\alpha_1 p+...+\alpha_n p^n)\|_p < p^{-n}\,;\, 0 \leq \alpha_n < p$$

Posons $a_n = \alpha_0+\alpha_1 p+...+\alpha_n p^n$. Alors $(a_n)_{n\in\mathbb{N}}$ est une suite qui satisfait

$$\begin{cases} a_n \in \mathbb{Z},\ 0 \leq a_n < p^n \\ a_{n+1} \equiv a_n (\text{mod } p^{n+1}). \text{ ie., une suite de Cauchy} \\ \|a-a_n\|_p < p^{-n} \\ \lim\limits_{n\longrightarrow\infty} \|a_n\|_p = \|a\|_p \end{cases}$$

■

Conclusion 1.1.17 *La suite de Cauchy $(a_n)_n$ qui vérifie les conditions précédentes s'appelle représentant canonique de a. ie.,*

$$\forall a \in \mathbb{Q}_p : \|a\|_p \leq 1 \Rightarrow \exists a_n \in \mathbb{Z} : a_n = \alpha_0+\alpha_1 p+...+\alpha_{n-1}p^{n-1}$$

Et de plus

$$a = \lim_{n\longrightarrow\infty} a_n = \sum_{n=0}^{\infty} \alpha_n p^n = .\alpha_0\alpha_1\ ...\alpha_s\ ...$$

* *Les α_j représentent les chiffres p-adiques et $\sum\limits_{n=0}^{\infty}\alpha_n p^n$ s'appelle la série de Hensel ou développement p-adique de a. Autrement dit, on peut approcher le nombre p-adique a par une série convergente unique S définie par*

$$S = \sum_{n=0}^{\infty} \alpha_n p^n$$

Démontrons l'unicité de la représentation. Si a admet deux développements p-adiques

$$\begin{aligned} a &= \sum_{n=0}^{\infty} \alpha_n p^n = \alpha_0+\alpha_1 p+...+\alpha_n p^n+... \\ a &= \sum_{n=0}^{\infty} \alpha'_n p^n = \alpha'_0+\alpha'_1 p+...+\alpha'_n p^n+... \end{aligned}$$

Soit d le premier entier tel que $\alpha_d \neq \alpha'_d$. Donc; on peut supposer que $\alpha_d < \alpha'_d$. On a

$$1 \leq \alpha'_d - \alpha_d \leq p-1$$

Posons $\beta_n = \alpha_0 + \alpha_1 p + ... + \alpha_n p^n$ et $\beta'_n = \alpha'_0 + \alpha'_1 p + ... \alpha'_n p^n$. On aura

$$\begin{aligned} \beta'_d - \beta_d &= (\alpha'_d - \alpha_d)\, p^d \\ &\Longrightarrow \quad \|\beta'_d - \beta_d\|_p = p^{-d} \end{aligned}$$

D'autre part, on a

$$\begin{aligned} \|\beta'_d - \beta_d\|_p &= \|\beta'_d - \alpha + \alpha - \beta_d\|_p \\ &\leq \max\left\{\|\beta'_d - \alpha\|_p, \|\alpha - \beta_d\|_p\right\} \end{aligned}$$

qui est une contradiction $\Longrightarrow$ d n'existe pas. On conclut donc que le développement p-adique est unique.

Conclusion 1.1.18 1) *Tout nombre p-adique a admet un développement p-adique sous forme d'une série convergente $a = \sum_{k=-m}^{\infty} \beta_k p^k$; $0 \leq \beta_k < p$.*
2) *Si $\beta_{-m} \neq 0$; alors $\|a\|_p = p^m$.*
3) *Le développement p-adique est analogue au développement décimal d'un nombre réel, puisque tout nombre réel x s'écrit sous la forme*

$$x = \sum_{k=-\infty}^{n} \theta_k 10^k$$

4) *On note par $[x]$ la partie entière d'un nombre p-adique $x \in \mathbb{Q}_p$, telle que*

$$\forall\ x \in \mathbb{Q}_p : [x] = \sum_{k=0}^{\infty} \beta_k p^k = .\beta_0 \beta_1 ... \beta_s ...$$

Et on note par $\langle x \rangle$ la partie fractionnaire de x, telle que

$$\forall x \in \mathbb{Q}_p : \langle x \rangle = \sum_{k<0} \beta_k p^k = ...\beta_{-3}\beta_{-2}\beta_{-1}.$$

Alors, pour tout x de $\mathbb{Q}_p$, on écrit : $x = [x] + \langle x \rangle$.

Définition 1.1.19 *On dit que a est un entier p-adique si son développement p-adique ne contient que des puissances positives de p. Autrement dit*

$$a = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + ... + \alpha_n p^n + ...$$

Notation 1.1.20 *On note par $\mathbb{Z}_p$ l'ensemble des entiers p-adiques .*

$$\mathbb{Z}_p = \left\{ a \in \mathbb{Q}_p : a = \sum_{n=0}^{\infty} \alpha_n p^n \right\}$$

Puisque dans le cas d'un entier p-adique a, $V_p(x)$ est positive, on a la caractérisation suivante

$$\mathbb{Z}_p = \left\{ a \in \mathbb{Q}_p : \|a\|_p = p^{-V_p(x)} \leq 1 \right\}$$

C'est-à-dire : $\mathbb{Z}_p$ représente le disque d'unité de rayon 1 et de centre 0.

Remarque 1.1.21 1) *Tout nombre p-adique $a \in \mathbb{Q}_p$ est une limite d'une suite de cauchy de nombres rationnels.*

2) *Le corps $\mathbb{Q}_p$ est l'ensemble des fractions de $\mathbb{Z}_p$. ie :*

$$\mathbb{Q}_p = \left\{ \frac{a}{b} \, ; \, (a,b) \in \mathbb{Z}_p . \mathbb{Z}_p^* \right\}$$

Définition 1.1.22 *(unité p-adique) Soit $a \in \mathbb{Q}_p$, on dit que a est unitaire ou inversible si $a \in \mathbb{Z}_p$ et le premier chiffre est différent de zéro. On note par $\mathbb{Z}_p^*$ (ou U_p) l'ensemble des unités p-adiques.*

$$U_p = \left\{ \sum_{n=0}^{\infty} \alpha_n p^n, \; \alpha_0 \neq 0 \right\} = \{ a \in \mathbb{Z}_p \, ; \, \alpha_0 \neq 0 \}$$

* *U_p est un groupe multiplicatif, et on a le théorème suivant.*

Théorème 1.1.23

$$U_p = \left\{ a \in \mathbb{Z}_p \, ; \; \|a\|_p = 1 \right\}$$

Preuve. Puisque $a \in U_p \implies a = \alpha_0 + \alpha_1 p + ... + \alpha_n p^n + ...$ Alors $V_p(\alpha) = 0$, ce qui implique que

$$\|a\|_p = p^{-0} = 1$$

■

1.1.3 Propriétés analytiques des nombres p-adiques

Généralement les Propriétés analytiques de $\mathbb{Q}_p$ sont analogues à celles de $\mathbb{R}$, mais la différence remarquable entre ses deux corps réside dans les critères de convergence des suites et des séries de puissances.

Théorème 1.1.24 *Soit $(a_n)_{n\in\mathbb{N}}$ une suite de $\mathbb{Q}_p$; alors $(a_n)_{n\in\mathbb{N}}$ est une suite de Cauchy et par conséquent convergente si et seulement si*

$$\lim_{n\longrightarrow\infty} \|a_{n+1} - a_n\|_p = 0 \qquad (*)$$

Preuve. Si $(a_n)_{n\in\mathbb{N}}$ est une suite de Cauchy, alors $\lim_{\substack{m\longrightarrow\infty \\ n\longrightarrow\infty}} \|a_m - a_n\|_p = 0$. En particulier, pour $m = n+1$ ce qui démontre $*$.

Inversement, Supposons que $\lim_{n\longrightarrow\infty} \|a_{n+1} - a_n\|_p = 0$, par conséquent on en déduit que

$$\forall\, \varepsilon > 0, \exists\, N \in \mathbb{N}\ ; \forall\, n \geq N : \|a_{n+1} - a_n\|_p \leq \varepsilon$$

Prenons $m > n \geq N$ et examinons $\|a_m - a_n\|_p$. On a

$$\|a_m - a_n\|_p = \|a_m - a_{m-1} + a_{m-1} - a_{m-2} + a_{m-2} - \ldots - a_n\|_p$$

$$\leq \max\left\{\|a_m - a_{m-1}\|_p, \|a_{m-1} - a_{m-2}\|_p, \ldots, \|a_{n+1} - a_n\|_p\right\} < \varepsilon$$

On en déduit donc que $(a_n)_{n\in\mathbb{N}}$ est une suite de Cauchy.

Voici maintenant une caractérisation des séries qui distingue les corps $\mathbb{Q}_p$ et $\mathbb{R}$. ∎

Proposition 1.1.25 *Soit $\sum_{n=0}^{\infty} a_n$ une série dans $\mathbb{Q}_p$; alors*

1) $\sum_{n=0}^{\infty} a_n$ *converge dans* $\mathbb{Q}_p \iff \lim_{n\longrightarrow\infty} a_n = 0.$

2) $\left\|\sum_{n=0}^{\infty} a_n\right\|_p \leq \max_{n\geq 0}\left\{\|a_n\|_p\right\}.$

Preuve.

1) *On sait que la série $\sum_{n=0}^{\infty} a_n$ converge si la suite des sommes partielles $S_n = \sum_{i=0}^{n} a_i$ converge. On a $S_n - S_{n-1} = a_n$; et d'après le théorème* (1.1.24), *la série $\sum_{n=0}^{\infty} a_n$ converge si et seulement si a_n tend vers* 0.

2) *Supposons que $\sum_{n=0}^{\infty} a_n$ converge. Puisque $a_n \longrightarrow 0$; alors*

$$\exists\, N \in \mathbb{N} : \left\|\sum_{n=0}^{\infty} a_n\right\|_p = \left\|\sum_{n=0}^{N} a_n\right\|_p \text{ et } \max\left\{\|a_n\|_p, 0 \leq n \leq N\right\} = \max_{n\geq 0}\left\{\|a_n\|_p\right\}$$

D'où

$$\left\|\sum_{n=0}^{N} a_n\right\|_p \leq \max\left\{\|a_n\|_p, 0 \leq n \leq N\right\} = \max_{n\geq 0}\left\{\|a_n\|_p\right\}$$

∎

Remarque 1.1.26 *Dans $\mathbb{R}$ la deuxième implication est généralement fausse.*

Exemple 1.1.27 *La série harmonique* $\sum_{n=1}^{\infty} \frac{1}{n}$ *est divergente pourtant son terme général tend vers* 0.

Théorème 1.1.28 *(de Strassman) Soit* $F(x) = \sum_{n=0}^{\infty} a_n\, x^n \in \mathbb{Q}_p[x]$ *une série entière non nule. C'est-à-dire : une série telle qu'il existe au moins un* $a_n \neq 0$. *Supposons que* $\lim_{n \longrightarrow +\infty} a_n = 0$, *alors* $F(x)$ *converge pour tout* x *de* $\mathbb{Z}_p$. *De plus ; si* $N \in \mathbb{N}$ *est défini par*

$$\begin{cases} i)\ \|a_N\|_p = \max\limits_{n \geq 0} \left\{ \|a_n\|_p \right\} \\ ii)\ \|a_n\|_p < \|a_N\|_p\ ,\ pour\ n \succ N \end{cases}$$

Alors $F(x) : \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ *admet au plus* N *zéros.*

Preuve. Raisonons par récurrence. Si $N = 0$, notre hypothèse signifie que pour tout $n > 0$, on a $\|a_0\|_p > \|a_n\|_p$. On va montrer que dans ce cas $F(x)$ n'admet aucune racine dans $\mathbb{Z}_p$. Supposons le contraire. ie : $F(x) = a_0 + a_1x + ... + ... = 0$. On en déduit que

$$\|a_0\|_p = \left\|a_1x + a_2x^2 + ... + ...\right\|_p \leq \max_{n \geq 1} \left\{ \|a_n\|_p \right\}$$

$$< \|a_0\|_p$$

qui est une contradiction (puisque $x \in \mathbb{Z}_p \implies \|x\|_p \leq 1$). Donc $F(x)$ n'admet aucune racine dans $\mathbb{Z}_p$.

Supposons maintenant que $N > 0$ et que les deux hypothèses du théorème sont satisfaites. ie.,

$$\|a_N\|_p = \max_{n \geq 0} \left\{ \|a_n\|_p \right\} \text{ et } \|a_n\|_p < \|a_N\|_p\ , \text{ pour } n > N$$

Montrons que $F(x)$ admet au plus N zéros dans $\mathbb{Z}_p$. Soit $\alpha \in \mathbb{Z}_p$ tel que $F(\alpha) = 0$, alors

$$\forall\ x \in \mathbb{Z}_p : F(x) = F(x) - F(\alpha) = \sum_{n=0}^{\infty} a_n \left(x^n - \alpha^n\right)$$

$$= (x - \alpha) \sum_{n \geq 1} \sum_{j=0}^{n-1} a_n x^j \alpha^{n-1-j}$$

Posons $k = n - j - 1 \implies n = j + k + 1$ et en remplaçant dans l'expression précédente, on aura

$$F(x) = (x - \alpha) \sum_{j=0}^{\infty} b_j x^j = (x - \alpha)\, g(x) \text{ où } b_j = \sum_{k=0}^{\infty} a_{j+1+k} \alpha^k$$

On a

$$\|b_j\|_p \leq \max \left\{ \|a_{j+1+k}\|_p \right\} \leq \|a_N\|_p\ ;\ \forall\ j = o, ..., \infty$$

De plus

$$\|b_{N-1}\|_p = \left\|a_N + a_{N+1}\alpha + a_{N+2}\alpha^2 + ... + ...\right\|_p = \|a_N\|_p$$

* Si $j > N$, on a

$$\|b_j\|_p \leq \max_{k\geq 0}\left\{\|a_{j+1+k}\|_p\right\} \leq \max_{j\geq N+1}\left\{\|a_j\|_p\right\} < \|a_N\|_p$$

On en déduit que b_{N-1} a une norme maximale. Alors le nombre magique de $g(x)$ est $N-1$. Par hypothèse de récurrence g admet au plus $N-1$ zéros, et par conséquent $F(x)$ admet au plus N zéros. ■

1.2 Nombres algébriques

1.2.1 Corps de nombres algébriques

Définition 1.2.1 *Soit $\mathbb{k}$ un sous-corps de $\mathbb{C}$. On dit que $\mathbb{k}$ est un corps de nombres si considéré comme espace vectoriel sur $\mathbb{Q}$, il est de dimension finie d. Cette dimension s'appelle le degré de $\mathbb{k}$ et se note $[\mathbb{k} : \mathbb{Q}] = d$.*

Définition 1.2.2 *Soit $\alpha \in \mathbb{C}$. On dit que α est un nombre algébrique s'il existe un polynôme $P \in \mathbb{Z}[x]$ non nul tel que $P(\alpha) = 0$.*

Exemple 1.2.3 *1) $\alpha = \frac{1}{\sqrt{2}}$ est algébrique car $2\alpha^2 - 1 = 0$.*
2) $\beta = 1 + \sqrt[3]{5}$ est algébrique puisque β vérifie $(\beta-1)^3 - 5 = \beta^3 - 3\beta^2 + 3\beta - 6 = 0$.

Remarque 1.2.4 *Dans le cas particulier, si $\deg(P) = 2$ et $\Delta \neq 0$ alors α est dit irrationnel quadratique.*
Par exemple le nombre d'or $\Phi = \frac{1}{2}\left(1+\sqrt{5}\right)$ est irrationnel quadratique puisqu'il vérifie l'équation $x^2 - x - 1 = 0$. D'une façon générale tout nombre irrationnel quadratique est de la forme

$$x = \alpha + \beta\sqrt{d}$$

où $\alpha, \beta \in \mathbb{Q}$ et $d \in \mathbb{Z}$ n'est pas un carré parfait.

Définition 1.2.5 *Soit $a = \alpha + \beta\sqrt{d}$ un irrationnel quadratique, le nombre $\alpha - \beta\sqrt{d}$ est appelé le conjugué de a et se note a^*.*

Proposition 1.2.6 *On peut vérifier facilement les propriétés suivantes.*
1)*Si* $a = \alpha + \beta\sqrt{d}$ *est un irrationnel quadratique, alors* $\frac{1}{\alpha}$ *l'est également et on a* $\left(\frac{1}{\alpha}\right)^* = \frac{1}{\alpha^*}$.
2)*Si* α *est irrationnel quadratique et* $r \in \mathbb{Q}$ *; alors* $r + \alpha$ *est irrationnel quadratique. De plus, on a* $(r+\alpha)^* = r + \alpha^*$.
$*$ *Soit* α *un nombre algébrique et* $P \neq 0$ *un polynôme de* $\mathbb{Z}[x]$ *de dégré minimal tel que* $P(\alpha) = 0$. *En divisant* P *par le coéfficient de son terme de plus haut dégré, on obtient un polynôme unitaire* $P_\alpha \in \mathbb{Q}[x]$ *qui vérifie* $p_\alpha(\alpha) = 0$.

Définition 1.2.7 *le polynôme de dégré minimal* P_α *s'appelle le polynôme minimal de* α.

Remarque 1.2.8 *le polynôme minimal* P_α *est unique.*

Définition 1.2.9 *Soit* $P(x)$ *un polynôme. Le corps partagé de* $P(x)$ *est le plus petit corps où* $P(x)$ *peut être décomposé en facteurs linéaires.*

Définition 1.2.10 *Le dégré du polynôme minimal* P_α *du nombre algébrique* α *s'appelle le dégré de* α *et se note* $\deg(\alpha)$.

Exemple 1.2.11 1)*Si* $\alpha \in \mathbb{Q}$, *alors* α *est un nombre algébrique de dégré* 1, *et de polynôme minimal* $(x - \alpha)$.
2)*Si* a *est irrationnel quadratique, alors* a *est algébrique de dégré* 2 *et de polynôme minimal* $(x-a)(x-a^*)$.

Notation 1.2.12 *Soit* $\alpha \in \mathbb{C}$ *un nombre algébrique de dégré* d. *On pose*

$$\Bbbk = \mathbb{Q}(\alpha) = \left\{a_0 + a_1\alpha + \ldots + a_{d-1}\alpha^{d-1}\ ;\ a_0\ ,\ a_1, \ldots,\ a_{d-1} \in \mathbb{Q}\right\}$$

Exemple 1.2.13 1) $\alpha = 1 \Rightarrow \Bbbk = \mathbb{Q}$ *est un corps de nombres algébriques de dégré* $d = 1$.
2) *Si* $\alpha = \sqrt{d}$ *où* $d \in \mathbb{Z}$ *est sans facteur carré ; alors* $\Bbbk = \mathbb{Q}\left(\sqrt{d}\right)$ *est un corps de nombres algébriques appelé corps quadratique de dégré* 2. *De plus* $\Bbbk$ *s'écrit sous la forme*

$$\Bbbk = \mathbb{Q}\left(\sqrt{d}\right) = \left\{a + b\sqrt{d};\ a,\ b \in \mathbb{Q}\right\}$$

$*$ *Si* $d > 0$ *; alors* $\Bbbk$ *est dit quadratique réel et si* $d < 0$ *;* $\Bbbk$ *est dit quadratique imaginaire.*

1.2.2 Entiers algébriques

Définition 1.2.14 *Soit α un nombre algébrique. On dit que α est un entier algébrique s'il est entier ou si son polynôme minimal P_α est à coéfficients entiers. Autrement dit s'il existe $a_0, a_1, ..., a_{d-1} \in \mathbb{Z}$ tels que*

$$\alpha^d + a_{d-1}\alpha^{d-1} + ... + a_1\alpha + a_0 = 0$$

Exemple 1.2.15 *i)* $\sqrt{2}$ *est un entier algébrique puisqu'il est racine du polynôme* $x^2 - 2$. *ii) Le nombre d'or* $\Phi = \frac{1}{2}\left(1 + \sqrt{5}\right)$ *et* $\omega = e^{\frac{2i\pi}{p}}$ *sont aussi des entiers algébriques puisque ses polynômes minimals sont* $x^2 - x - 1$ *(respectivement* $x^{p-1} + x^{p-2} + ... + x + 1$*).*

Remarque 1.2.16 *L'ensemble des entiers de* $\mathbb{k}$ *est un anneau qui s'appelle l'anneau des entiers de* $\mathbb{k}$ *et se note* $A_\mathbb{k}$.

Théorème 1.2.17 *Soit* $\mathbb{k} = \mathbb{Q}\left(\sqrt{d}\right)$ *un corps de nombres quadratiques, alors l'ensemble* $A_\mathbb{k}$ *des entiers de* $\mathbb{k}$ *est un sous-anneau de* $\mathbb{k}$. *De plus, on a*
i) Si $d \equiv 2$ *ou* $3 (\text{mod } 4)$, *alors*

$$\begin{aligned} A_\mathbb{k} &= \left\{x \in \mathbb{k};\ x = \alpha + \beta\sqrt{d} \text{ tel que } \alpha, \beta \in \mathbb{Z}\right\} \\ &= \mathbb{Z}\left(\sqrt{d}\right) \end{aligned}$$

ii) Si $d \equiv 1 (\text{mod } 4)$, *alors*

$$\begin{aligned} A_\mathbb{k} &= \left\{x \in \mathbb{k};\ x = \frac{\alpha + \beta\sqrt{d}}{2} \text{ où } \alpha, \beta \in \mathbb{Z} \text{ et } \alpha, \beta \text{ de même parité}\right\} \\ &= \mathbb{Z}\left(\frac{1 + \sqrt{d}}{2}\right) \end{aligned}$$

Preuve. pour la preuve, voir [16] ∎

Définition 1.2.18 *(symbole de Legendre) Soit* $p \in \mathbb{N}$ *un nombre premier. On définit le symbole de Legendre pour tout entier* n *par*

$$\begin{cases} \left(\frac{n}{p}\right) = 0, \text{ si } n \equiv 0 (\text{mod } p) \\ \left(\frac{n}{p}\right) = 1, \text{ si } n \not\equiv 0 (\text{mod } p) \text{ et est un carré modulo } p \\ \left(\frac{n}{p}\right) = -1, \text{ si } n \not\equiv 0 (\text{mod } p) \text{ et } n \text{ n'est pas un carré modulo } p \end{cases}$$

Exemple 1.2.19 *i)* $\left(\frac{2}{7}\right) = 1$ *car* $2 \equiv 3^2 \pmod 7$.

ii) $\left(\frac{3}{7}\right) = -1$ *car les seuls carrés modulo* 7 *sont* 0, 1, 2, 4.

Critère d'Euler :

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} (\text{mod } p)$$

Exemple 1.2.20 $\left(\frac{7}{11}\right) \equiv 7^5 (\text{mod } 11)$. *D'autre part* $7^5 \equiv -1 (\text{mod } 11)$ *et donc* 7 *n'est pas un carré modulo* 11.

Corollaire 1.2.21 *Le symbole de Legendre est multiplicatif. Autrement dit*

$$\left(\frac{m.n}{p}\right) = \left(\frac{m}{p}\right).\left(\frac{n}{p}\right) \text{ pour tout nombre premier } p$$

En effet.

$$\left(\frac{m.n}{p}\right) \equiv (m.n)^{\frac{p-1}{2}} \equiv m^{\frac{p-1}{2}}.n^{\frac{p-1}{2}} (\text{mod } p) \equiv \left(\frac{m}{p}\right).\left(\frac{n}{p}\right) (\text{mod } p)$$

Il suffit donc de savoir calculer $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ *et* $\left(\frac{p}{q}\right)$ *pour tout nombre premier impair* p.

On remarque que l'expression de $\left(\frac{-1}{p}\right)$ *découle directement du critère d'Euler*

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} (\text{mod} p)$$

ie : $\left(\frac{-1}{p}\right) = 1$ *si* $p = 4k+1$ *et* $\left(\frac{-1}{p}\right) = -1$ *si* $p = 4k-1$.

1.3 Suites linéaires récurrentes

Dans cette dernière partie, on va aborder succintement la définition et les propriétés des suites linéaires récurretes, tout en s'intéressant à des cas particuliers qui servent de modèles pour l'étude qui viendra aux autres chapitres.

1.3.1 Généralités

Définition 1.3.1 *Soit* $(x_n)_{n\in\mathbb{N}}$ *une suite définie sur un corps de nombres algébriques* $\mathbb{k}$. $(x_n)_{n\in\mathbb{N}}$ *est dite linéaire récurrente d'ordre* k *si elle vérifie une relation de récurrence de la forme*

$$x_n = a_1 x_{n-1} + a_2 x_{n-2} + \ldots + a_k x_{n-k}; \forall n \geq k \qquad (1.3.1)$$

avec $a_1, a_2, \ldots, a_k \in \mathbb{k}$ *et* $a_k \neq 0$. *Les termes* $x_0, x_1, \ldots, x_{k-1}$ *sont appelés les conditions initiales.*

Exemple 1.3.2 1) *Si $k = 1$; la suite $(x_n)_{n\in\mathbb{N}}$ est de la forme : $x_n = a\, x_{n-1}$. Et, dans ce cas la suite $(x_n)_{n\in\mathbb{N}}$ est géométrique de raison a et de terme initial x_0. Le terme général de $(x_n)_{n\in\mathbb{N}}$ est donné par $x_n = x_0.a^n$*
2) *Si $k = 2$; alors $(x_n)_{n\in\mathbb{N}}$ est de la forme*

$$x_n = a_1 x_{n-1} + a_2 x_{n-2}$$

C'est une suite linéaire récurrente du second ordre.

1.3.2 Polynôme caractéristique

Définition 1.3.3 *Soit $(x_n)_{n\in\mathbb{N}}$ une suite linéaire récurrente vérifiant la relation* (1.3.1). *Le polynôme*

$$P(x) = x^k - a_1 x^{k-1} - a_2 x^{k-2} - \ldots - a_k$$

s'appelle le polynôme caractéristique de la suite $(x_n)_{n\in\mathbb{N}}$.

Remarque 1.3.4 1) *Une suite linéaire récurrente non homogène est une relation de récurrence de la forme*

$$x_{n+k} = a_1 x_{n+k-1} + a_2 x_{n+k-2} + \ldots + a_k x_n + a_{k+1}$$

où a_1, a_2,..., a_{k+1} sont des nombres algébriques. Une telle suite vérifie la relation de récurrence homogène

$$x_{n+k+1} = (a_1 + 1)\, x_{n+k} + \sum_{i=1}^{k-1} (a_{i+1} - a_i)\, x_{n+k-i} - a_{k+1} x_n$$

d'ordre $k+1$ et de polynôme caractéristique

$$f(x) = \left(x^k - a_1 x^{k-1} - a_2 x^{k-2} - \ldots - a_k\right)(x - 1)$$

2) *La connaissance des conditions initiales x_0, x_1,..., x_{k-1} peut déterminer tous les autres termes de la suite. De plus si a_k est inversible dans le corps $\mathbb{k}$, la suite peut être continuer dans le sens opposé et on peut donc trouver les valeurs : x_{-1}, x_{n-2} , ...*

Proposition 1.3.5 *Etant donné un polynôme f défini sur un corps de nombres $\mathbb{k}$. Considérons l'ensemble $L(f)$ de toutes les suites linéaires récurrentes satisfaisant* (1.3.1) *et $L^*(f)$ de*

toutes les suites linéaires récurrentes telles que f soit leurs polynôme caractéristique. Alors on peut vérifier aisément les propriétés suivantes.

$*$ Si g est un diviseur de f, alors $L(g) \subset L(f)$.

$*$Si f est irréductible, alors $L^*(f)$ contient toutes les suites de $L(f)$ sauf la suite nule.

Théorème 1.3.6 *Soient f, g deux polynômes définis sur un corps $\mathbb{k}$, on a*

i) Si $(a_n)_n \in L(f)$, $(b_n)_n \in L(g)$, alors

$$(c_n)_n = (a_n)_n + (b_n)_n \in L(p.p.c.m(f,g))$$

ie : la somme de deux suites linéaires récurrentes est encore linéaire récurrente.

ii) $L(f) \cap L(g) = L(p.g.c.d(f,g))$.

iii) $L(f) \subset L(g) \iff f$ divise g.

Remarque 1.3.7 *Si $d_n = a_n.b_n$ avec $(a_n)_n \in L(f)$, $(b_n)_n \in L(g)$. Alors $(d_n)_n$ est aussi une suite linéaire récurrente, mais il est très laborieux de déterminer son polynôme caractéristiqe.*

Conclusion 1.3.8 *D'une façon générale, on peut montrer que les suites linéaires récurrentes vérifient les axiomes d'un anneau unitaire commutatif. ie : l'ensemble des suites linéaires récurrentes est un anneau, commutatif et unitaire.*

1.3.3 Quelques suites linéaires récurrentes particulières

On a vu que la suite géométrique est une suite linéaire récurrente de terme général $x_n = x_0\, a^n$, par ailleurs les grandes recherches concernant les suites linéaires récurrentes sont portées sur les suites d'ordre *deux* et troix. Dans cette section, on va rappeler quelques célèbres suites linéaires récurrentes qui ont été considérées comme point de départ de la plupart des études sur les suites.

Suite de Fibonacci :

C'est une suite définie pour la première fois par le mathématicien italien Leonardo Fibonacci en 1202. Elle est notée F_n et définie par $F_0 = 0$, $F_1 = 1$ et $F_n = F_{n-1} + F_{n-2}$ pour tout $n \geq 2$. Son polynôme caractéristique est $P(x) = x^2 - x - 1$ et ses racines sont $\alpha_1 = \frac{1+\sqrt{5}}{2}; \alpha_2 = \frac{1-\sqrt{5}}{2}$. De plus, on pourra démontrer (voir chapitre 3) que son terme général est donné par :

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right) - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)$$

Suites de Lucas :

Ce sont des suites linéaires récurrentes d'ordre *deux* de la forme

$$u_{n+2} = Mu_{n+1} - Nu_n \text{ où } M, N \text{ sont des entiers relatifs}$$

* La suite de Lucas du premier type est définie par $u_0 = 0$, $u_1 = 1$.
* La suite de Lucas du deuxième type est définie par $u_0 = 2$; $u_1 = M$.

Suites de Lehmer :

Ce sont des suites linéaires récurrentes d'ordre *deux* définie par la formule

$$u'_{n+2} = \mp\sqrt{M}u'_{n+1} - Nu'_n; \forall n \geq 0 \text{ avec } N \in \mathbb{Z} \text{ et } M \in \mathbb{N}$$

La suite de Lehmer du premier type est définie par les valeurs initiales $u'_0 = 0$, $u'_1 = 1$. Celle du deuxième type est donnée par les valeurs initiales $u'_0 = 2$, $u'_1 = \pm\sqrt{M}$.

1.3.4 Multiplicité d'une suite linéaire récurrente

Définition 1.3.9 *Soit $(x_n)_n$ une suite linéaire récurrente et soit d un nombre algébrique. La multiplicité de d est le nombre d'indices n tels que $x_n = d$.*

Notation 1.3.10 *La multiplicité du nombre d est notée $m(d)$. La multiplicité de la suite $(x_n)_n$ est alors définie par*

$$m = \max_{d \in \mathbb{k}} m(d)$$

L'étude de cette multiplicité sera l'objet du deuxième chapitre.

Chapitre 2

Multiplicité des suites linéaires récurrentes entières d'ordre deux

Après que nous avons défini les différentes notions de nombres algébriques et de suites linéaires récurrentes, on va consacrer le présent chapitre à l'étude du problème de la multiplicité des suites linéaires récurrentes non dégénérées d'ordre deux à termes entiers du fait de la diversité de ses applications.

Pour bien gérer notre étude on va la partager en deux parties. La première concerne une étude de la multiplicité en s'appuyant sur des arguments p-adiques, et l'autre est une étude basée sur des arguments algébriques inspirée essentiellement des derniers travaux de *Beukers* [5], *Schlickewei* [26] et *Schmidt* [28] qui ont donné une bonne amélioration de la borne supérieure de la multiplicité d'une suite linéaire récurrente en prouvant que pour une suite linéaire récurrente entière d'ordre deux on a $m(d) + m(-d) \leq 3$ mieux que la conjecture de Morgan Ward qui a désigné que 5 est la borne supérieure de la multiplicité.

2.1 Multiplicité des suites linéaires récurrentes binaires en arguments p-adiques

2.1.1 Suites linéaires récurrentes non dégénérées

Définition 2.1.1 *Soit* $(a_n)_{n\in\mathbb{N}}$ *une suite linéaire récurrente entière d'ordre deux satisfaisant la relation*

$$a_{n+2} = Ma_{n+1} - Na_n \text{ où } M, N \text{ des entiers fixés et } |a_0| + |a_1| \neq 0 \qquad (2.1.1)$$

Soit $P(x) = x^2 - Mx + N$ le polynôme caractéristique de $(a_n)_{n\in\mathbf{N}}$. Si au moins une des racines de $P(x)$ ou le quotient des deux racines de $P(x)$ est une racine de l'unité; alors $(a_n)_{n\in\mathbf{N}}$ est dite "dégénérée". Dans tous les autres cas, on dit qu'elle est "non – dégénérée".
***Rappel** : on rappelle que la multiplicité d'un nombre algébrique d dans une suite linéaire récurrente $(a_n)_{n\in\mathbf{N}}$ définie sur un corps algébrique K est le nombre de solutions de l'équation : $a_n = d$. Et donc la multiplicité de $(a_n)_{n\in\mathbf{N}}$ notée $M(a_n)$ est définie par*

$$M(a_n) = \sup_{d\in\mathbf{k}} m(d)$$

Remarque 2.1.2 *Si une suite linéaire récurrente entière d'ordre deux est dégénérée, alors sa multiplicité $M(a_n)$ peut être infinie.*

Exemple 2.1.3 *La suite linéaire récurrente définie par $a_{n+2} = a_{n+1} - a_n$; $a_0 = 0$, $a_1 = 1$ consiste au répétition des nombres $0, 1, 1, 0, -1, -1$. Et donc*

$$m(0) = m(1) = m(-1) = \infty$$

**Par contre la multiplicité de toute suite linéaire récurrente non-dégénérée d'ordre deux est finie.*

2.1.2 Multiplicité des suites linéaires récurrentes non dégénérées

Dans les années trente, *Morgan Ward* a conjecturé que la multiplicité d'une suite linéaire récurrente entière non dégénérée d'ordre deux est au plus 5. Dans le cas particulier si $(M, N) = 1$, la multiplicité est au plus 4. L'objet de cette section est de démontrer cette conjecture en utilisant des méthodes p-adiques. Dans l'étude qui suive le discréminant $\Delta = M^2 - 4N$ joue un rôle important.

Théorème 2.1.4 *Soient $(a_n)_{n\in\mathbf{N}}$ une suite linéaire récurrente entière d'ordre deux vérifiant (2.1.1) et $(V_n)_{n\in\mathbf{N}}$ la suite de Lucas du deuxième type qui vérifie (2.1.1) avec $V_0 = 2$, $V_1 = M$. Alors pour tout $k > 0$ et $0 \leq i < k$, la sous-suite $(a_{kn+i})_{n\in\mathbf{N}}$ est linéaire récurrente d'ordre deux et vérifie la relation de récurrence*

$$a_{k(n+2)+i} = V_K a_{k(n+1)+i} - N^K a_{kn+i}$$

Preuve. Soit $\mathbb{Q}\left(\sqrt{\Delta}\right)$ un corps quadratique et soit $E = \mathbb{Q}\left(\sqrt{\Delta}\right).\mathbb{Q}\left(\sqrt{\Delta}\right)$ un espace vectoriel de dimension deux sur $\mathbb{Q}$ défini par les deux opérations :

1) $\forall (r,s),(t,u) \in \mathbb{Q}\left(\sqrt{\Delta}\right)$:

$$\begin{aligned}(r,s)+(t,u) &= \left(r+s\sqrt{\Delta}\right)+\left(t+u\sqrt{\Delta}\right)\\ &= \left((r+t)+(s+u)\sqrt{\Delta}\right)\\ &= ((r+t),(s+u))\end{aligned}$$

2)$\forall (r,s),(t,u) \in \mathbb{Q}\left(\sqrt{\Delta}\right)$:

$$\begin{aligned}(r,s).(t,u) &= \left(r+s\sqrt{\Delta}\right).\left(t+u\sqrt{\Delta}\right)\\ &= (rt+\Delta su, st+ru)\end{aligned}$$

Définissons les fonctions multiplicatives

$$\overline{(r,s)} = (r,-s) \text{ et } N(r,s) = (r,s).\overline{(r,s)} = r^2-\Delta s^2$$

On peut facilement vérifier l'identité

$$(r,s).\left(\frac{t}{2},\frac{u}{2}\right)^2 = t(r,s)\left(\frac{t}{2},\frac{u}{2}\right)-\left[\left(\frac{t^2-u^2\Delta}{4}\right)(r,s)\right] \tag{2.1.2}$$

Posons $c = 2a_1 - a_0M$ et définissons une autre suite $(d_n)_{n\in\mathbb{N}}$ par

$$(d_n,a_n) = (c,a_0).\left(\frac{M}{2},\frac{1}{2}\right)^n \tag{2.1.3}$$

On peut vérifier aisément par récurrence que $(d_n)_{n\in\mathbb{N}}$ est linéaire récurrente satisfaisant (2.1.1) avec

$$d_0 = c \text{ et } d_1 = \frac{cM+\Delta a_0}{2}$$

En effet. Pour $n = 0$; on a

$$(d_0,a_0) = (c,a_0) \implies d_0 = c$$

pour $n = 1$, on aura

$$(d_1,a_1) = (c,a_0)\left(\frac{M}{2},\frac{1}{2}\right)^1 = \left[\frac{cM+\Delta a_0}{2}+\left(\frac{c}{2}+\frac{Ma_0}{2}\right)\sqrt{\Delta}\right]$$

$$\Rightarrow d_1 = \frac{cM+\Delta a_0}{2} \text{ et } a_1 = \left(\frac{c}{2}+\frac{Ma_0}{2}\right) = a_1-\frac{a_0M}{2}+\frac{a_0M}{2} = a_1$$

Calculons maintenant d_{n+1}. On a

$$(d_{n+1},a_{n+1}) = (c,a_0)\left(\frac{M}{2},\frac{1}{2}\right)^{n+1}$$

$$= (c, a_0)\left(\frac{M}{2}, \frac{1}{2}\right)^{n-1}\left(\frac{M}{2}, \frac{1}{2}\right)^2$$

Et en utilisant (2.1.2) ; on obtient

$$(d_{n+1}, a_{n+1}) = M(d_{n-1}; a_{n-1})\left(\frac{M}{2}, \frac{1}{2}\right) - \frac{M^2 - \Delta}{4}(d_{n-1}, a_{n-1})$$

$$\Rightarrow (d_{n+1}, a_{n+1}) = M(d_n, a_n) - N(d_{n-1}, a_{n-1})$$

$$\Rightarrow \begin{cases} d_{n+1} = Md_n - Nd_{n-1};\ n \geq 1 \\ a_{n+1} = Ma_n - Na_{n-1};\ n \geq 1 \end{cases}$$

En particulier, les suites $(b_n)_n$ et $(V_n)_n$ qui satisfont (2.1.1) avec $b_0 = 0$, $b_1 = 1$; $V_0 = 2$ et $V_1 = M$ satisfont aussi la relation suivante

$$(V_n, b_n) = (2, 0)\left(\frac{M}{2}, \frac{1}{2}\right)^n \tag{2.1.4}$$

Par (2.1.2) et la relation

$$\frac{V_K^2 - b_k^2\Delta}{4} = N\left(\frac{V_k}{2}, \frac{b_k}{2}\right) = N\left(\frac{M}{2}, \frac{1}{2}\right)^k = N^k$$

Il s'ensuit que la suite $(a_{kn+i})_{n\in\mathbb{N}} = (e_n)_{n\in\mathbb{N}}$ satisfait

$$e_{n+2} = V_k e_{n+1} - N^k e_n$$

En effet,

$$\left(d_{k(n+2)+i}, a_{k(n+2)+i}\right) = (c, a_0)\left(\frac{M}{2}, \frac{1}{2}\right)^{kn+i+2k}$$

$$= (c, a_0)\left(\frac{M}{2}, \frac{1}{2}\right)^{kn+i}\left[\left(\frac{M}{2}, \frac{1}{2}\right)^k\right]^2$$

$$= (d_{kn+i}, a_{kn+i})\left(\frac{V_k}{2}, \frac{b_k}{2}\right)^2$$

$$= V_k(d_{kn+i}, a_{kn+i})\left(\frac{V_k}{2}, \frac{b_k}{2}\right) - \frac{V_K^2 - b_k^2\Delta}{4}(d_{kn+i}, a_{kn+i})$$

$$= V_k\left(\frac{M}{2}, \frac{1}{2}\right)^k(d_{kn+i}, a_{kn+i}) - N^k(d_{kn+i}, a_{kn+i})$$

$$= V_k\left(d_{k(n+1)+i}, a_{k(n+1)+i}\right) - N^k(d_{kn+i}, a_{kn+i})$$

$$\Rightarrow e_{n+2} = a_{k(n+2)+i} = V_k a_{k(n+1)+i} - N^k a_{kn+i}$$

$$\Rightarrow e_{n+2} = V_k e_{n+1} - N^k e_n$$

ie., la suite $(a_{kn+i})_{n\in\mathbb{N}}$ est linéaire récurrente vérifiant (2.1.1). ■

Théorème 2.1.5 *Soit $(a_n)_{n\in\mathbb{N}}$ une suite linéaire récurrente non-dégénérée d'ordre deux satisfaisant (2.1.1) avec $(a_0, a_1) = 1$. On a*
1) Si $M^2 - 4N > 0$, alors la multiplicité de $(a_n)_{n\in\mathbb{N}}$ est au plus 3.
2) Si p est premier tel que $0 < V_p(M^2) < V_p(N)$, alors la multiplicité de $(a_n)_{n\in\mathbb{N}}$ est au plus 2.
3) Si $M^2 - 4N < 0$ et s'il existe un diviseur premier $p \geq 5$ de $M^2 - 4N$ qui ne divise ni M ni $2a_1 - a_0M$, alors la multiplicité de $(a_n)_{n\in\mathbb{N}}$ est bornée supérieurement par $p - 1$.
4) Si $M^2 - 4N <$

Théorème 2.1.6 *+++0 et s'il existe un diviseur premier $p \geq 5$ qui ne divise pas M tel que $V_p(2a_1 - a_0.M) \geq V_p(M^2 - 4N)$, alors la multiplicité de $(a_n)_{n\in\mathbb{N}}$ est bornée supérieurement par 2.*

Preuve. pour la preuve voir [12]. ■

Théorème 2.1.7 *Soit $(V_n)_{n\in\mathbb{N}}$ (respectivement $(u_n)_{n\in\mathbb{N}}$) les suites de Lucas satisfaisant (2.1.1) avec $V_0 = 2$; $V_1 = M = 1$ (respectivement $u_0 = 2$; $u_1 = M = -1$). Si $N \neq 0, 1$; alors,*
i) L'équation $V_n = -1$ n'a pas de solutions $n \in \mathbb{N}$ et l'équation $V_n = 1$ n'a pas de solutions $n \neq 1$ sauf si $N = 2$ et $n = 4$.
ii) L'équation $u_n = -1$ a seulement la solution $n = 1$ et l'équation $u_n = 1$ a seulement la soiution $(N = 2, n = 4)$.

Preuve. les résultats concernant $(V_n)_{n\in\mathbb{N}}$ sont démontrés par P. Chowla, Dunton et Lewis[11]. Ceux concernant $(u_n)_{n\in\mathbb{N}}$ se déduisent de $(V_n)_{n\in\mathbb{N}}$ puisque $u_n = (-1)^n V_n$. ■

2.1.3 Multiplicité dans Le cas $(a_0,a_1)=1$

Théorème 2.1.8 *[1] Soit A_1 (respectivement A_2) la suite $(a_n)_{n\in\mathbb{N}}$ vérifiant (2.1.1) avec $(a_0, a_1) = 1$, $N = 2$ et $M = 1$ (respectivement $N = 2$, $M = -1$). Alors A_1 (respectivement A_2) est de multiplicité ≤ 3 (respectivement ≤ 4).*

Preuve. *Pour* $\Delta < 0$. *Posons* $f = \sqrt{\Delta}$ *et travaillons dans l'anneau* $\mathbb{Q}\left(\sqrt{\Delta}\right)$. *Par la relation* (2.1.3) *de la preuve du théorème* (2.1.4) ; *on aura*

$$a_n = \frac{1}{2f}\left\{(c+a_0 f)\left(\frac{M+f}{2}\right)^n - (c-a_0 f)\left(\frac{M-f}{2}\right)^n\right\} \tag{2.1.5}$$

En developpant par la formule du binôme, on obtient

$$a_n\left(\frac{4}{\Delta}\right)^{\frac{n-1}{2}} = \frac{1}{2}\sum_{j=0}^{\infty}\left\{cC_n^{2j} + a_0 M C_n^{2j+1}\right\}\left(\frac{M^2}{\Delta}\right)^j \text{ ; si } n \text{ est impair} \tag{2.1.6}$$

$$a_n\left(\frac{4}{\Delta}\right)^{\frac{n}{2}} = \sum_{j=0}^{\infty}\left\{a_0 C_n^{2j} + \frac{c\,M}{\Delta}C_n^{2j+1}\right\}\left(\frac{M^2}{\Delta}\right)^j, \text{ si } n \text{ est pair} \tag{2.1.7}$$

Si $c = 2a_1 - a_0$; *alors on voit que* A_1 *est donnée par*

$$a_n = \frac{1}{2^n}\sum_{j=0}^{\infty}\left\{a_0 C_n^{2j} + cC_n^{2j+1}\right\}(-7)^j \tag{2.1.8}$$

Donc $(a_0, c) = 1$ *et pour* $0 \le i \le 2$; *on peut réécrire* (2.1.8) *comme suit*

$$\begin{aligned} a_{3t+i} &= \left(\frac{1}{2^i}\right)(1+7)^t\left\{a_0 + c\,(3t+i) - a_0 7C_{3t+i}^2 - 7c\;C_{3t+i}^3 + 7^2 G(t)\right\} \\ &= \left(\frac{1}{2^i}\right)\left\{a_0 + c\;(3t+i) - 7a_0 C_{3t+i}^2 + 7a_0 t + 7c\;(3t+i)\,t + 7^2 D(t)\right\} \quad (2.1.9) \end{aligned}$$

Où $G(t)$, $D(t)$ *sont des séries de puissances 7-adiques. Considérons maintenant l'équation* $a_n = k$ *où* $k \not\equiv 0 \pmod 7$.

1) *Si* $7 \nmid c$; *alors* (2.1.9) *donne un polynôme linéaire et d'après le théorème de Strassman [chapitre 1], il y a au plus* 7 *solutions pour chaque* i=0, 1, 2.

2) *Si* $7/c$, *alors* $7 \nmid a_0$ *et* (2.1.9) *modulo* 49 *contient un terme de la forme* $-a_0\frac{3t^2}{2}$. *Alors par le théorème de Strassman, il existe au plus* 2 *solutions de l'équation* $a_n = k$ *pour chaque classe de congruence modulo* 3.

∗*De plus* (2.1.9) *modulo* 7 *donne* $k \equiv \left(\frac{1}{2^i}\right)a_0 \pmod 7$. *Et donc toutes les solutions appartiennent au même classe d'équivalence modulo* 3. *Alors,*

i) Si $k \not\equiv 0 \pmod 7$; *on aura*

$$m(k) \le 3$$

ii) Si $7/k$ *et puisque* $(c, a_0) = 1$, *alors l'équation* $a_n = k$ *implique que* $7 \nmid c$. *En appliquant le théorème de Strassman à l'équation* (2.1.9), *on conclut qu'il existe au plus une solution de* $a_n = k$ *dans chaque classe de congruence modulo* 3, *ce qui achève la preuve concernant* A_1.

Pour démontrer les résultats de A_2, on peut distinguer deux cas.

1) *Si* $2/a_0a_1$ *et en utilisant* (2.1.1), *on peut démontrer par récurrence que*

$$a_{n+2} \equiv a_{n+1} \equiv a_1 (\text{mod } 2)$$

En effet: Puisque $a_{n+2} = Ma_{n+1} - Na_n = -a_{n+1} - 2a_n$. *Donc, pour* $n = 0$ *; on a*

$$a_2 \equiv -a_1 (\text{mod } 2)$$

$$\Rightarrow a_2 \equiv -a_1 + 2a_1 (\text{mod } 2)$$

$$\Rightarrow a_2 \equiv a_1 (\text{mod } 2)$$

Supposons que $a_{k+2} \equiv a_1 (\text{mod } 2)$, *pour* $0 \leq k \leq n-1$. *Alors, on obtient*

$$a_{n+2} = -a_{n+1} - 2a_n \equiv -a_{n+1} \equiv a_{n+1} \equiv a_1 (\text{mod } 2)$$

Il s'ensuit donc que

$$m(a_0) = 1$$

2) *Si* $2 \nmid a_0a_1$, *alors en examinant toutes les possibilités pour* a_0 *et* a_1 *modulo* 8, *on voit que les solutions de* $a_n = a_0$ *appartiennent au plus à* 4 *différentes classes d'équivalences modulo* 6. *Il est clair que* A_2 *satisfait la relation suivante*

$$a_n = -\left(\frac{-1}{2}\right)^n \sum_{i=0}^{\infty} \left\{cC_n^{2i+1} - a_0C_n^{2i}\right\} (-7)^i \qquad (2.1.10)$$

Alors. i) Si $7 \nmid c$, *en appliquant le théorème de Strassman à toute sous-suite* (a_{6t+r}) $(r = 0, 1, ..., 5)$ *de* A_2 *on voit qu'il existe au plus une solution de* $a_n = a_0$ *dans chaque classe d'équivalence modulo* 6. *D'où*

$$m(a_0) \leq 4$$

ii) Si $7/c$ *et donc* $7 \nmid a_0$, *alors* (2.1.10) *modulo* 7 *donne*

$$a_0 \equiv a_0 \left(\frac{-1}{2}\right)^n (\text{mod } 7)$$

Qui signifie que toute solution de l'équation $a_n = a_0$ *appartient à une seule classe d'équivalence modulo* 6. *D'autre part, en réduisant* (2.1.10) *modulo* 49 *et en appliquant le théorème de Strassman on déduit que*

$$m(a_0) \leq 2$$

Théorème 2.1.9 *Soit $(a_n)_{n\in\mathbb{N}}$ une suite linéaire récurrente non dégénérée satisfaisant*

$$a_{n+2} = Ma_{n+1} - Na_n$$

avec $N \neq \pm 1$ et $(a_0, a_1) = 1$. Alors, on a

$-$Si $M = 1$ les solutions de $a_n = a_0$ avec $n \succ 0$ appartiennent à la même classe d'équivalence modulo N.

$-$Si $M = -1$ et $N \neq \pm 1, \pm 2$, alors les solutions de $a_n = a_0$ avec $n \succ 0$ sont toutes de même parité.

Preuve. *Si $M = 1$, il est facile de vérifier que, pour $n \geq 2$; on a*

$$a_n \equiv a_1 - (a_0 + (n-2)\,a_1)\,N \pmod{N^2} \tag{2.1.11}$$

En effet. Pour $n = 2$, on a $a_2 = a_1 - Na_0 \equiv a_1 - (a_0 + (2-2)\,a_1)\,N \pmod{N^2}$. Supposons maintenant que

$$a_k \equiv a_1 - (a_0 + (k-2)\,a_1)\,N \pmod{N^2}; 2 \leq k \leq n$$

On a

$$a_{n+1} = a_n - Na_{n-1}$$

$$\begin{aligned}
&\Rightarrow \quad a_{n+1} \equiv ((a_1 - (a_0 + (n-2)\,a_1)\,N - N(a_1 - (a_0 + (n-3)\,a_1)\,N)) \pmod{N^2}\\
&\Rightarrow \quad a_{n+1} \equiv a_1 - (a_0 + (n-2+1)\,a_1)\,N \pmod{N^2}\\
&\Rightarrow \quad a_{n+1} \equiv a_1 - (a_0 + (n-1)\,a_1)\,N \pmod{N^2}
\end{aligned}$$

Donc par induction, on conclut que ; $\forall n \geq 2 : a_n \equiv a_1 - (a_0 + (n-2)\,a_1)\,N \pmod{N^2}$.

i) Si $a_0 = a_1 = \pm 1$; alors $a_n = a_0$ implique

$$a_0 \equiv a_1 - (a_0 + (n-2)\,a_1)\,N \equiv a_1 - (n-1)\,a_1 N \pmod{N^2}$$

Il ressort que $n \equiv 1 \pmod{N}$ et toutes les solutions appartiennent à cette classe.

ii) Si $a_0 \neq a_1$ et $a_n = a_m = a_0$, pour $n \geq 2$. Alors (2.1.11) donne

$$\begin{aligned}
&a_1 - (a_0 + (n-2)\,a_1)\,N \equiv a_1 - (a_0 + (m-2)\,a_1)\,N \pmod{N^2}\\
\Rightarrow \quad &(n-m)\,a_1 \equiv 0 \pmod{N}
\end{aligned}$$

De plus, si $(a_1, N) = 1$, alors $n \equiv m \pmod{N}$. ie : n, m appartiennent au même classe de congruence modulo N. C.Q.F.D

– Si $(a_1, N) \neq 1$. Soit q un facteur premier de (a_1, N). Puisque $a_{n+2} = a_{n+1} - Na_n$ et q/N, on aura

$$a_{n+2} \equiv a_{n+1} \pmod{q}$$

Et par récurrence $a_n \equiv a_1 \equiv 0 \pmod{q}$. Et puisque $q \nmid a_0$, il n'existe pas de solutions $n \neq 0$ de l'équation $a_n = a_0$ et alors la première assertion est démontrée.

**) Si $M = -1$; on peut montrer par induction que*

$$a_n \equiv (-1)^n (-a_1) \pmod{N};\ \forall\ n \geq 1$$

En effet. pour $n = 1$, on aura

$$a_1 = (-1)(-a_1) \Rightarrow a_1 \equiv a_1 \pmod{N}$$

Supposons que la propriété est vraie jusqu'à l'ordre n. ie., $a_n \equiv (-1)^n (-a_1) \pmod{N}$, et montrons qu'elle est vraie pour l'ordre $n+1$. On a

$$a_{n+1} = -a_n - Na_{n-1} \equiv -a_n \pmod{N} \equiv (-1)^{n+1}(-a_1) \pmod{N}$$

Par induction ; on conclut que $a_n \equiv (-1)^n (-a_1) \pmod{N}$; $\forall\ n \geq 1$.

** Maintenant si $a_r = a_{2s+1} = a_0$, alors*

$$a_0 \equiv a_1 \equiv (-a_1) \pmod{N} \Rightarrow 2a_0 \equiv 0 \pmod{N} \text{ et } 2a_1 \equiv 0 \pmod{N}$$

Ce qui donne

$$2a_0 = kN \text{ et } 2a_1 = k'N$$

$$\Rightarrow k'a_0 = ka_1 \Rightarrow a_0/k \text{ (puisque } (a_0, a_1) = 1)$$

$$\Rightarrow k = \alpha.a_0 \text{ avec } \alpha \in \mathbb{Z}$$

En remplaçant dans la relation $2a_0 = kN$; on obtient $N/2$ qui est une contradiction (puisque $N \neq \pm 1, \pm 2$). On en déduit donc que les solutions sont de même parité. ■

■

2.1.4 Critère de multiplicité

Théorème 2.1.10 (*Laxton*)[21] *Soit $(a_n)_{n\in\mathbb{N}}$ une suite linéaire récurrente non dégénérée satisfaisant* (2.1.1) *et soit q le plus petit naturel pair tel que $r_1^q \equiv r_2^q \equiv 1 \pmod 4$ où r_1, r_2 sont les racines du polynôme caractéristique $x^2 - Mx + N$. On a*

i) Si $r_1,\ r_2 \in \mathbb{Z}_2$, *alors la multiplicité de* $(a_n)_{n\in\mathbb{N}}$ *est au plus* 4.
ii) Si $r_1,\ r_2 \notin \mathbb{Z}_2$, *alors pour tout* k *de* $\mathbb{Z}$ *; l'équation* $a_n = k$ *a au plus deux solutions dans chaque classe d'équivalence modulo* q. *De plus, s'il existe deux distinctes classes d'équivalences* $u \pmod q$ *et* $v \pmod q$ *contenant chacune deux solutions, alors* $u - v \equiv \frac{q}{2} \pmod q$.

Lemme 2.1.11 *[1] Soit* $(a_n)_{n\in\mathbb{N}}$ *une suite linéaire récurrente non dégénérée satisfaisant*

$$\forall n \geq 0 : a_{n+2} = 2Ma_{n+1} - Na_n \tag{2.1.12}$$

avec $(a_0, a_1) = 1$ *;* $2 \nmid Na_0$ *,* $M \neq 0$ *et* $M^2 - 4N \prec 0$. *Alors*
i) Si M *est impair et* $N \equiv 3 \pmod 4$, *on a*

$$m(a_0) \leq 3$$

(respectivement si M *impair et* $N \equiv 1 \pmod 4$*), on a*

$$m(a_0) \leq 4$$

ii) Si M *est pair et* $N \equiv 1 \pmod 4$, *alors*

$$m(a_0) \leq 3$$

(respectivement M *pair et* $N \equiv 3 \pmod 4$*), on aura*

$$m(a_0) \leq 4$$

Preuve. *Puisque* $M^2 - 4N \prec 0$, *alors,* r_1, r_2 *sont complexes conjuguées et donc* $\frac{r_1}{r_2}$ *n'est pas une racine de l'unité. De plus* r_1, r_2 *ne sont pas des racines de l'unité (puisque si* r_i $(i = 1, 2)$ *est une racine de l'unité), alors* $r_i = \pm 1$ *et* $M^2 - 4N \geq 0$, *qui est une contradiction. Par suite on peut appliquer le théorème de Laxton. Les racines du polynôme caractéristique sont* $r_i = M \pm (M^2 - N)^{\frac{1}{2}}$, $i = 1, 2$ *qui donne*

$$r_i^2 = 2M^2 - N \pm 2M\left(M^2 - N\right)^{\frac{1}{2}} \tag{2.1.13}$$

i) Si M *est impair, alors* $r_i^2 \equiv 1 + \left(1 - N \pm 2M\left(M^2 - N\right)^{\frac{1}{2}}\right) \pmod 4$ *et puisque* N *est impair, on a deux cas.*
−Si $N \equiv 1 \pmod 4$, *l'entier* q *du théorème de Laxton est* 2. *On en déduit que la multiplicité de* $(a_n)_{n\in\mathbb{N}}$ *notée* $M(a_n)$ *est telle que*

$$M(a_n) \leq 4 \ (les\ r_i \in \mathbb{Z}_2)$$

$-Si\ N \equiv 3 (\mathrm{mod}\ 4)$, alors $M^2 - N \equiv 2 (\mathrm{mod}\ 4)$ et on conclut donc que $r_i^2 \not\equiv 1 (\mathrm{mod}\ 4)$. D'autre part

$$r_i^4 = \left(2M^2 - N\right)^2 + 4M^2\left(M^2 - N\right) \pm 4M\left(2M^2 - N\right)\left(M^2 - N\right)^{\frac{1}{2}}$$

$$\Rightarrow r_i^4 \equiv \left(2M^2 - N\right)^2 \equiv 1 \ (\mathrm{mod}\ 4)$$

Et dans ce cas le q du théorème de Laxton est 4. D'après (.12) on voit que modulo 4 la suite $(a_n)_{n\in\mathbb{N}}$ est telle que $a_n \equiv a_0,\ a_1,\ 2+a_0,\ 2+a_1,\ a_0,\ a_1,\ 2+a_0,\ 2+a_1 ... (\mathrm{mod}\ 4)$. Donc par le théorème de Laxton, la multiplicité est au plus 3.

ii) Supposons maintenant que M est pair. Et comme précédemment, on distingue deux cas.

$-Si\ N \equiv 3\ (\mathrm{mod}\ 4)$, alors d'après (2.1.13) on a $r_i^2 \equiv 1 (\mathrm{mod}\ 4)$. ie., le q du théorème de Laxton est 2. Ainsi la multiplicité $M(a_n)$ est telle que $M(a_n) \leq 4$.

$-Si\ N \equiv 1\ (\mathrm{mod}\ 4)$, alors par (2.1.13) on aura $r_i^4 \equiv 1 (\mathrm{mod}\ 4)$. ie., $q = 4$. De plus, on voit que modulo 4, $(a_n)_{n\in\mathbb{N}}$ est congrue aux valeurs suivantes $a_0,\ a_1,\ 3a_0,\ 3a_1,\ a_0,\ a_1,\ 3a_0,\ 3a_1 ...$ et par conséquent le théorème de Laxton implique que $M(a_n) \leq 3$.

Lemme 2.1.12 *Soit $(a_n)_{n\in\mathbb{N}}$ une suite linéaire récurrente non dégénérée satisfaisant la relation (2.1.1) avec $(a_0, a_1) = 1$ et $2 \nmid M.N$. Alors la multiplicité de $(a_n)_{n\in\mathbb{N}}$ est bornée supérieurement par 5. ie., $M(a_n) \leq 5$.*

■

Preuve. *il est simple de vérifier que $r_i^6 \equiv 1\ (\mathrm{mod}\ 4)$; $i = 1,\ 2$ où $r_1,\ r_2$ sont les racines du polynôme caractéristique $x^2 - Mx + N$.*

En effet ; on a $r_i = \frac{M \pm \left(M^2 - 4N\right)^{\frac{1}{2}}}{2}$, et par suite

$$r_i^2 = \frac{\left(2M^2 - 4N\right) \pm 2M\left(M^2 - 4N\right)^{\frac{1}{2}}}{4}$$

$$\Rightarrow r_i^4 = \frac{\left(2M^2 - 4N\right)^2 + 4M^2\left(M^2 - 4N\right) \pm 4M\left(2M^2 - 4N\right)\left(M^2 - 4N\right)^{\frac{1}{2}}}{16}$$

$$\Rightarrow 2r_i^2 \equiv (1 - 2N) \pm M\left(M^2 - 4N\right)^{\frac{1}{2}}$$

De plus, on a

$$2r_i^4 \equiv (3 - 4N) \pm M\left(M^2 - 2N\right)\left(M^2 - 4N\right)^{\frac{1}{2}}$$

Et puisque N, M sont impairs ; alors

$$(1 - 2N) \equiv 3\ (\mathrm{mod}\ 4)\ ;\ \left(M^2 - 2N\right) \equiv 3\ (\mathrm{mod}\ 4)\ et\ \left(M^2 - 4N\right) \equiv 1\ (\mathrm{mod}\ 4)$$

$$\Rightarrow 4r_i^6 \equiv ((9+3) \pm (9+3)M)\ (\mathrm{mod}\ 4)$$

$$\Rightarrow 4r_i^6 \equiv \pm 12M \equiv \pm 4M\ (\mathrm{mod}\ 4)$$

i) Si $M \equiv 1 \pmod 4$, *on aura* $4M \equiv 4 \pmod{16}$. *ie.,* $4r_i^6 \equiv 4 \pmod{16}$. *En divisons tous les membres par* 4 *; on aura*

$$r_i^6 \equiv 1 \pmod 4$$

ii) Si $M \equiv 3 \equiv -1 \pmod 4$, *on en déduit que* $-4M \equiv 4 \pmod{16}$. *Alors d'une façon analogue ; on aura*

$$r_i^6 \equiv 1 \pmod 4$$

On en déduit que le q *du théorème de Laxton est ou bien* 2 *ou bien* 6. *Le cas* $q = 2$ *est traité précédemment. Il suffit donc de considérer le cas* $q = 6$. *Examinons la suite* $(a_n)_{n\in\mathbb{N}}$ *modulo* 4 *suivant les différents cas de* M, N.

1) *Si* $M \equiv -N \equiv 1 \pmod 4$ *; alors* $(a_n)_{n\in\mathbb{N}}$ *est congru à* 1, 1, 2, 3, 1, 0 (mod 4).

2) *Si* $M \equiv N \equiv 1 \pmod 4 \Rightarrow (a_n)_{n\in\mathbb{N}}$ *modulo* 4 *est une répétition des valeurs* 1, 1, 0, 3, 3, 0 *ou* 1, 3, 2, 3, 1, 2

3) *Si* $M \equiv -N \equiv -1 \pmod 4 \Rightarrow (a_n)_{n\in\mathbb{N}}$ *modulo* 4 *est une répétition des valeurs* 1, 1, 2 *ou* 1, 3, 0.

4) *Si* $M \equiv N \equiv 3 \pmod 4 \Rightarrow (a_n)_{n\in\mathbb{N}}$ *est congrue à* 1, 1, 0, 1, 3, 2. ∎

Conclusion 2.1.13 *– Dans les trois premier cas, pour tout* $d \in \mathbb{Z}$, *l'équation* $a_n = d$ *admet des solutions appartenant au plus à trois classes d'équivalences modulo* 6.
Pour le dernier cas les solutions de $a_n = d$ *appartiennent au plus à* 4 *classes d'équivalences modulo* 6. *Par suite, on en déduit que dans tous les cas, la multiplicité* $M(a_n)$ *est telle que*

$$M(a_n) \leq 5$$

Théorème 2.1.14 *Soit* $(a_n)_{n\in\mathbb{N}}$ *une suite récurrente linéaire non dégénérée satisfaisant* (2.1.1) *avec* $6 \nmid N$. *Alors, la multiplicité* $M(a_n)$ *est ou bien infinie, ou bien bornée supérieurement par* 5.

Preuve. *Supposons de plus que* $(a_0, a_1) = 1$. *Si* $2 \nmid N$, *alors le résultat est une conséquence des lemmes* (2.1.11) *et* (2.1.12). *Il suffit donc de supposer que* $2/N$ *et* $3 \nmid N$ *et d'appliquer le théorème de Laxton avec* $p = 3$.
Soit r_1, r_2 *les racines du polynôme caractéristique* $x^2 - Mx + N$ *de* $(a_n)_{n\in\mathbb{N}}$. *Si* $r_1, r_2 \in \mathbb{Z}_3$, *alors* $M^2 - 4N$ *est un carré* 3*-adique et comme* $3 \nmid N$, *on aura* $3/M$ *et* $N \equiv 2 \pmod 3$. *Alors ; il suffit de démontrer que*

$$m(a_0) \leq 5$$

∗ *Supposons que* $3/a_0$, *alors* $3 \nmid a_1$ *et comme* $3/M$, *on obtient*

$$a_{n+2} \equiv -Na_n \equiv a_n \pmod 3$$

Qui signifie que toutes les solutions de $a_n = a_0$ sont paires. Le polynôme caractéristique de $(a_{2n})_{n\in\mathbb{N}}$ est

$$x^2 - \left(M^2 - 2N\right)x + N^2$$

De plus $M^2 - 2N \not\equiv 0 \pmod 3$, qui implique que $r_1, r_2 \notin \mathbb{Z}_3$ (contradiction). Donc il suffit de traiter le cas $r_i \notin \mathbb{Z}_3$ $(i = 1, 2)$. En examinant les différents cas de M, N modulo 3 et en appliquant le théorème de Laxton, on obtient les résultats suivants :

** Si $d(N, M.q)$ est le nombre maximal des classes d'équivalences modulo q qui contient chacune une solution de l'équation $a_n = a_0$; on trouve*

$$d(1,0,4) = 2 \text{ et } d(1,1,6) = d(1,2,3) = d(2,1,8) = d(2,2,8) = 3$$

■

2.1.5 Le cas (M,N)=1

Théorème 2.1.15 *Soit $(a_n)_{n\in\mathbb{N}}$ une suite linéaire récurrente non dégénérée satisfaisant (2.1.1) avec $(M, N) = 1$, alors la multiplicité de $(a_n)_{n\in\mathbb{N}}$ est ou bien infinie ou bien bornée supérieurement par 4.*

Preuve. Il suffit de montrer que $m(a_0)$ est soit *infinie*, soit bornée supérieurement par 4 si $(a_0, a_1) = 1$. Par le théorème (2.1.5) (assertion (1)) il suffit de considérer le cas $a_0 \neq 0$ et $M^2 - 4N < 0$. Et d'après le lemme (2.1.11), il suffit de démontrer le théorème pour M impair.

Supposons que q est premier tel que q/M et q/a_0. Alors

$$q \nmid c = 2a_1 - a_0 M$$

D'autre part, en traitant (2.1.6) modulo q, on conclut que $a_n = a_0$ n'a pas de solution impaire. Alors la multiplicité $m(a_0)$ de a_0 dans $(a_n)_{n\in\mathbb{N}}$ est la même que sa multiplicité dans $(a_{2n})_{n\in\mathbb{N}}$. D'autre part, on sait que $(a_{2n})_{n\in\mathbb{N}}$ satisfait la relation de récurrence

$$\begin{aligned} a_{2(n+2)} &= V_2\, a_{2(n+1)} - N^2\, a_{2n} \\ &\Rightarrow a_{2(n+2)} = \left(M^2 - 2N\right) a_{2(n+1)} - N^2 a_{2n} \end{aligned}$$

où $(V_n)_{n\in\mathbb{N}}$ est la suite de Lucas du deuxième type. Le polynôme caractéristique de $(a_{2n})_{n\in\mathbb{N}}$ est

$$x^2 - \left(M^2 - 2N\right)x + N^2$$

* Si on recommence ce processus avec un diviseur premier de $(M^2 - 2N)$; on constate que si l'équation $a_n = a_0$ a des solutions $n \neq 0$, alors ou bien ce processus se termine après un nombre fini d'étapes, ou bien on obtient la relation de récurrence suivante :

$$a_{n+2} = \pm a_{n+1} - N a_n$$

* Puisque $M^2 - 4N \prec 0$, alors on peut supposer que $N \succ 0$. Selon les valeurs de N, on distingue trois cas.

i) Si $N = 1$, le polynôme caractéristique est $x^2 \pm x + 1 = 0$, et ses racines sont des racines de l'unité. Donc par [12], on conclut que

$$M(a_n) \leq 4$$

ii) Si $N = 2$, le résultat se déduit du théorème (2.1.8).

iii) Si $N > 2$, le lemme (2.1.11) nous permet de remplacer $(a_n)_{n\in\mathbb{N}}$ soit par $(a_{Nn+i})_{n\in\mathbb{N}}$, soit par $(a_{2n+i})_{n\in\mathbb{N}}$ (i un entier fixé). Il reste alors à démontrer que la nouvelle suite a une multiplicité, ou bien infinie ou bien bornée supérieurement par 4. La nouvelle suite peut être traiter par les méthodes précédentes. Son polynôme caractéristique est $x^2 - V_N\, x + N^N$ (respectivement $x^2 - V_2 x + N^2$). Comme précédemment, on peut choisir un diviseur premier de V_N ou de V_2. Mais dans ce cas le processus doit se terminer.

■

2.2 Suites linéaires récurrentes d'ordre deux en arguments algébriques

Dans cette partie, on va investir les suites linéaires récurrentes d'ordre deux non dégénérées à termes rationnels. Les résultats fondamentaux de cette section sont dûs à *Beukers* [5] ; [7] et *Tijdeman* [30]. On va établir dans la suite un résultat de *Beukers* qui indique que pour toute suite linéaire récurrente non dégénérée rationnelle d'ordre deux et $\omega \in \mathbb{Q}$, on a $m(\omega) + m(-\omega) \leq 3$.

2.2.1 Multiplicité des suites linéaires récurrentes rationnelles

Soit $(a_n)_{n\in\mathbb{N}} \subset \mathbb{Q}$ une suite linéaire récurrente non dégénérée satisfaisant

$$\forall n \geq 2 : a_n = c_1 a_{n-1} + c_2 a_{n-2} \qquad (2.2.1)$$

avec c_1, $c_2 \in \mathbb{Z}$, et si $s \in \mathbb{Z}$ est le plus petit dénominateur commun à a_0 et a_1, alors :
1) $(sa_n)_{n\geq 0} \subset \mathbb{Z}$ et la $d-$multiplicité de $(a_n)_{n\in\mathbb{N}}$ est équivalente à la $sd-$multiplicité de $(sa_n)_{n\geq 0}$ avec $d \in \mathbb{Q}$, qui signifie que notre étude peut se réstreindre au cas des suites entières. De plus, on a
2)$\forall\ n \geq 0 : (a_0, a_1)\ /a_n$ et donc on peut supposer que $(a_0, a_1) = 1$ et $a_0 \geq 0$.
3) Puisque la suite donnée par $u_n = (-1)^n a_n$, $\forall n \geq 0$ vérifie la relation de récurrence

$$u_n = -c_1 u_{n-1} + c_2 u_{n-2}\ ;\ \forall\ n \geq 2$$

Alors, on peut supposer que $c_1 \geq 0$ et de plus, on a

$$\{n \geq 0 : a_n = \pm a_0\} = \{n \geq 0 : u_n = \pm u_0\}$$

Avant de donner les théorèmes fondamentaux de cette partie, on a besoin des lemmes suivants.

Lemme 2.2.1 *Soit $(a_n)_{n\in\mathbb{N}} \subset \mathbb{Z}$ une suite linéaire récurrente non dégénérée satisfaisant*

$$a_n = c_1 a_{n-1} + c_2 a_{n-2}$$

Avec c_1, $c_2 \in \mathbb{Z}$, et soient α_1, α_2 les racines du polynôme caractéristique $x^2 - c_1 x - c_2$. Posons $\lambda_1 = a_1 - a_0\alpha_2$ et $\lambda_2 = a_1 - a_0\alpha_1$, alors

$$\forall\ n \geq 0 : a_n = \frac{\lambda_1 \alpha_1^n - \lambda_2 \alpha_2^n}{\alpha_1 - \alpha_2}$$

Preuve. Ce résultat se démontre par récurrence sur $n \geq 0$.
–Si $n = 0$, on a

$$\begin{aligned} a_n &= a_0 \text{ et } \frac{\lambda_1 \alpha_1^0 - \lambda_2 \alpha_2^0}{\alpha_1 - \alpha_2} = \frac{\lambda_1 - \lambda_2}{\alpha_1 - \alpha_2} \\ &= \frac{-a_0\alpha_2 + a_0\alpha_1}{\alpha_1 - \alpha_2} = a_0 \frac{\alpha_1 - \alpha_2}{\alpha_1 - \alpha_2} = a_0 \end{aligned}$$

Supposons que la relation est vraie jusqu'a l'ordre n. ie., $a_k = \frac{\lambda_1 \alpha_1^k - \lambda_2 \alpha_2^k}{\alpha_1 - \alpha_2}$; $0 \leq k \leq n$. Calculons a_{n+1}. On a

$$a_{n+1} = c_1 a_n + c_2 a_{n-1}$$

$$\begin{aligned} \Rightarrow\ a_{n+1} &= c_1 \frac{\lambda_1 \alpha_1^n - \lambda_2 \alpha_2^n}{\alpha_1 - \alpha_2} + c_2 \frac{\lambda_1 \alpha_1^{n-1} - \lambda_2 \alpha_2^{n-1}}{\alpha_1 - \alpha_2} \\ &= \frac{c_1\alpha_1 + c_2}{\alpha_1 - \alpha_2} \lambda_1 \alpha_1^{n-1} - \frac{c_1\alpha_2 + c_2}{\alpha_1 - \alpha_2} \lambda_2 \alpha_2^{n-1} \end{aligned}$$

Or $\alpha_1.\alpha_2 = -c_2$; $\alpha_1 + \alpha_2 = c_1$. D'où

$$\begin{aligned} a_{n+1} &= \frac{\alpha_1^2 + \alpha_1\alpha_2 - \alpha_1\alpha_2}{\alpha_1 - \alpha_2}\lambda_1\alpha_1^{n-1} - \frac{\alpha_1.\alpha_2 + \alpha_2^2 - \alpha_1\alpha_2}{\alpha_1 - \alpha_2}\lambda_2\alpha_2^{n-1} \\ \Rightarrow\ a_{n+1} &= \frac{\alpha_1^2}{\alpha_1 - \alpha_2}\lambda_1\alpha_1^{n-1} - \frac{\alpha_2^2}{\alpha_1 - \alpha_2}\lambda_2\alpha_2^{n-1} \\ \Rightarrow\ a_{n+1} &= \frac{\lambda_1\alpha_1^{n+1} - \lambda_2\alpha_2^{n+1}}{\alpha_1 - \alpha_2} \end{aligned}$$

Donc la propriété est vraie pour $n+1$. Et donc par induction on conclut que, pour tout $n \geq 0 : a_n = \frac{\lambda_1\alpha_1^n - \lambda_2\alpha_2^n}{\alpha_1 - \alpha_2}$.

* On va borner le cardinal de l'ensemble $\{n \geq 0 : a_n = \pm a_0\}$, qui est d'après le lemme (2.2.1) donné par

$$\left\{n \geq 0 : \frac{\lambda_1\alpha_1^n - \lambda_2\alpha_2^n}{\alpha_1 - \alpha_2} = \pm\frac{\lambda_1 - \lambda_2}{\alpha_1 - \alpha_2}\right\}$$

Donc, il suffit de borner le cardinal de l'ensemble

$$\{n \geq 0 : \lambda_1\alpha_1^n - \lambda_2\alpha_2^n = \pm(\lambda_1 - \lambda_2)\} \tag{2.2.2}$$

De plus, on peut supposer que les entiers algébriques λ_1 et λ_2 n'ont pas de facteurs entiers en communs dans l'anneau des entiers de $\mathbb{Q}(\alpha_1, \alpha_2)$. Si $a_0 = 0$, on obtient $\lambda_1 = \lambda_2$ et (2.2.2) se réduit à $\alpha_1^n - \alpha_2^n = 0$ qui n'a pas de solutions $n \neq 0$ (puisque $\frac{\alpha_1}{\alpha_2}$ n'est pas une racine de l'unité). Alors, on peut supposer dorénavant que $a_0 \neq 0$.

Dans les lemmes qui suivent, on va supposer que le déscriminant $\Delta = c_1^2 + 4c_2$ du polynôme caractéristique $x^2 - c_1x - c_2$ est tel que $\Delta \prec 0$ qui implique que α_1, α_2 sont des entiers algébriques dans un corps quadratique imaginaire $\mathbb{Q}(\sqrt{\Delta})$; $\alpha_2 = \overline{\alpha_1}$ et $\lambda_2 = \overline{\lambda_1}$. ■

Lemme 2.2.2 *Soit λ et α des entiers algébriques dans un corps quadratique imaginaire $\mathbb{k}$ d'anneau des entiers $O_{\mathbb{k}}$. Supposons que λ et $\overline{\lambda}$ n'ont pas de facteurs entiers en commun dans l'anneau des entiers algébriques $O_{\mathbb{k}}$. Si $\lambda\alpha^n - \overline{\lambda}\overline{\alpha}^n = \varepsilon\left(\lambda - \overline{\lambda}\right)$, pour un $\varepsilon \in \{-1, 1\}$ et $n \in \mathbb{N}$, alors*

$$\exists\ a \in \mathbb{Z}\ \textit{tel que} : \alpha^n = \varepsilon + a\overline{\lambda}$$

Preuve. Puisque $\lambda(\alpha^n - \varepsilon) = \overline{\lambda}(\overline{\alpha}^n - \varepsilon)$; on constate que $\lambda(\alpha^n - \varepsilon)$ est un entier qu'on le note par d par exemple.

*De plus ; on a $d\overline{\lambda} = \lambda\overline{\lambda}(\alpha^n - \varepsilon)$. Alors, si $\lambda\overline{\lambda} \nmid d \overset{Gauss}{\Rightarrow}$ il existe un facteur premier p de $\lambda\overline{\lambda}$ qui divise $\overline{\lambda}$ dans $O_{\mathbb{k}}$. Mais, on aura alors p/λ (puisque $p \in \mathbb{Z}$) ; ce qui contredit l'hypothèse λ, $\overline{\lambda}$ n'ont pas de facteurs entiers en commun. D'où $\lambda\overline{\lambda}/d$ qui implique que

$$\exists\ a \in \mathbb{Z} : \alpha^n - \varepsilon = a\overline{\lambda} \Rightarrow \alpha^n = \varepsilon + a\overline{\lambda} \qquad \text{(c.q.f.d)}$$

*En remplaçant (2.2.2) par son conjugué complexe s'il est nécessaire et α par $-\alpha$; λ par $-\lambda$ on peut supposer que $0 \leq Arg\ \alpha \leq \frac{\pi}{2}$ et $0 \leq Arg\ \lambda \leq \pi$. Et puisque α est la racine d'un polynôme irréductible et $\frac{\alpha}{\overline{\alpha}}$ n'est pas une racine de l'unité, on conclut que $0 < Arg\ \alpha < \frac{\pi}{2}$. De plus, puisque $a_0 \neq 0$; on peut supposer que $0 < Arg\ \lambda < \pi$. ■

Lemme 2.2.3 *Soit* $\mathbb{k}$ *un corps quadratique imaginaire d'anneau des entiers* $O_{\mathbb{k}}$ *et soient* γ, $\mu \in O_{\mathbb{k}}$, $t \in \mathbb{Z}^*$. *Considérons l'équation*

$$\gamma(1+t\mu)^n - \overline{\gamma}(1+t\overline{\mu})^n = \gamma - \overline{\gamma}\,;\ n \in \mathbb{N} \tag{2.2.3}$$

1) *Supposons que* $\gamma\mu - \overline{\gamma\mu} \neq 0$ *et soit* $\beta \in O_{\mathbb{k}}$ *tel que* $\beta \neq 0$ *et* β *divise* $\gamma\mu^l - \overline{\gamma\mu}^l$, $\forall\ l \geq 1$. *Alors* (2.2.3) *n'admet pas de solutions* $n \succ 0$ *si l'une des conditions suivantes est satisfaite.*

a) $t \equiv 0 \pmod 2$ *et* $\frac{t}{2} \nmid \frac{\gamma\mu-\overline{\gamma\mu}}{\beta}$.

b) $t \not\equiv 0 \pmod 2$ *et* $t \nmid \frac{\gamma\mu-\overline{\gamma\mu}}{\beta}$.

2) *Supposons que* $\gamma\mu - \overline{\gamma\mu} = 0$ *et* $\gamma\mu \neq 0$. *Soit* $\beta \in O_{\mathbb{k}}$, $\beta \neq 0$ *divisant* $\mu - \overline{\mu}$. *Alors,* $n = 1$ *est la seule solution si l'une des conditions suivantes est satisfaite.*

a) $t \equiv 0 \pmod 3$ *et* $\frac{t}{3} \nmid \frac{\mu-\overline{\mu}}{\beta}$.

b) $t \equiv 0 \pmod 3$, $t \nmid \frac{\mu-\overline{\mu}}{\beta}$ *et* $\frac{\mu^2-\overline{\mu}^2}{\beta} \equiv 0 \pmod 3$.

c) $t \not\equiv 0 \pmod 3$ *et* $t \nmid \frac{\mu-\overline{\mu}}{\beta}$.

Preuve. Supposons que l'équation (2.2.3) a une solution $n \succ 0$. Alors (2.2.3) peut se réécrire comme suit

$$\gamma - \overline{\gamma} + \sum_{j=1}^{n} C_n^j \left(\gamma\mu^j - \overline{\gamma\mu}^j\right) t^j = \gamma - \overline{\gamma}$$

qui donne

$$\sum_{j=1}^{n} C_n^j \left(\gamma\mu^j - \overline{\gamma\mu}^j\right) t^j = 0 \tag{2.2.4}$$

* Dans les deux cas du lemme, on a $\beta \neq 0$. Alors on peut multiplier (2.2.4) par β. D'une façon analogue, puisque $n \succ 0$ et $t \neq 0$, on peut multiplier (2.2.4) par n^{-1} et t^{-1}. Alors en tenant compte que $C_n^j = \frac{n}{j} C_{n-1}^{j-1}$; on obtient

$$\sum_{j=1}^{n} \frac{t^{j-1}}{j} C_{n-1}^{j-1} \frac{\gamma\mu^j - \overline{\gamma\mu}^j}{\beta} = 0 \tag{2.2.5}$$

* Traitons la première partie du lemme.

a) Supposons que $t \equiv 0 \pmod 2$ et $\frac{t}{2} \nmid \frac{\gamma\mu-\overline{\gamma\mu}}{\beta}$. Si $j = 2$, on conclut que $\frac{t^{j-1}}{j} \equiv 0 \pmod{\frac{t}{2}}$ et si $j \geq 3$, alors $\frac{t^{j-1}}{j} \equiv 0 \pmod t$. Il ressort que $\frac{t}{2}$ doit diviser le premier terme de (2.2.5). ie., $\frac{t}{2} / \frac{\gamma\mu-\overline{\gamma\mu}}{\beta}$, qui est une contradiction. On en déduit que (2.2.3) n'admet aucune solution $n > 0$.

b) Supposons que $t \not\equiv 0 \pmod 2$ et $t \nmid \frac{\gamma\mu-\overline{\gamma}\overline{\mu}}{\beta}$. Alors, on a $\frac{t^{j-1}}{j} \equiv 0 \pmod t$ pour tout $j \geq 2$. D'où $t/\frac{\gamma\mu-\overline{\gamma}\overline{\mu}}{\beta}$ qui est une contradiction. Alors dans tous les cas, il n'existe pas de solution $n \in \mathbb{N}^*$ pour l'équation (2.2.3).

* Pour la partie (2) supposons que $n \geq 2$ et puisque $\gamma\mu = \overline{\gamma}\overline{\mu}$. Alors, (2.2.5) se réduit à

$$\sum_{j=2}^{n} \frac{t^{j-1}}{j} C_{n-1}^{j-1} \frac{\mu^{j-1} - \overline{\mu}^{j-1}}{\beta} = 0$$

Donc, en appliquant $C_{n-1}^{j-1} = \frac{n-1}{j-1} C_{n-2}^{j-2}$ et en multipliant par $\frac{2}{t(n-1)}$ (puisque $t \neq 0$ et $n \geq 2$); on aura

$$\sum_{j=2}^{n} 2\frac{t^{j-2}}{j(j-1)} C_{n-2}^{j-2} \frac{\mu^{j-1} - \overline{\mu}^{j-1}}{\beta} = 0 \tag{2.2.6}$$

a) Supposons que $t \equiv 0 \pmod 3$. Si $j = 3$, on a $2\frac{t^{j-2}}{j(j-1)} \equiv 0 \pmod{\frac{t}{3}}$ et si $j \geq 4$, on aura $2\frac{t^{j-2}}{j(j-1)} \equiv 0 \pmod t$. On conclut que $\frac{t}{3}$ divise le premier terme de (2.2.6). ie., $\frac{t}{3} / \frac{\mu-\overline{\mu}}{\beta}$, qui est une contradiction. Donc il n'existe pas de solution $n \geq 2$ si $\frac{t}{3} \nmid \frac{\mu-\overline{\mu}}{\beta}$.

b) Si $\frac{\mu^2-\overline{\mu}^2}{\beta} \equiv 0 \pmod 3$, alors t divise le terme correspondant à $j = 3$. Et donc, il doit diviser aussi le premier terme $\frac{\mu-\overline{\mu}}{\beta}$ qui est une contradiction. Il s'ensuit que, si $t \nmid \frac{\mu-\overline{\mu}}{\beta}$, alors, il n'existe pas de solution $n \geq 2$.

c) Supposons que $t \not\equiv 0 \pmod 3$ et $t \nmid \frac{\mu-\overline{\mu}}{\beta}$. Alors; on aura

$$\forall\, t \geq 3 : 2\frac{t^{j-2}}{j(j-1)} \equiv 0 \pmod 3$$

Qui implique que t divise le premier terme de (2.2.6). C'est-à-dire $t/\frac{\mu-\overline{\mu}}{\beta}$, qui est une contradiction. On conclut donc qu'il n'existe pas de solution $n \geq 2$ pour l'équation (2.2.3). ∎

Lemme 2.2.4 *Soit $\mathbb{k}$ un corps quadratique imaginaire d'anneau des entiers $O_{\mathbb{k}}$ et soit λ, α des entiers algébriques de $\mathbb{k}$ tels que $0 < Arg\ \lambda < \pi$; $0 < Arg\ \alpha < \frac{\pi}{2}$ et $\frac{\alpha}{\overline{\alpha}}$ n'est pas une racine de l'unité. Supposons qu'il existe des naturels k, l ($k \leq l$) tels que $\alpha^k = \varepsilon + a\overline{\lambda}$ et $\alpha^l = \varepsilon' + a'\overline{\lambda}$ pour $a, a' \in \mathbb{Z}$ avec $|a| > 1$ et $\varepsilon, \varepsilon' \in \{-1, 1\}$. Posons $l = kq + r$ avec $0 \leq r < k$ (division euclidienne de l par k). Alors*

$$\lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r = \varepsilon'\varepsilon^q\left(\lambda - \overline{\lambda}\right)$$

Preuve. Si $l = k$, on aura $r = 0$, $a = a'$ et $\varepsilon = \varepsilon'$. Donc le résultat est trivial. Supposons donc que $l > k$. On voit que

$$\varepsilon'\left(\lambda - \overline{\lambda}\right) = \lambda\alpha^l - \overline{\lambda}\overline{\alpha}^l = \lambda\alpha^r\left(\varepsilon + a\overline{\lambda}\right)^q - \overline{\lambda}\overline{\alpha}^r\left(\varepsilon + a\lambda\right)^q$$

Alors

$$\varepsilon'\varepsilon^q\left(\lambda-\overline{\lambda}\right)=\lambda\alpha^r-\overline{\lambda}\overline{\alpha}^r+a\lambda\overline{\lambda}\left[\frac{\alpha^r\left(1+\varepsilon a\overline{\lambda}\right)^q-1}{a\overline{\lambda}}-\frac{\overline{\alpha}^r\left(1+\varepsilon a\lambda\right)^q-1}{a\lambda}\right] \tag{2.2.7}$$

**Si $k=1$, alors $r=0$ et le terme entre parenthèse dans (2.2.7) est divisible par $a(\lambda-\overline{\lambda})$, ce qui donne*

$$a^2\lambda\overline{\lambda}\left(\lambda-\overline{\lambda}\right)\ \text{divise}\ \left(\lambda-\overline{\lambda}\right)-\varepsilon'\varepsilon^q\left(\lambda-\overline{\lambda}\right)$$

–Puisque $|a|>1$; alors ceci est possible seulement si $\varepsilon'\varepsilon^q=1$, et le lemme est établi dans ce cas.

**Supposons maintenant que $k\geq 2$ et soit d un entier positif qui n'est pas un carré parfait tel que $\mathbb{k}$ soit un corps quadratique imaginaire de la forme $k=\mathbb{Q}\left(\sqrt{-d}\right)$.*

Notons que le terme entre parenthèses dans (2.2.7) est divisible par $\sqrt{-d}$, si $d\equiv -1 \pmod 4$ et par $2\sqrt{-d}$ si $d\not\equiv -1 \pmod 4$ dans $O_{\mathbb{k}}$. Posons

$$C(d)=\begin{cases}\sqrt{d}\ si\ d\ \equiv -1\ (\text{mod}\ 4)\\ 2\sqrt{d}\ si\ d\not\equiv -1\ (\text{mod}\ 4)\end{cases}$$

Alors (2.2.7) implique que : $iC(d)\,a\lambda\overline{\lambda}/\lambda\alpha^r-\overline{\lambda}\overline{\alpha}^r-\varepsilon'\varepsilon^q\left(\lambda-\overline{\lambda}\right)$. Supposons donc que $\lambda\alpha^r-\overline{\lambda}\overline{\alpha}^r\neq\varepsilon'\varepsilon^q\left(\lambda-\overline{\lambda}\right)$; Par conséquent, on en déduit que

$$C(d)\left|a\lambda\overline{\lambda}\right|\leq\left|\lambda\alpha^r-\overline{\lambda}\overline{\alpha}^r-\varepsilon'\varepsilon^q\left(\lambda-\overline{\lambda}\right)\right|$$

En utilisant $\alpha^k=\varepsilon+a\overline{\lambda}$ et l'inégalité triangulaire ; on obtient

$$|\lambda|C(d)\left(|\alpha|^k-1\right)\leq C(d)|\lambda|\left|\alpha^k-\varepsilon\right|\leq C(d)\left|a\lambda\overline{\lambda}\right|\leq 2|\lambda|\left(|\alpha|^r+1\right)$$

$$\Rightarrow 1<\frac{2}{C(d)}+\frac{1+\frac{2}{C(d)}}{|\alpha|^k} \tag{2.2.8}$$

** Puisque α est un entier algébrique dans $\mathbb{Q}\left(\sqrt{-d}\right)$ et $0<Arg\ \alpha<\frac{\pi}{2}$, on aura*

$$|\alpha|\geq\sqrt{1+d}$$

** Maintenant si $d\not\equiv -1 \pmod 4$ et $d\geq 2$, on obtient*

$$\frac{2}{|\alpha|C(d)}+\frac{1+\frac{2}{C(d)}}{|\alpha|^k}\leq\frac{1}{\sqrt{1+d}.\sqrt{d}}+\frac{1+\frac{1}{\sqrt{d}}}{1+d}\leq\frac{1}{\sqrt{6}}+\frac{1+\frac{1}{\sqrt{2}}}{3}<1$$

** Si $d\equiv -1 \pmod 4$ et $d\geq 11$, alors*

$$\frac{2}{|\alpha|C(d)}+\frac{1+\frac{2}{C(d)}}{|\alpha|^k}\leq\frac{4}{\sqrt{1+d}\,\sqrt{d}}+\frac{4+\frac{8}{\sqrt{d}}}{1+d}\leq\frac{2}{\sqrt{33}}+\frac{4+\frac{8}{\sqrt{11}}}{12}<1$$

On voit que pour toute solution de (2.2.8), *on doit avoir* $d = 1, 3, 7$. *Par quelques calculs, on peut montrer que ses solutions sont données par*

$$\alpha = \frac{1+\sqrt{-7}}{2},\ 1+i,\ 1+\sqrt{-3},\ \frac{3+\sqrt{-3}}{2},\ \frac{1+\sqrt{-3}}{2}$$

Toutes les solutions (sauf $\alpha = \frac{1+\sqrt{-7}}{2}$*) vérifient que* $\frac{\alpha}{\overline{\alpha}}$ *est une racine de l'unité, et donc elles sont rejetées.*

* *Soit* $\alpha = \frac{1+\sqrt{-7}}{2}$. *Alors* (2.2.8) *implique que* $k \leq 3$ *et avec la condition* $\alpha^k = \varepsilon + a\overline{\lambda}$; $a \in \mathbb{Z}$ *et* $|a| > 1$, *on conclut que* $\left(\frac{1+\sqrt{-7}}{2}\right)^k - \varepsilon$ *est divisible par un entier de valeur absolue au moins égale à deux, qui est impossible si* $k \leq 3$. *Alors*

$$\lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r - \varepsilon'\varepsilon^q\left(\lambda - \overline{\lambda}\right) = 0 \Rightarrow \lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r = \varepsilon'\varepsilon^q\left(\lambda - \overline{\lambda}\right) \qquad \text{(c.q.f.d)}$$

Lemme 2.2.5 *Soit* $\mathbb{k}$ *un corps quadratique imaginaire et* α *un entier algébrique de* $\mathbb{k}$ *avec* $0 < Arg\ \alpha < \frac{\pi}{2}$ *et* $\frac{\alpha}{\overline{\alpha}}$ *n'est pas une racine de l'unité. Soient* k, l *des entiers naturels tels que* $k < l$. *Alors, on aura*

i) Si $\alpha^l \pm \alpha^k = \pm 2$ *pour un choix de* $\pm$ *signe ; on obtient*

$$(k, l, \alpha) = \left(1, 3, \frac{1+\sqrt{-7}}{2}\right) \text{ ou } \left(1, 2, \frac{1+\sqrt{-7}}{2}\right)$$

ii) Si $\alpha^l \pm 2\alpha^k = \pm 3$ *pour un choix de signe* $\pm$ *; on trouve*

$$(k, l, \alpha) = \left(1, 3, \frac{1+\sqrt{-11}}{2}\right) \text{ ou } \left(1, 2, 1+\sqrt{-2}\right)$$

iii) Si $\alpha^l \pm 3\alpha^k \in \{\pm 2, \pm 4\}$ *pour certain choix de* $\pm$ *signe ; alors*

$$(k, l, \alpha) = \left(2, 4, \frac{1+\sqrt{-7}}{2}\right), \left(1, 4, \frac{1+\sqrt{-7}}{2}\right), \left(1, 2, \frac{3+\sqrt{-7}}{2}\right) \text{ ou } \left(1, 3, \frac{1+\sqrt{-15}}{2}\right)$$

Preuve. i) Si α *satisfait* $\alpha^l \pm \alpha^k = \pm 2$; *alors* $\alpha^k/2$ *et* $k \leq 2$. *De plus*

$$|\alpha^l| \leq |\alpha^k| + 2 \leq |\alpha^2| + 2$$

ce qui donne

$$k \leq 2 \text{ et } l \leq 4$$

* *Si* $k = 2$ *et* $l = 4$, *alors on obtient une équation quadratique en* α^2 *qui est* $\alpha^4 \pm \alpha^2 \mp 2 = 0$. *En résolvant cette équation, on obtient* $\alpha = \pm i, \pm\sqrt{-2}$; *mais dans ce cas* $\frac{\alpha}{\overline{\alpha}}$ *sera une racine*

de l'unité, et par conséquent ces solutions sont rejetées.

* *Si $k = 2$ et $l = 3$; alors $\alpha^l \pm \alpha^k = \pm 2$ s'écrit $\alpha^3 \pm \alpha^2 \mp 2 = 0$. Si cette équation admet un entier algébrique comme racine, alors elle doit avoir des solutions dans $\mathbb{Z}$ et ceci est vérifié dans le cas où $\alpha^3 + \alpha^2 - 2 = 0$, ce qui donne les solutions $\alpha = 1, -1 \pm i$ qui sont rejetées (puisque $\frac{\alpha}{\bar{\alpha}}$ sera une racine de l'unité).*

* *Le cas $k = 1$, $l = 3$ donne*

$$\alpha = \frac{1 + \sqrt{-7}}{2}$$

* *Si $l = 4$ et $k = 1$, on aura $|\alpha|^4 \leq |\alpha| + 2$ qui contredit $|\alpha| \geq \sqrt{2}$ (puisque α est un entier algébrique).*

* *Si $l = 2$ et $k = 1$, on obtient $\alpha = \frac{\pm 1 \pm \sqrt{-7}}{2}$. Dans tous les cas la condition $0 < Arg\ \alpha < \frac{\pi}{2}$ donne*

$$\alpha = \frac{1 + \sqrt{-7}}{2}$$

ii) Si α est tel que $\alpha^l \pm 2\alpha^k = \pm 3$, alors $\alpha^k / 3$ et $k \leq 2$. De plus, on aura

$$|\alpha|^l \leq 2\,|\alpha|^k + 3 \leq 2\,|\alpha|^2 + 3$$

ce qui donne

$$l \leq 4 \text{ (puisque } |\alpha|^2 \geq 3)$$

D'une façon similaire à (i), en résolvant l'équation $\alpha^l \pm 2\alpha^k = \pm 3$ on trouve simplement les solutions indiquées dans le lemme.

iii) Si α satisfait $\alpha^l \pm 3\alpha^k \in \{\pm 2, \pm 4\}$, alors $\alpha^k / 4$ et $k \leq 4$.

Supposons que $\alpha/4$; $0 < Arg\ \alpha < \frac{\pi}{2}$ et $\frac{\alpha}{\bar{\alpha}}$ n'est pas une racine de l'unité, on en déduit que

$$\alpha \in \left\{ \frac{1 + \sqrt{-7}}{2}, \frac{3 + \sqrt{-7}}{2}, 1 + \sqrt{-7}, \frac{1 + \sqrt{-15}}{2} \right\}$$

Alors par ces choix $\alpha^k / 4$ implique $k \leq 2$.

Si $k = 2$ (c'est-à-dire : $\alpha^2 / 4$), on aura $\alpha = \frac{1 + \sqrt{-7}}{2}$. Et donc, si $\alpha^{l-2} \pm 3 \in \left\{ \frac{\pm 2}{\alpha^2}, \frac{\pm 4}{\alpha^2} \right\}$, on trouve $l = 4$.

* *Si $k = 1$, on considère l'équation $\alpha^{l-1} \pm 3 \in \left\{ \frac{\pm 2}{\alpha}, \frac{\pm 4}{\alpha} \right\}$ pour les valeurs de α suivantes :*

$$\alpha = \frac{1 + \sqrt{-7}}{2}, \frac{3 + \sqrt{-7}}{2}, 1 + \sqrt{-7}, \frac{1 + \sqrt{-15}}{2}$$

Et par conséquent, on trouve les solutions

$$(k, l, \alpha) = \left(1, 4, \frac{1 + \sqrt{-7}}{2}\right), \left(1, 2, \frac{3 + \sqrt{-7}}{2}\right) \text{ et } \left(1.3, \frac{1 + \sqrt{-15}}{2}\right)$$

■

Lemme 2.2.6 *Soit α un entier algébrique dans un corps quadratique complexe tel que $\frac{\alpha}{\overline{\alpha}}$ n'est pas une racine de l'unité et $0 < Arg\ \alpha < \frac{\pi}{2}$. Supposons qu'il existe deux naturels l, k avec $l > k$ et un entier quadratique λ tels que $\alpha^k = \varepsilon + a\overline{\lambda}$ et $\alpha^l = \varepsilon' + a'\overline{\lambda}$ pour ε, $\varepsilon' \in \{-1, 1\}$ et a, $a' \in \mathbb{Z}$. Alors*

$$|a| \leq |a'|$$

■

Preuve. Supposons que $|a| > |a'|$. Comme $\left|\alpha^k - \varepsilon\right| = \left|a\overline{\lambda}\right|$ et $\left|\alpha^l - \varepsilon'\right| = \left|a'\overline{\lambda}\right|$, on aura

$$\left(|a'| - |a|\right)\left|\overline{\lambda}\right| = \left|\alpha^l - \varepsilon'\right| - \left|\alpha^k - \varepsilon\right| \geq |\alpha|^l - |\alpha|^k - 2$$

D'où

$$|\alpha|^l - |\alpha|^k - 2 \leq \left(|a'| - |a|\right) \leq -1 \text{ (puisque } |a'| - |a| < 0 \text{ et } \left|\overline{\lambda}\right| \geq \sqrt{2})$$

$$\Rightarrow |\alpha|^k \left(|\alpha|^{l-k} - 1\right) \leq 1$$

Et puisque $|\alpha| \geq \sqrt{2}$, on aura $l = k + 1$. De plus, si $|\alpha| = \sqrt{2}$ et $k \leq 2$; alors on doit avoir

$$\alpha = \frac{1 + \sqrt{-7}}{2}$$

*Maintenant considérons le cas $k = 1$. ie : $\alpha = \frac{1+\sqrt{-7}}{2} = \varepsilon + a\overline{\lambda}$ et $\alpha^l = \alpha^2 = \varepsilon' + a'\overline{\lambda}$ pour $\varepsilon \in \{-1, 1\}$; $a \in \mathbb{Z}$. Il s'ensuit que $a = \pm 1$. Alors $|a| > |a'|$ donne $a' = 0$, ce qui contredit $\alpha^2 = \left(\frac{1+\sqrt{-7}}{2}\right)^2 = \varepsilon' + a'\overline{\lambda}$. Il ressort donc que

$$|a| \leq |a'| \qquad \text{(c.q.f.d)}$$

■

Lemme 2.2.7 *Soit $\mathbb{k}$ un corps quadratique imaginaire et α, λ des entiers algébriques dans $\mathbb{k}$ tels que $0 < Arg\ \alpha < \frac{\pi}{2}$; $0 < Arg\ \lambda < \pi$ et $\frac{\alpha}{\overline{\alpha}}$ n'est pas une racine de l'unité. Supposons que $\alpha^k = \varepsilon + a\overline{\lambda}$ $(k \in \mathbb{N})$, $\varepsilon \in \{-1, 1\}$ et $a \in \mathbb{Z}$ avec $|a| > 3$. Alors l'équation $\lambda\alpha^n - \overline{\lambda}\overline{\alpha}^n = \pm\left(\lambda - \overline{\lambda}\right)$ n'a pas de solution $n > k$.*

Preuve. Supposons que

$$\lambda\alpha^n - \overline{\lambda}\overline{\alpha}^n = \varepsilon\left(\lambda - \overline{\lambda}\right) \tag{2.2.9}$$

pour $\varepsilon \in \{-1, 1\}$ et $n > k$. Soit q, r le quotient et le reste de la division de n par k. ie., $n = qk + r$; $0 \leq r < k$ et $q > 0$. Alors d'après le lemme (2.2.4) on a $\lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r = \varepsilon'\varepsilon^q\left(\lambda - \overline{\lambda}\right)$ et donc (2.2.9) s'écrit

$$\lambda\alpha^r\left(\varepsilon + a\overline{\lambda}\right)^q - \overline{\lambda}\overline{\alpha}^r\left(\varepsilon + a\lambda\right)^q = \varepsilon^q\left(\lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r\right)$$

D'où

$$\lambda\alpha^r\left(1+\varepsilon a\overline{\lambda}\right)^q-\overline{\lambda}\overline{\alpha}^r\left(1+\varepsilon a\lambda\right)^q=\lambda\alpha^r-\overline{\lambda}\overline{\alpha}^r$$

* Si $\alpha^r-\overline{\alpha}^r=0$, on aura $r=0$ (puisque $\frac{\alpha}{\overline{\alpha}}$ n'est pas une racine de l'unité). Il est évident qu'on peut donc appliquer la partie (2) du lemme (2.2.3) avec $\gamma=\lambda\alpha'$, $\mu=\overline{\lambda}$, $\beta=\lambda-\overline{\lambda}$, $t=\varepsilon a$ et $\frac{\mu-\overline{\mu}}{\beta}=-1$. Puisque $|a|>3$, les conditions de la partie (2) du lemme (2.2.3) sont satisfaites. D'où $q=1$. ie., $n=k$, qui contredit le fait que $n>k$.

* Supposons que $\alpha^r-\overline{\alpha}^r\neq 0$. Comme $\lambda\alpha^r-\overline{\lambda}\overline{\alpha}^r=\varepsilon'\varepsilon^q\left(\lambda-\overline{\lambda}\right)$, alors le lemme (2.2.2) implique que

$$\alpha^r=\varepsilon"+a'\overline{\lambda}\text{ pour }a'\in\mathbb{Z}\text{ et }\varepsilon"\in\{-1,1\}$$

Maintenant on peut appliquer la partie (1) du lemme (2.2.3) avec $\gamma=\lambda\alpha^r$, $\mu=\lambda'$, $\beta=\lambda\overline{\lambda}\left(\lambda\alpha^r-\overline{\lambda}\overline{\alpha}^r\right)$ et $t=\varepsilon a$ et par conséquent on obtient

$$\frac{\gamma\mu-\overline{\gamma\mu}}{\beta}=\frac{\lambda\overline{\lambda}\left(\alpha^r-\overline{\alpha}^r\right)}{\lambda\overline{\lambda}\left(\lambda\alpha^r-\overline{\lambda}\overline{\alpha}^r\right)}=\frac{a'\left(\overline{\lambda}-\lambda\right)}{\varepsilon"\left(\lambda-\overline{\lambda}\right)}=-\varepsilon"a'$$

$$\Rightarrow\beta/\gamma\mu^l-\overline{\gamma\mu}^l\,;\,\forall l\geq 1$$

Maintenant la partie (1) du lemme (2.2.3) implique que : ou bien $q=0$ (qui contredit l'hypothèse $q>0$), ou bien

$$\begin{cases} a/a' \text{ si } a\equiv 1\ (\text{mod } 2)\\ \frac{a}{2}/a' \text{ si } a\equiv 0\ (\text{mod } 2)\end{cases}$$

D'après le lemme (2.2.6), on a $|a'|\leq|a|$ et par conséquent on conclut que $|a|=|a'|$ ou $|a|=2|a'|$.

*Supposons premièrement que $|a|=|a'|$, comme $\alpha^k=\varepsilon+a\overline{\lambda}$ et $\alpha^r=\varepsilon"\pm a'\overline{\lambda}$, on aura

$$\alpha^k\pm\alpha^r=\pm 2\text{ ou }0$$

Et puisque $\frac{\alpha}{\overline{\alpha}}$ n'est pas une racine de l'unité, alors l'équation $\alpha^k\pm\alpha^r=0$ est impossible. Il reste à étudier l'équation $\alpha^k\pm\alpha^r=\pm 2$. Si $\alpha^k\pm\alpha^r=\pm 2$; on aura $\alpha^r/2$ et $|\alpha|^r\leq 2$, ce qui contredit $\alpha^r=\varepsilon"\pm a'\overline{\lambda}$ (car $|a'|=|a|>3$).

* Maintenant si $|a|=2|a'|$, alors $\alpha^k=\varepsilon\pm 2a'\overline{\lambda}$ et $\alpha^r=\varepsilon"\pm a'\overline{\lambda}$. On conclut donc que

$$\alpha^k\pm 2\alpha^r=\pm 1,\pm 3$$

Et comme α n'est pas une racine de l'unité, on doit avoir $\alpha^k\pm 2\alpha^r=\pm 3$. Alors par le lemme (2.2.5), on obtient

$$(r,k,\alpha)=\left(1,3,\frac{1+\sqrt{-11}}{2}\right)\text{ ou }\left(1,2,1+\sqrt{-2}\right)$$

Puisque $\alpha^r = \varepsilon" \pm a'\overline{\lambda}$ avec $|a'| \geq 2$, il s'ensuit que l'un des nombres $\pm 1 + \frac{1+\sqrt{-11}}{2}$ et l'un des nombres $\pm 1 + 1 + \sqrt{-2}$ est divisible par un entier de valeur absolue supérieur à 1 dans O_k, qui est une contradiction. Alors il n'y a pas de solution n avec $n > k$. ■

Lemme 2.2.8 *Etant donné α, λ. Alors toutes les solutions des équations $\lambda\alpha^n - \overline{\lambda}\overline{\alpha}^n = \pm(\lambda - \overline{\lambda})$ où $n \geq 0$ sont bien déterminées. De plus, on a*

1) *Si* $(\alpha, \lambda) = \left(\frac{1+\sqrt{-7}}{2}, \frac{1+\sqrt{-7}}{2}\right)$, *alors* $n = 0, 1, 2, 4, 12$.
2) *Si* $(\alpha, \lambda) = \left(1+\sqrt{-2}, \sqrt{-2}\right)$, *alors* $n = 0, 1, 2, 5$.
3) *Si* $(\alpha, \lambda) = \left(\frac{1+\sqrt{-11}}{2}, \frac{1+\sqrt{-11}}{2}\right)$, *alors* $n = 0, 1, 4$.
4) *Si* $(\alpha, \lambda) = \left(\frac{1+\sqrt{-11}}{2}, \frac{-3+\sqrt{-11}}{2}\right)$, *alors* $n = 0, 1, 3$.
5) *Si* $(\alpha, \lambda) = \left(\frac{1+\sqrt{-15}}{2}, \frac{-3+\sqrt{-15}}{2}\right)$, *alors* $n = 0, 1, 3$.
6) *Si* $(\alpha, \lambda) = \left(\frac{1+\sqrt{-19}}{2}, \frac{1+\sqrt{-19}}{2}\right)$, *alors* $n = 0, 1, 6$.

Preuve. Les parties 1, 2, 3 et 6 s'établissent par le lemme (2.2.7) puisque

$$\left(\frac{1+\sqrt{-7}}{2}\right)^{12} = -1 - 45\left(\frac{1-\sqrt{-7}}{2}\right); \left(1+\sqrt{-2}\right)^5 = 1 - 11\sqrt{-2}$$

$$\left(\frac{1+\sqrt{-11}}{2}\right)^4 = 1 + 5\left(\frac{1-\sqrt{-11}}{2}\right) \text{ et } \left(\frac{1+\sqrt{-19}}{2}\right)^6 = 1 - 56\left(\frac{1-\sqrt{-19}}{2}\right)$$

Alors dans ces cas toutes les solutions satisfont $n \leq 12$, $n \leq 5$, $n \leq 4$ et $n \leq 6$ respectivement. Ce petit ensemble de possibilités qu'on peut le déterminer en considérant les suites linéaires récurrentes correspondantes donne l'ensemble des solutions comme il est énoncé ci-dessus.

* Pour la partie (4), notons que $\alpha^4 = 1 + 5\overline{\alpha}$, et soit $n = 4q + r$ avec $0 \leq r < 4$. On cherche alors les solutions de l'équation

$$\lambda\alpha^r (1+5\overline{\alpha})^q - \overline{\lambda}\overline{\alpha}^r (1+5\alpha)^q = \pm(\lambda - \overline{\lambda})$$

* Si $1 \leq r \leq 3$ et puisque $\alpha\overline{\alpha} = 3$, alors la relation précédente peut s'écrire comme suit

$$\lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r \equiv \pm(\lambda - \overline{\lambda}) \pmod{15}$$

Maintenant ; on a $\left|\lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r\right| < 15$ (puisque $r \leq 3$). Par conséquent, on aura

$$\lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r = \pm(\lambda - \overline{\lambda})$$

Notons que celle-ci est triviale si $r = 0$. Donc

$$\lambda\alpha^r (1+5\overline{\alpha})^q - \overline{\lambda}\overline{\alpha}^r (1+5\alpha)^q = \lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r$$

Et on peut par suite appliquer la partie (1) du lemme (2.2.3) avec $\gamma = \lambda\alpha^r$, $\mu = \overline{\alpha}$, $\beta = \sqrt{-11}$ et $t = 5$ qui donne $q = 0$, et par suite $n = r$. Il ressort donc que toute solution doit satisfaire $n \leq 3$ et on vérifie facilement que les solutions sont $n = 0, 1, 3$.

– Pour (5), on a $\alpha^3 = -1 + 3\lambda'$. Ecrivons $n = 3q + r$, $0 \leq r \leq 2$ et supposons que $\lambda\alpha^n - \overline{\lambda}\overline{\alpha}^n = \varepsilon\left(\lambda - \overline{\lambda}\right)$ pour un $\varepsilon \in \{-1, 1\}$.

* Si $n \geq 3$, alors d'après le lemme (2.2.4), on a $\lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r = (-1)^q \varepsilon\left(\lambda - \overline{\lambda}\right)$, qui nous permet d'écrire

$$\lambda\alpha^r\left(1 - 3\overline{\lambda}\right)^q - \overline{\lambda}\overline{\alpha}^r(1 - 3\lambda)^q = \lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r$$

i) Si $r = 0$, on peut appliquer la partie (2) du lemme (2.2.3) avec $\gamma = \lambda$, $\mu = \overline{\lambda}$, $\beta = \left(\lambda - \overline{\lambda}\right)$ et $t = -3$, ce qui donne $q \leq 1$.

ii) Si $r \neq 0$, on applique la première partie du lemme (2.2.3) avec $\gamma = \lambda\alpha^r$, $\mu = \overline{\lambda}$, $\beta = 6\sqrt{-15}$ et $t = -3$. Et on voit qu'il n'existe pas de solutions vérifiant $q \geq 1$. Alors on doit avoir $n \leq 3$ et par des calculs simples, on aura $n = 0, 1, 3$.

Remarque 2.2.9 *le lemme précédent montre que la multiplicité de la suite $(a_n)_{n\in\mathbb{N}}$ est selon les six cas étudiés la suivante*

$$\begin{aligned}
1)\ m(a_0) + m(-a_0) &= 5\\
2)\ m(a_0) + m(-a_0) &= 4\\
3)\ m(a_0) + m(-a_0) &= 3\\
4)\ m(a_0) + m(-a_0) &= 3\\
5)\ m(a_0) + m(-a_0) &= 3\\
6)\ m(a_0) + m(-a_0) &= 3
\end{aligned}$$

■

Théorème 2.2.10 *Soit $(a_n)_{n\in\mathbb{N}}$ une suite linéaire récurrente à termes entiers non dégénérée d'ordre deux satisfaisant* (2.2.1) *et soit $x^2 - c_1x - c_2$ son polynôme caractéristique avec $a_0 > 0$, $(a_0, a_1) = 1$, $c_1 \geq 0$ et $\Delta = c_1^2 + 4c_2 < 0$. Si $a_n = \pm a_0$ a plus de trois solutions; alors les conditions suivantes sont satisfaites*

1) $c_1 = 1$, $c_2 = -2$, $a_0 = a_1 = 1$ *qui a les solutions* $n = 0, 1, 2, 4, 12$.

2) $c_1 = 1$, $c_2 = -2$, $a_0 = 1$, $a_1 = -1$ *qui a les solutions* $n = 0, 1, 3, 11$.

3) $c_1 = 3$, $c_2 = -4$, $a_0 = a_1 = 1$ *qui a les solutions* $n = 0, 1, 2, 6$.

4) $c_1 = 2$, $c_2 = -3$, $a_0 = a_1 = 1$ *qui a les solutions* $n = 0, 1, 2, 5$.

Preuve. D'après le lemme (2.2.1), la suite est donnée par

$$a_n = \frac{\lambda\alpha^n - \overline{\lambda}\overline{\alpha}^n}{\alpha - \overline{\alpha}} \; ; \; \forall n \geq 0$$

On prend α la racine de partie imaginaire positive. Puisque $\alpha + \overline{\alpha} = c_1$; $\alpha\overline{\alpha} = -c_2$ et $\frac{\alpha}{\overline{\alpha}}$ n'est pas une racine de l'unité, on aura Re $\alpha \neq 0$ qui donne $0 < Arg\ \alpha < \frac{\pi}{2}$. D'autre part puisque $a_0 > 0$ on conclut que $\lambda \notin \mathbb{R}$ et $0 < Arg\ \lambda < \pi$. L'équation $a_n = \pm a_0$ s'écrit

$$\lambda\alpha^n - \overline{\lambda}\overline{\alpha}^n = \pm\left(\lambda - \overline{\lambda}\right) \tag{2.2.10}$$

*On peut supposer que λ, $\overline{\lambda}$ n'ont pas de facteur entier en commun dans $O_{\mathbf{k}(\alpha)}$ qui n'est pas une condition réstrictive puisqu'on peut diviser (2.2.10) par de tel facteur.
Supposons que (2.2.10) a au moins quatre solutions $n = 0$, k, l, m vérifiant $0 < k < l < m$. Alors d'après le lemme (2.2.2) ; on sait qu'il existe a, $a' \in \mathbb{Z}$ tels que $\alpha^k = \varepsilon + a\overline{\lambda}$ et $\alpha^l = \varepsilon' + a'\overline{\lambda}$ pour $\varepsilon, \varepsilon' \in \{-1, 1\}$. Puisque la solution m est telle que $m > l$; alors par les lemmes (2.2.6) et (2.2.7) on obtient

$$|a| \leq |a'| \leq 3$$

1) Supposons que $|a| = |a'|$; alors $\alpha^l \pm \alpha^k \in \{-2, 0, 2\}$. Et puisque α n'est pas une racine de l'unité, on aura $\alpha^l \pm \alpha^k = \pm 2$ et en utilisant le lemme (2.2.5) ; on obtient

$$(k, l, \alpha) = \left(1, 2, \frac{1+\sqrt{-7}}{2}\right) \text{ ou } \left(1, 3, \frac{1+\sqrt{-7}}{2}\right)$$

Alors $\alpha^k = \pm 1 + a\overline{\lambda}$ et $\alpha^l = \pm 1 + a'\overline{\lambda}$ pour λ un entier quadratique de $\mathbb{Q}\left(\sqrt{-7}\right)$ avec $0 < Arg\lambda < \pi$, ce qui donne $\lambda = \frac{1+\sqrt{-7}}{2}$ si $l = 2$ et $\lambda = \frac{-3+\sqrt{-7}}{2}$ si $l = 3$.
2) Supposons que $|a| = 2$ et $|a'| = 3$, alors $2\alpha^l \pm 3\alpha^k \in \{-5, -1, 1, 5\}$. Et puisque α n'est pas une racine de l'unité, on aura $2\alpha^l \pm 3\alpha^k = \pm 5$. Donc $\alpha^k/5$ et par suite $|\alpha|^k = \sqrt{5}$ ou 5 et $k \leq 2$. On a aussi

$$|\alpha|^l \leq \frac{3}{2}|\alpha|^k + \frac{5}{2} \leq 10 \Rightarrow l \leq 2$$

Si on résout l'équation $2\alpha^2 \pm 3\alpha = \pm 5$, on obtient des solutions qui ne vérifient pas (2.2.10).
3) Supposons maintenant que $|a| = 1$ et $|a'| = 3$, donc $\alpha^l \pm 3\alpha^k \in \{-4, -2, 2, 4\}$. Alors par le lemme (2.2.5), on obtient

$$(k, l, \alpha) = \left(1, 4, \frac{1+\sqrt{-7}}{2}\right) ; \left(2, 4, \frac{1+\sqrt{-7}}{2}\right) ; \left(1, 2, \frac{3+\sqrt{-7}}{2}\right) \text{ ou } \left(1, 3, \frac{1+\sqrt{-15}}{2}\right)$$

–Les équations $|\alpha|^k = \pm 1 + a\overline{\lambda}$ et $\alpha^l = \pm 1 + a'\overline{\lambda}$ donnent

$$\lambda = \frac{1+\sqrt{-7}}{2}, \frac{1+\sqrt{-7}}{2}, \frac{-1+\sqrt{-7}}{2} \text{ ou } \frac{-3+\sqrt{-15}}{2} \text{ respectivement}$$

4) Supposons que $|a| = 1$ et $|a'| = 2$, alors $\alpha^l \pm 2\alpha^k \in \{-3, -1, 1, 3\}$. Et puisque α n'est pas une racine de l'unité; on aura $\alpha^l \pm 2\alpha^k = \pm 3$. Le lemme (2.2.5) donne alors $(k, l, \alpha) = (1, 2, 1 + \sqrt{-2})$ ou $\left(1, 3, \frac{1+\sqrt{-11}}{2}\right)$. Enfin, on en déduit que les équations $\alpha^k = \pm 1 + a\overline{\lambda}$ et $\alpha^l = \pm 1 + a'\overline{\lambda}$ impliquent que $\lambda = \sqrt{-2}$ ou $\frac{-3+\sqrt{-11}}{2}$ respectivement.

Conclusion 2.2.11 *Si l'équation* (2.2.10) *admet au moins quatre solutions, alors* (λ, α) *est donné par l'un des valeurs suivantes .*

$$\left(\frac{1+\sqrt{-7}}{2}, \frac{1+\sqrt{-7}}{2}\right), \left(\frac{-1+\sqrt{-7}}{2}, \frac{3+\sqrt{-7}}{2}\right), \left(\frac{-3+\sqrt{-7}}{2}, \frac{1+\sqrt{-7}}{2}\right),$$
$$\left(\frac{-3+\sqrt{-11}}{2}, \frac{1+\sqrt{-11}}{2}\right), \left(\frac{-3+\sqrt{-15}}{2}, \frac{1+\sqrt{-15}}{2}\right) \text{ ou } \left(\sqrt{-2}, 1+\sqrt{-2}\right)$$

Dans le premier cas, il s'ensuit d'après le lemme (2.2.8) *que* (2.2.10) *admet les solutions* $n = 0, 1, 2, 4$ *et* 12. *Dans le deuxième cas (puisque* $\frac{3-\sqrt{-7}}{2} = -\left(\frac{1+\sqrt{-7}}{2}\right)^2$*), on obtient l'équation*

$$-\frac{1+\sqrt{-7}}{2}\left(\frac{1+\sqrt{-7}}{2}\right)^{n+1} + \frac{1-\sqrt{-7}}{2}\left(\frac{1-\sqrt{-7}}{2}\right)^{n+1} = \pm\sqrt{-7}$$

qui admet les solutions $n = 0, 1, 3, 11$ *représentant les quatres dernières solutions du premier cas.*

Enfin pour le quatrième, le cinquième et le sixième cas les solutions sont données par le lemme (2.2.8) *et seulement dans le sixième cas qu'on a plus de trois solutions :* $n = 0, 1, 2, 5$.

**Pour les paires* (λ, α) *pour lesquels* (2.2.10) *a plus de trois solutions, on trouvera les récurrences indiquées dans le théorème.*

■

Remarque 2.2.12 1) *Si une suite linéaire récurrente prend la valeur* $\pm\lambda$ *plus de trois fois, alors elle satisfait l'une des conditions du théorème précédent.*

2) *Soit* m_0 *la plus petite solution de l'équation* $|a_n| = \lambda$ *et considérons la suite linéaire récurrente commençant par* a_{m_0} , a_{m_0+1}, a_{m_0+2} ,... *Divisons les termes de cette suite par* $p.g.c.d(a_{m_0}, a_{m_0+1})$ *; alors la suite obtenue satisfait les conditions du théorème précédent et prend sa valeur initiale plus de trois fois en valeur absolue.*

Inversement : On peut construire d'après le théorème (2.2.10) *toutes les suites* $(a_n)_{n\in\mathbb{N}}$ *telles que*

$$m(\lambda) + m(-\lambda) \geq 3\,;\ \textit{par inversement du processus}$$

Théorème 2.2.13 *Soit* $(a_n)_{n\in\mathbb{N}}$ *une suite linéaire récurrente non dégénérée à termes entiers d'ordre deux satisfaisant* (2.2.1). *Supposons que* $a_0 > 0$, $(a_0, a_1) = 1$; $c_1 \geq 0$ *et* $\Delta = c_1^2 + 4c_2 \geq 0$. *Alors l'équation* $a_n = \pm a_0$ *a au plus trois solutions sauf si* $c_1 = c_2 = 1$, $a_0 = 1$ *et* $a_1 = -1$ *où dans ce cas les solutions sont*

$$n = 0, 1, 3, 4$$

Preuve. Comme dans la preuve du théorème (2.2.10), on considère l'équation (2.2.10) avec λ_1 et α_1 sont des entiers algébriques dans un corps algébrique réel de dégré au plus égal à deux. Soit d un entier qui n'est pas un carré parfait tel que $\mathbb{k} = \mathbb{Q}\left(\sqrt{d}\right)$. On prend $d = 1$ si $\Delta = c_1^2 + 4c_2 = 0$. Puisque $c_1 \geq 0$, on peut supposer que $\alpha_1 \geq |\alpha_2|$. De plus, on a $\frac{\alpha_1}{\alpha_2} \neq \pm 1 \Rightarrow c_1 = \alpha_1 + \alpha_2 \geq 1$, et puisque $\frac{\alpha_1 - \alpha_2}{\sqrt{d}} \in \mathbb{Z}$, on aura

$$\alpha_1 - \alpha_2 \geq 1 \text{ qui implique que } \alpha_1 \geq |\alpha_2| + 1$$

1) Supposons premièrement que $\alpha_2 = 1$; alors (2.2.2) devient

$$\alpha_1^n \in \left\{1, \frac{2\lambda_2}{\lambda_1} - 1\right\} \tag{2.2.11}$$

On voit que (2.2.11) a au plus une solution (puisque α_1 n'est pas une racine de l'unité).
2) Si $\alpha_2 = -1$; alors en considérant les solutions paires et impaires séparément, on aura les deux équations suivantes

$$\begin{cases} a)\ \alpha_1^n \in \left\{1, \frac{2\lambda_2}{\lambda_1} - 1\right\} \text{ si } n \text{ est pair} \\ b)\ \alpha_1^n \in \left\{-1, 1 - \frac{2\lambda_2}{\lambda_1}\right\} \text{ si } n \text{ est impair} \end{cases}$$

Toute équation a au plus une solution et donc on peut supposer que $\alpha_2 \neq \pm 1$. On a $\alpha_2 \neq \pm 1 \Rightarrow \alpha_1 \neq \pm 1$ (puisque $\alpha_1 \geq |\alpha_2| + 1$). Supposons qu'on a quatre solutions $n = 0$, k, l, m. Par élimination de λ_1 et λ_2 des équations

$$\begin{aligned} i)\lambda_1\alpha_1^k - \lambda_2\alpha_2^k &= \pm(\lambda_1 - \lambda_2) \\ ii)\lambda_1\alpha_1^l - \lambda_2\alpha_2^l &= \pm(\lambda_1 - \lambda_2) \\ iii)\ \lambda_1\alpha_1^m - \lambda_2\alpha_2^m &= \pm(\lambda_1 - \lambda_2) \end{aligned}$$

On obtient

$$\frac{\alpha_1^k - \varepsilon}{\alpha_2^k - \varepsilon} = \frac{\alpha_1^l - \varepsilon'}{\alpha_2^l - \varepsilon'} = \frac{\alpha_1^m - \varepsilon''}{\alpha_2^m - \varepsilon''} = \frac{\lambda_1}{\lambda_2} \text{ pour } \varepsilon, \varepsilon', \varepsilon'' \in \{-1, 1\} \tag{2.2.12}$$

On voit qu'au moins deux épsilons sont égaux. On traite donc les deux cas correspondant à -1 et 1.

* Premièrement supposons que

$$l > k \text{ et } \frac{\alpha_1^k - 1}{\alpha_2^k - 1} = \frac{\alpha_1^l - 1}{\alpha_2^l - 1} \tag{2.2.13}$$

Si $\alpha_2 > 0$, alors

$$\begin{aligned} \forall x \in \mathbb{N}: \left|\frac{\alpha_1^x - 1}{\alpha_2^x - 1}\right| \left|\frac{\alpha_1^{x+1} - 1}{\alpha_2^{x+1} - 1}\right|^{-1} &= \left|\frac{\alpha_1^x - 1}{\alpha_1^{x+1} - 1}\right| \left|\alpha_2 + \frac{\alpha_2 - 1}{\alpha_2^x - 1}\right| \\ &< \frac{1}{\alpha_1}\left|\alpha_2 + \frac{1}{\alpha_2^{x-1} + \ldots + 1}\right| \leq \frac{1}{\alpha_1}(|\alpha_2| + 1) \leq 1 \end{aligned}$$

ie., la fonction $\left|\frac{\alpha_1^x - 1}{\alpha_2^x - 1}\right|$ est strictement croissante et donc (2.2.13) est non vérifiable. Alors on a forcément $\alpha_2 < 0$. On distingue trois cas.

1) Si k et l sont tous deux pairs, alors on peut traiter (2.2.13) avec α_1^2 à la place de α_1. Et puisque $\alpha_2^2 > 0$, cela est impossible.

2) Si k est impair, alors

$$\frac{\alpha_1^k - 1}{|\alpha_1| + 1} = \left|\frac{\alpha_1^k - 1}{\alpha_2^k - 1}\right| = \left|\frac{\alpha_1^l - 1}{\alpha_2^l - 1}\right| \geq \frac{\alpha_1^l - 1}{|\alpha_2|^l + 1}$$

Or, on voit que $\frac{\alpha_1^x - 1}{|\alpha_2|^x + 1}$ est strictement croissante pour tout $x \geq 1$, puisque

$$\begin{aligned} \frac{\alpha_1^x - 1}{|\alpha_2|^x + 1}\left(\frac{\alpha_1^{x+1} - 1}{|\alpha_2|^{x+1} + 1}\right)^{-1} &= \frac{\alpha_1^x - 1}{\alpha_1^{x+1} - 1}\frac{|\alpha_2|^{x+1} + 1}{|\alpha_2|^x + 1} \\ &< \frac{1}{\alpha_1}\left(|\alpha_2| + \frac{1 - |\alpha_2|}{|\alpha_2|^x + 1}\right) \\ &< \frac{1}{\alpha_1}(|\alpha_2| + 1) \leq 1 \end{aligned}$$

Par conséquent (2.2.13) est impossible si $\alpha_2 < 0$ et k impair.

3) Si k est pair et l impair; par comparaison des signes dans (2.2.13), on peut trouver $-1 < \alpha_2 < 0$, qui signifie que α_1, α_2 sont des entiers quadratiques conjugués. Et puisque $\alpha_1 > 0$ et $\alpha_2 > -1$, on aura

$$(\alpha_1 + 1)(\alpha_2 + 1) \geq 1$$

$$\Rightarrow \left|\frac{\alpha_1^k - 1}{\alpha_2^k - 1}\right| = \frac{1}{\alpha_2 + 1}\frac{\alpha_1^k - 1}{\left|\alpha_2^{k-1} - \alpha_2^{k-2} + \ldots - 1\right|} \leq \frac{1}{|\alpha_2 + 1|}\frac{\alpha_1^k - 1}{|\alpha_2| + 1}$$

$$\Longrightarrow \left|\frac{\alpha_1^k - 1}{\alpha_2^k - 1}\right| \leq (\alpha_1 + 1)\frac{\alpha_1^k - 1}{|\alpha_2| + 1} \tag{*}$$

D'une façon analogue, on obtient aussi

$$\left|\frac{\alpha_1^l - 1}{\alpha_2^l - 1}\right| > \frac{\alpha_1^l - 1}{2} \qquad (**)$$

Par ces deux inégalités et (2.2.13), on obtient

$$\alpha_1^l - 1 < 2\frac{\alpha_1 + 1}{|\alpha_2| + 1}\left(\alpha_1^k - 1\right) \qquad (2.2.14)$$

Et par conséquent, on aura

$$\alpha_1^l - 2\alpha_1^{k+1} - \alpha_1^k + \alpha_1 + 1 < 0$$

On en déduit donc que : si $l \geq k+3$, alors $\alpha_1 < 2$. Or le seul entier quadratique irrationnel positif α_1 tel que $\frac{\alpha_1}{\alpha_2} \neq \pm 1$ est $\alpha_1 = \frac{1+\sqrt{5}}{2}$, qui ne satisfait pas (2.2.14). Alors on a forcément $l = k+1$. De plus, on sait qu'il existe une troisième solution m et on en déduit que

$$(2.2.12) \Rightarrow \frac{\alpha_1^m - \varepsilon''}{\alpha_2^m - \varepsilon''} = \frac{\alpha_1^k - 1}{\alpha_2^k - 1}$$

* Si $\varepsilon'' = +1$, on conclut que $m > k$ et m est impair, qui implique que $\frac{\alpha_1^m - 1}{\alpha_2^m - 1} = \frac{\alpha_1^l - 1}{\alpha_2^l - 1}$ avec m, l sont impairs, ce qui est impossible.

* Si $\varepsilon'' = -1$; alors $\frac{\alpha_1^m + 1}{\alpha_2^m + 1}$ et $\frac{\alpha_1^k - 1}{\alpha_2^k - 1}$ ont des signes opposés. Et d'après les cas précédents (1), (2) et (3) on conclut que dans (2.2.12), il y a au plus un epsilon égale à 1.

ii) Supposons que

$$l > k \text{ et } \frac{\alpha_1^k + 1}{\alpha_2^k + 1} = \frac{\alpha_1^l + 1}{\alpha_2^l + 1} \qquad (2.2.15)$$

Puisque $\left(\frac{\alpha_1^x + 1}{\alpha_2^x + 1}\right)$ est une fonction strictement croissante pour tout $x \geq 1$, alors : si $\alpha_2 > 0$, la condition (2.2.15) n'est pas établie. Et par suite on doit supposer que $\alpha_2 < 0$. On distingue quatre cas.

1) Si k et l sont tous deux pairs ; alors on peut considérer (2.2.15) avec α_1^2 au lieu de α_1, ce qui est impossible.

2) Si k est pair et l impair et en considérant les signes dans (2.2.15), on voit simplement que $-1 < \alpha_2 < 0$, qui donne

$$\alpha_1^k + 1 > \frac{\alpha_1^k + 1}{\alpha_2^k + 1} = \frac{\alpha_1^l + 1}{\alpha_2^l + 1} > \alpha_1^l + 1$$

qui est impossible puisque $\alpha_1 > 1$.

3) Si k et l sont tous deux impairs, alors la condition (2.2.15) peut s'écrire

$$\frac{\alpha_1^k + 1}{|\alpha_2|^k - 1} = \frac{\alpha_1^l + 1}{|\alpha_2|^l - 1}$$

On voit que $\frac{\alpha_1^{2x-1}+1}{|\alpha_2|^{2x-1}-1}$ est croissante pour tout $x \geq 1$, puisque

$$\begin{aligned}\left(\frac{\alpha_1^{2x-1}+1}{|\alpha_2|^{2x-1}-1}\right)\left(\frac{\alpha_1^{2x+1}+1}{|\alpha_2|^{2x+1}-1}\right)^{-1} &= \frac{\alpha_1^{2x-1}+|\alpha_2|^{2x+1}-1}{\alpha_1^{2x+1}+|\alpha_2|^{2x-1}-1} \\ &\leq \frac{\alpha_1+|\alpha_2|^3-1}{\alpha_1^3+|\alpha_2|-1} \\ &\leq \frac{|\alpha_2|^2+|\alpha_2|+1}{(|\alpha_2|+1)^2-|\alpha_2|}=1 \qquad (2.216)\end{aligned}$$

−De plus si (2.2.16) devient une égalité; alors $x=1$ et $\alpha_1 = 1-\alpha_2$. Et on trouve $k=1$, $l=3$.

* Notons qu'on a une troisième solution m vérifiant $\frac{\alpha_1^m-\varepsilon''}{\alpha_2^m-\varepsilon''}=\frac{\alpha_1+1}{\alpha_2+1}$.

−Supposons que $\alpha_1 > 2$. Puisque on a supposé que $\alpha_2 = 1-\alpha_1$ et $\alpha_1 \neq -1$, on en déduit que $\alpha_2 < -1$, $\alpha_1 > 2$ et m est impair. ie., $m \geq 5$. D'où

$$\begin{aligned}\frac{\alpha_1^5-1}{(\alpha_1-1)^5+1} &\leq \frac{\alpha_1^m-\varepsilon''}{(\alpha_1-1)^m+\varepsilon''}=-\frac{\alpha_1^m-\varepsilon''}{\alpha_2^m-\varepsilon''}=-\frac{\alpha_1+1}{\alpha_2+1}=\frac{\alpha_1+1}{\alpha_1-2} \\ &\Rightarrow \quad 2\alpha_1^5-5\alpha_1^4+5\alpha_1^2-6\alpha_1+2\leq 0\end{aligned}$$

Et on peut constater que $\alpha_1 < \frac{1+\sqrt{13}}{2}$. Mais, il n'existe aucun entier algébrique de la forme

$$2<\alpha_1<\frac{1+\sqrt{13}}{2}$$

On doit donc forcément supposer que $\alpha_1 < 2$, ce qui donne $\alpha_1 = \frac{1+\sqrt{5}}{2}$. Il ressort que

$$\begin{aligned}\frac{\alpha_1^m-1}{\alpha_1} &\leq \left|\frac{\alpha_1^m-\varepsilon''}{\alpha_2^m-\varepsilon''}\right|=\left|\frac{\alpha_1+1}{\alpha_1-2}\right|=\alpha_1^4 \\ &\Rightarrow \quad m\leq 5 \text{ et } \frac{\alpha_1^m-\varepsilon''}{\alpha_2^m-\varepsilon''}=\frac{\alpha_1+1}{\alpha_1-2} \\ &\Rightarrow \quad \varepsilon''=-1 \text{ et } m=1\ ,\ 3\ ,\ 4\end{aligned}$$

4) Si k est impair et l est pair, et en comparant les signes dans (2.2.15) comme précédemment ; on obtient $-1<\alpha_2<0$ qui donne

$$\begin{aligned}(\alpha_1+1)\left(\alpha_1^k+1\right) &\geq \frac{\alpha_1^k+1}{\alpha_2+1}\frac{1}{1+|\alpha_2|+...+|\alpha_2|^{k-1}} \\ &= \frac{\alpha_1^k+1}{\alpha_2^k+1}=\frac{\alpha_1^l+1}{\alpha_2^l+1}\succ\frac{\alpha_1^l+1}{2} \\ &\Rightarrow \quad \alpha_1^l+1\prec 2(\alpha_1+1)\left(\alpha_1^k+1\right)\end{aligned}$$

* Si $l \geq k+3$, alors $\alpha_1 < \frac{11}{5}$ qui donne $\alpha_1 = \frac{1+\sqrt{5}}{2}$. Puisque $\alpha_1 \cdot \alpha_2 = -1$, on obtient $\frac{\alpha_1^l+1}{\alpha_2^l+1}=\alpha_1^l$ et d'après (2.2.15), on aura

$$\alpha_1^l=\frac{\alpha_1^k+1}{\alpha_2^k+1}\leq\frac{\alpha_1^k+1}{\alpha_2+1}=\alpha_1^2\left(\alpha_1^k+1\right)$$

qui admet la solution

$$k = 1 \text{ et } l = 4$$

* Supposons que $l = k+1$ ou $k = 1, l = 4$. On sait qu'il existe une troisième solution m telle que

$$\frac{\alpha_1^m - \varepsilon"}{\alpha_2^m - \varepsilon"} = \frac{\alpha_1^l + 1}{\alpha_2^l + 1}$$

−Si $\varepsilon" = +1$; alors les termes ont des signes opposés, ce qui est impossible. On a donc forcément $\varepsilon" = -1$.

* Si $m > l$, on aboutit à une contradiction (puisque l est pair et on a montré que la plus petite des deux solutions ne peut être paire). On en déduit donc que $m < l$ et m est impair et d'après (2.2.12), on trouve

$$(k, l, m) = (1, 3, 4) \text{ ou } (3, 4, 1) \text{ et } \alpha_1 = \frac{1+\sqrt{5}}{2}$$

On voit que

$$\frac{\lambda_1}{\lambda_2} = \frac{\alpha_1^l + 1}{\alpha_2^l + 1} = \alpha_1^l = \left(\frac{1+\sqrt{5}}{2}\right)^4$$

qui donne

$$\lambda_1 = \pm\left(\frac{3-\sqrt{5}}{2}\right)$$

Enfin, on conclut que les solutions de (2.2.12) sont données par

$$k = 1, l = 3, m = 4\,;\ \alpha_1 = \frac{1+\sqrt{5}}{2} \text{ et } \lambda_1 = \pm\left(\frac{3-\sqrt{5}}{2}\right)$$

* Ces valeurs de α_1, λ_1 vérifient la suite linéaire récurrente comme il est énoncé. c .q .f .d ■

Chapitre 3

Solutions effectives des suites linéaires récurrentes

Dans le chapitre précédent, nous avons étudié un problème intéressant concernant les suites linéaires récurrentes, à savoir la multiplicité. Cette étude provoque naturellement autres questions qui semblent être importantes du point de vue mathématique telles que la détermination de la solution générale de telles suites, la structure de l'ensemble des zéros de ces suites,... la présence de carrés parfaits dans une suite linéaire récurrente d'ordre deux. L'objet du présent chapitre est de chercher une formule représentant le terme général de telles suites, en reposant sur quelques résultats d'algèbre linéaire et des équations diophantiènnes. Notons de plus qu'il existe une étroite correspondance entre les suites linéaires récurrentes et les sommes de puissances généralisées appelées souvent séries de puissances formelles.

3.1 Formule générale des solutions des suites linéaires récurrentes

Définition 3.1.1 *On appelle somme de puissances généralisées toute somme exponentielle finie de la forme*

$$u(n) = \sum_{i=1}^{r} A_i(n)\ \alpha_i^n\ , n \in \mathbb{N}.$$

avec $A_i(n)$ sont des coéfficients polynômiaux.

$*$Soient $n_i \in \mathbb{N}$ et posons $\sum_{i=1}^{r} n_i = k$. Les distincts α_i sont appelés les racines caractéristiques de la somme $u(n)$. n_i est la multiplicité de α_i et les $A_i(n)$ tels que dégré $(A_i(n)) \leq n_i - 1$ sont les coéfficients de cette somme.

Pour comprendre la relation entre une somme de puissances généralisées et une suite linéaire récurrente, on définit un opérateur E sur l'ensemble des suites par

$$(E(u))(n) = u_{n+1}, \forall n \in \mathbb{Z}$$

Alors ; si la suite $(u_n)_{n\in\mathbb{N}}$ satisfait $u_{n+k} = c_1 u_{n+k-1} + ... + c_{k-1} u_{n+1} + c_k u_n, \forall n \geq 0$, on voit que la somme de puissances généralisées $\sum_{i=1}^{r} A_i(n)\ \alpha_i^n$ est engendrée par l'opérateur

$$\prod_{i=1}^{r} (E - \alpha_i)^{n_i} = E^k - c_1 E^{k-1} - ... - c_{k-1} E - c_k$$

Le théorème suivant établit bien la relation entre les suites linéaires récurrentes et la somme de puissances généralisées.

Théorème 3.1.2 *Soit $(u_n)_{n\in\mathbb{N}}$ une suite linéaire récurrente d'ordre k définie par les valeurs initiales $u_0, u_1, ..., u_{k-1}$ et la relation de récurrence suivante*

$$u_n = c_{k-1} u_{n-1} + c_{k-2} u_{n-2} + ... + c_0 u_{n-k}\ ,\ \forall n \geq k \tag{3.1}$$

Et soit

$$P(x) = x^k - c_{k-1} x^{k-1} - ... - c_1 x - c_0 = \prod_{i=1}^{r} (x - \alpha_i)^{n_i} \tag{3.2}$$

son polynôme caractéristique où les $(\alpha_i)_{i=\overline{1,r}}$ sont les racines de $P(x)$ et n_i est la multiplicité de α_i. Soit F le corps partagé de $P(x)$; alors $\forall i$; $1 \leq i \leq r$, il existe un polynôme unique $P_i(x) \in F[x]$ avec $dég(P_i) \leq n_i - 1$ tels que

$$\forall n \in \mathbb{N} : u_n = P_1(n)\,\alpha_1^n + P_2(n)\alpha_2^n + ... + P_r(n)\,\alpha_r^n \tag{3.3}$$

De plus, si la suite $(u_n)_{n\in\mathbb{N}}$ est d'ordre k ; alors $dég(P_i) = n_i - 1$, $\forall i$; $1 \leq i \leq r$.

Inversement : *Supposons que α_1, α_2,..., α_r sont des nombres complexes distincts non nuls et $P_1(x)$, $P_2(x)$,...,$P_r(x)$ des polynômes non nuls appartenant à $C[x]$. Pour tout i tel que $1 \leq i \leq r$, soit n_i un entier strictement supérieur à $dég(P_i)$. Posons $k = n_1 + n_2 + ... + n_r$ et définissons c_0, c_1,..., c_{k-1} par (3.2). Alors la suite définie par (3.3) satisfait la relation de récurrence (3.1). De plus ; si $n_i = dég(P_i) + 1$, alors $(u_n)_{n\in\mathbb{N}}$ est d'ordre k.*

Remarque 3.1.3 *Le théorème (3.1.2) est valable dans tout corps de caractéristique 0. Mais, dans le cas d'un corps de caractéristique $p \neq 0$ et s'il existe une racine α_i de multiplicité $n_i \succ p$, alors $(u_n)_n$ ne peut plus avoir des solutions sous la forme*

$$u_n = \sum_{i=1}^{r} P_i(n)\,\alpha_i^n$$

* *Pour démontrer la première partie de ce théorème, on a besoin du lemme suivant.*

Lemme 3.1.4 *Soit S l'ensemble des suites linéaires récurrentes de $\mathbb{C}$ vérifiant la relation de récurrence* (3.1) *avec les conditions initiales u_0, u_1,..., u_{k-1}. Alors, l'ensemble S est un sous espace vectoriel sur $\mathbb{C}$ de dimension k.*

Preuve. Si $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ sont deux éléments de S. On a

$$\begin{aligned} u_n &= c_{k-1}u_{n-1} + ... + c_1u_{n-k+1} + c_0u_{n-k} \\ v_n &= c_{k-1}v_{n-1} + ... + c_1v_{n-k+1} + c_0v_{n-k} \\ &\Longrightarrow u_n - v_n = c_{k-1}(u_{n-1} - v_{n-1}) + ... + c_1(u_{n-k+1} - v_{n-k+1}) + c_0(u_{n-k} - v_{n-k}) \\ &\Longrightarrow (u_n - v_n)_{n\in\mathbb{N}} \in S \end{aligned}$$

D'autre part; si $(u_n)_{n\in\mathbb{N}} \in S$ et $\lambda \in \mathbb{C}$, on aura

$$\begin{aligned} \lambda u_n &= \lambda c_{k-1}u_{n-1} + ... + \lambda c_0u_{n-k} \\ &= c_{k-1}(\lambda u_{n-1}) + ... + c_0(\lambda u_{n-k}) \\ &\Rightarrow (\lambda u_n)_{n\in\mathbb{N}} \in S \end{aligned}$$

Par conséquent S est un sous-espace de $\mathbb{C}$ de base $\{u_{n-1}, ..., u_{n-k}\}$. ie., S est un espace vectoriel de dimension k. ∎

Preuve. (du théorème) Pour la première partie, considérons l'espace vectoriel V de toutes les suites $(u_n)_{n\in\mathbb{N}} \subset \mathbb{C}$. Soit $P(x) = x^k - c_{k-1}x^{k-1} - ... - c_1x - c_0$ le polynôme caractéristique de $(u_n)_{n\in\mathbb{N}}$. Opérons P sur V par

$$P(u_n) = (v_n)_{n\in\mathbb{N}}$$

Où

$$v_n = u_n - c_{k-1}u_{n-1} - c_{k-2}u_{n-2} - ... - c_0u_{n-k}\ ,\forall\ n \geq k$$

Posons $W = KerP$. On sait bien que W est un sous-espace vectoriel de V de toutes les suites satisfaisant (3.1) et de dimension k. On va montrer que W est engendré par les suites

$$\left(n^j\alpha_i^n\right)_{n\in\mathbb{N}},\ \forall i,\ j \text{ tels que : } 1 \leq i \leq r \text{ et } 0 \leq j \leq n_i - 1 \tag{3.4}$$

On a k vecteurs $n^0\alpha_1^n$,..., $n^{n_1-1}\alpha_1^n$, $n^0\alpha_2^n$,..., $n^{n_2-1}\alpha_2^n$, $n^0\alpha_r^n$,..., $n^{n_r-1}\alpha_r^n$. De plus, ces vecteurs sont clairement linéairement indépendants. Il reste donc à montrer que chacun de ces vecteurs appartient à W. ie., que pour tout $n \in \mathbb{N}$, $0 \leq j \leq n_i - 1$ et $1 \leq i \leq r$, ces sous-suites diovent satisfaire

$$n^j\alpha_i^n - c_{k-1}(n-1)^j\alpha_i^{n-1} - ... - c_0(n-k)^j\alpha_i^{n-k} = 0 \tag{3.5}$$

Le membre gauche de (3.5) est égale à

$$\underbrace{z\frac{d}{d\,z}\left(\ldots\left(z\frac{d}{d\,z}z^{n-k}P(z)\ldots\right)\ldots\right)}_{j\text{ fois}}\Bigg|\; z=\alpha_i \tag{3.6}$$

qui est interprété par $\alpha_i^{n-k}P(\alpha_i)=0$, si $j=0$. Puisque pour tout i, $1\leq i\leq r$; α_i a une multiplicité n_i et $j\leq n_i-1$ on voit que (3.6) s'annule et donc (3.5) est établie. Et comme les suites $(n^j\alpha_i^n)_{n\in\mathbb{N}}$ forment une base de W; alors toute suite linéaire récurrente vérifiant (3.1) est donnée par

$$\begin{aligned} u_n &= a_{10}n^0\alpha_1^n+\ldots+a_{1(n_1-1)}n^{(n_1-1)}\alpha_1^n+\ldots+a_{r0}n^0\alpha_r^n+\ldots+a_{r(n_r-1)}n^{n_r-1}\alpha_r^n \\ &= P_1(n)\,\alpha_1^n+P_2(n)\alpha_2^n+\ldots+P_r(n)\,\alpha_r^n \text{ avec deg } P_i(n)\leq n_i-1 \end{aligned} \tag{3.7}$$

La preuve de la partie inverse du théorème(3.1.2) repose sur les lemmes suivants ■

Lemme 3.1.5 *Soit* $P(x)=x^k-\sum_{s=0}^{k-1}c_s\,x^s$ *un polynôme qui admet* α *comme un zéro de multiplicité* $m\geq 1$. *On définit* :$P_0(x)=P(x)$ *et* $P_{i+1}(x)=xP_i'(x)$, $\forall i\geq 1$. *Alors il existe des polynômes* $Q_i(x)$ *tels que*

$$P_i(x)=(x-\alpha)^{m-i}Q_i(x)\ ,\forall i\in\{0,1,\ldots,m-1\} \tag{3.8}$$

Inversement :
Si $\alpha\neq 0$ *et* $P_i(\alpha)=0$; $\forall i=\overline{0,m-1}$, *alors* $P_0(x)=(x-\alpha)^mQ_0(x)$ *pour un polynôme* $Q_0(x)$.

Preuve. Tout d'abord, on va montrer par récurrence que pour tout $i\geq 1$, $P_i(x)$ est représenté par

$$P_i(x)=\sum_{j=1}^{i}C_j^{(i)}x^jP^{(j)}(x) \text{ où chaque } C_j^{(i)}\in\mathbb{Z} \text{ et } C_1^{(i)}=C_i^{(i)}=1 \tag{3.9}$$

Le cas $i=1$ est évident (puisque $P_1(x)=xP'(x)$). Supposons maintenant que (3.9) est vraie jusqu'à l'ordre i. Alors

$$\begin{aligned} P_i'(x) &= \sum_{j=1}^{i}C_j^{(i)}\left(jx^{j-1}P^{(j)}(x)+x^jP^{(j+1)}(x)\right) \\ &= \sum_{j=1}^{i}C_j^{(i)}jx^{j-1}P^{(j)}(x)+\sum_{j=2}^{i+1}C_{j-1}^{(i)}x^{j-1}P^{(j)}(x) \end{aligned}$$

Et par conséquent

$$\begin{aligned} P_{i+1}(x) &= xP_i'(x) \\ &= xP'(x) + \sum_{j=2}^{i} \left(jC_j^{(i)} + C_{j-1}^{(i)} \right) x^j P^{(j)}(x) + x^{i+1} P^{(i+1)}(x) \\ \Longrightarrow \quad P_{i+1}(x) &= \sum_{j=1}^{i+1} C_j^{(i+1)} x^j P^{(j)}(x) \end{aligned}$$

D'autre part ; si α est une racine de $P(x)$ de multiplicité m, alors α est une racine de $P^{(j)}(x)$ avec multiplicité $m-j$, et ceci implique que $P^{(j)}(x) = (x-\alpha)^{m-j} R_j(x)$ pour quelque polynôme $R_j(x)$. Alors la première partie du lemme se déduit directement de cette expression de $P^{(j)}(x)$ et de la représentation (3.9).

La réciproque s'obtient aussi par récurrence, en utilisant la représentation (3.9).

En effet. Si $m = 1$, on aura

$$\begin{aligned} P_0(\alpha) &= P(\alpha) \Longrightarrow (x-\alpha)/P(x) \\ &\Longrightarrow P(x) = (x-\alpha).Q_0(x) \end{aligned}$$

Supposons que la propriété est vraie pour tout nombre inférieur à m. Si $P_{m-1}(\alpha) = 0$, on obtient

$$\begin{aligned} 0 &= \sum_{j=1}^{m-1} C_j^{(m-1)} \alpha^j P^{(j)}(\alpha) = 0 + ...0 + \alpha^{m-1} P^{(m-1)}(\alpha) \text{ pour tout } \alpha \neq 0 \\ &\Longrightarrow P^{(m-1)}(\alpha) = 0 \Longrightarrow (x-\alpha)^m / P(x) \\ &\Longrightarrow P(x) = (x-\alpha)^m Q_0(x) \end{aligned}$$

■

Lemme 3.1.6 *Sous les conditions du lemme précédent, on a*

$$i) \sum_{p=0}^{k-1} p^i c_p \alpha^p = k^i.\alpha^k \; ; \forall \overline{i = 0,\ m-1}$$

$$ii) \sum_{p=1}^{k} c_{k-p} p^i \alpha^{k-p} = 0 \; ; \forall \overline{i = 1,\ m-1}$$

$$iii) \sum_{p=1}^{k} c_{k-p} (n-p)^j \alpha^{k-p} = n^j \alpha^k \; ; \forall \overline{j = 0,\ m-1}$$

Preuve. *i*) Par récurrence, on a

$$P_i(x) = k^i x^k - \sum_{p=0}^{k-1} p^i c_p x^p; \ \forall \overline{i = 0,\ m-1}$$

En effet. Pour $i = 0$; on obtient

$$k^0 x^k - \sum_{p=0}^{k-1} p^0 c_p x^p = x^k - \sum_{p=0}^{k-1} c_p x^p = P_0(x)$$

Supposons maintenant que la relation est vraie jusqu'à l'ordre i. On a

$$\begin{aligned} P_{i+1}(x) &= xP_i'(x) = x\left[kk^{i-1}x^{k-1} - \sum_{p=0}^{k-1} pp^i c_p x^{p-1}\right] \\ &= k^{i+1}x^k - \sum_{p=0}^{k-1} p^{i+1} c_p x^p \end{aligned}$$

De plus ; d'après le lemme précédent, on a $P_i(\alpha) = 0$; $\forall i = \overline{0,\ m-1}$. Alors

$$\sum_{p=0}^{k-1} p^i c_p \alpha^p = k^i \alpha^k$$

ii) un calcul direct donne

$$\begin{aligned} \sum_{p=1}^{k} c_{k-p}\, p^i \alpha^{k-p} &= \sum_{p'=0}^{k-1} c_{p'}\,(k-p')^i\, \alpha^{p'} \text{ (en posant } p' = k-p) \\ &= \sum_{t=0}^{i} (-1)^t\, C_i^t k^{i-t} \sum_{p'=0}^{k-1} c_{p'} p'^t \alpha^{p'} \end{aligned}$$

Et par le lemme précédent, on aura

$$\sum_{p'=0}^{k-1} c_{p'} p'^t \alpha^{p'} = k^t \alpha^k$$

Alors

$$\sum_{p=1}^{k} c_{k-p}\, p^i \alpha^{k-p} = \sum_{t=0}^{i} (-1)^t\, C_i^t k^{i-t} k^t \alpha^k = k^i \alpha^k \sum_{t=0}^{i} (-1)^t\, C_i^t = 0$$

iii) On a

$$\begin{aligned}
\sum_{p=1}^{k} c_{k-p}\,(n-p)^j\,\alpha^{k-p} &= \sum_{p=1}^{k} c_{k-p} \sum_{t=0}^{j} C_j^t n^{j-t}\,(-p)^t\,\alpha^{k-p} \\
&= \sum_{t=0}^{j} C_j^t n^{j-t}\,(-1)^t \sum_{p=1}^{k} c_{k-p} p^t \alpha^{k-p} \\
&= \sum_{t=0}^{j} C_j^t n^{j-t}\,(-1)^t \sum_{p'=0}^{k-1} c_{p'}\,(k-p')^t\,\alpha^{p'} \\
&= \sum_{t=0}^{j} C_j^t n^{j-t}\,(-1)^t \sum_{i=0}^{t} (-1)^i\, C_t^i k^{t-i} \sum_{p'=0}^{k-1} c_{p'} p'^i \alpha^{p'} \\
&= \sum_{t=0}^{j} C_j^t n^{j-t}\,(-1)^t \sum_{i=0}^{t} (-1)^i\, C_t^i k^{t-i} k^i \alpha^k \\
&= n^j \alpha^k + \sum_{t=1}^{j} C_j^t n^{j-t}\,(-1)^t\, k^t \alpha^k \sum_{i=0}^{t} (-1)^i\, C_t^i \\
&= n^j \alpha^k \qquad \text{(c.q.f.d)}
\end{aligned}$$

Complété de la preuve du théorème(3.1.2)

Supposons que $(u_n)_{n\in\mathbb{N}}$ s'écrit sous la forme

$$u_n = \sum_{i=1}^{r} P_i(n)\,\alpha_i^n$$

Où $\alpha_1, \alpha_2, ..., \alpha_r$ sont les racines distinctes de $P(x) = x^k - c_{k-1}x^{k-1} - ... - c_1 x - c_0$ avec multiplicités n_1, n_2,..., n_r respectivement et $d\acute{e}gr\acute{e}(P_i) \le n_i - 1$. Alors

$$\begin{aligned}
&\forall\, n \ge k\,;\; u_n - c_{k-1}u_{n-1} - c_{k-2}u_{n-2} - ... - c_0 u_{n-k} \\
&= \sum_{i=1}^{r} P_i(n)\,\alpha_i^n - \sum_{s=1}^{k} c_{k-s} \sum_{i=1}^{r} P_i(n-s)\,\alpha_i^{n-s} \qquad (3.10)
\end{aligned}$$

En posons $c_k = -1$ et $P_i(x) = \sum_{j=0}^{n_i-1} p_{ij}\,x^j$, il s'ensuit que (3.10) s'écrit

$$\begin{aligned}
-\sum_{s=0}^{k} c_{k-s} \sum_{i=1}^{r} P_i(n-s)\,\alpha_i^{n-s} &= -\sum_{i=1}^{r}\sum_{s=0}^{k}\sum_{j=0}^{n_i-1} p_{ij}\,(n-s)^j\,c_{k-s}\alpha_i^{n-k}\alpha_i^{k-s} \\
&= -\sum_{i=1}^{r} \alpha_i^{n-k} \sum_{j=0}^{n_i-1} p_{ij} \sum_{s=0}^{k} c_{k-s}\,(n-s)^j\,\alpha_i^{k-s}
\end{aligned}$$

En utilisant le lemme précédent, on obtient

$$\sum_{s=0}^{k} c_{k-s}\,(n-s)^j\,\alpha_i^{k-s} = -n^j\alpha_i^k + \sum_{s=1}^{k} c_{k-s}\,(n-s)^j\,\alpha_i^{k-s} = -n^j\alpha_i^k + n^j\alpha_i^k = 0$$

$$\Longrightarrow u_n = c_{k-1}u_{n-1} + c_{k-2}u_{n-2} + ... + c_0 u_{n-k}\,;\ \forall n \geq k$$

■

Exemple 3.1.7 1) *Trouver la formule de solution de la suite de Fibonacci définie par*

$$F_n = F_{n-1} + F_{n-2};\ F_0 = 0 \text{ et } F_1 = 1$$

Le polynôme caractéristique de la suite $(F_n)_{n\in\mathbb{N}}$ *est* $x^2 - x - 1$. *Ses racines sont*

$$\alpha_1 = \frac{1+\sqrt{5}}{2}\,;\ \alpha_2 = \frac{1-\sqrt{5}}{2}$$

De plus, α_1 *et* α_2 *sont de multiplicités* 1. *Alors, d'après le théorème* (3.1.2) *le terme général de la suite est donné par*

$$F_n = c_1\alpha_1^n + c_2\alpha_2^n$$

En utilisant les conditions initiales $F_0 = 0\,;\ F_1 = 1$, *on obtient le système suivant*

$$\begin{cases} c_1 + c_2 = 0 ...* \\ c_1\alpha_1 + c_2\alpha_2 = 1 ... ** \end{cases}$$

Alors, on obtient

$$c_2(\alpha_2 - \alpha_1) = 1 \Longrightarrow -c_2\sqrt{5} = 1 \Longrightarrow c_2 = \frac{-1}{\sqrt{5}}$$

D'autre part

$$c_1 + c_2 = 0 \Longrightarrow c_1 = \frac{1}{\sqrt{5}}$$

Alors; F_n *s'écrit*

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Remarque 3.1.8 *i) Nous voyons bien que* $(F_n)_{n\in\mathbb{N}}$ *est à termes entiers; alors que la forme de solution de* F_n *est un nombre algébrique, ce qui signifie que la formule donnant la solution d'une suite linéaire récurrente est généralement une forme approchée.*
ii) On a $\left|\frac{1-\sqrt{5}}{2}\right| < 1 \Longrightarrow \lim_{n\longrightarrow\infty}\left(\frac{1-\sqrt{5}}{2}\right)^n = 0$. *Alors, au voisinage de l'infini, la formule précédente peut être réduite à*

$$F_n \cong \frac{1}{\sqrt{5}}\alpha_1^n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n$$

i) La suite de Lucas du premier type est donnée par

$$u_{n+2} = Mu_{n+1} - Nu_n$$

avec M, $N \in \mathbb{Z}$ et $u_0 = 0$, $u_1 = 1$. Soient $\beta_1 = \frac{M+\sqrt{M^2-4N}}{2}$; $\beta_2 = \frac{M-\sqrt{M^2-4N}}{2}$ les racines du polynôme caractéristique $P(x) = x^2 - Mx + N$. Alors, la formule de solution de la suite de Lucas est

$$u_n = c_1\beta_1^n + c_2\beta_2^n$$

Et avec les conditions initiales précédentes, on obtient le système suivant

$$\begin{cases} c_1 + c_2 = 0 \\ c_1\beta_1 + c_2\beta_2 = 1 \end{cases} \Longrightarrow \begin{cases} c_1 = -c_2 \\ c_1(\beta_1 - \beta_2) = 1 \end{cases}$$

$$\Longrightarrow c_1 = \frac{1}{\beta_1 - \beta_2}\,;\, c_2 = -\frac{1}{\beta_1 - \beta_2}$$

Ainsi, la suite $(u_n)_n$ s'écrit sous la forme

$$u_n = \frac{\beta_1^n + \beta_2^n}{\beta_1 - \beta_2}$$

ii) La suite de Lucas du deuxième type est définie par $V_{n+2} = MV_{n+1} - NV_n$; $V_0 = 2$, $V_1 = M$. Soient β_1, β_2 les racines de son polynôme caractéristique. On sait que $(V_n)_{n\in\mathbb{N}}$ s'écrit sous la forme

$$V_n = c_1\beta_1^n + c_2\beta_2^n$$

Pour déterminer les constantes c_1, c_2; on utilise les conditions initiales $V_0 = 2$, $V_1 = M$ et on obtient le système suivant

$$\begin{cases} c_1 + c_2 = 2 \\ c_1\beta_1 + c_2\beta_2 = M \end{cases} \Longrightarrow \begin{cases} c_2 = 2 - c_1 \\ c_1\beta_1 + (2 - c_1)\beta_2 = M \end{cases}$$

$$\Longrightarrow \begin{cases} c_2 = 2 - c_1 \\ c_1(\beta_1 - \beta_2) = M - 2\beta_2 = \beta_1 - \beta_2 \end{cases} \Longrightarrow \begin{cases} c_1 = 1 \\ c_2 = 1 \end{cases}$$

D'où

$$V_n = \beta_1^n + \beta_2^n$$

Dans toute l'étude qui reste la formule de solution $u_n = \sum_{i=1}^{r} P_i(n)\,\alpha_i^n$ sera l'outil principal. Voici quelques propriétés de cette formule.

Proposition 3.1.9 *Soit $u_n = \sum_{i=1}^{r} P_i(n)\,\alpha_i^n$ la formule de solution d'une suite linéaire récurrente $(u_n)_{n\in\mathbb{N}}$ d'ordre k définie par* (3.1). *Si $\alpha_{i_2} = \overline{\alpha_{i_1}}$, alors $P_{i_2}(x) = \overline{P_{i_1}(x)}$ où $\overline{P_{i_1}(x)}$ est le polynôme déduit de $P_{i_1}(x)$ en remplaçant chaque coefficient par son conjugué complexe.*

Preuve. Sans perdre de généralité, on peut supposer que $c_0 \neq 0$ et dans ce cas toutes les racines α_i, $\overline{i=1,\ r}$ sont différentes de zéro. Posons

$$P_i(x) = \sum_{j=0}^{n_i-1} p_{ij} x^j \text{ (puisque } \textit{dégré}(P_i) \leq n_i - 1)$$

Alors, pour déterminer les polynômes $P_i(x)$, il suffit de déterminer les coéfficients p_{ij}. Or les p_{ij}, $1 \leq i \leq r$ et $0 \leq j \leq n_i - 1$ sont les inconnues d'un système de k équations linéaires obtenues à partir de la forme

$$u_n = \sum_{i=1}^{r} P_i(n)\, \alpha_i^n$$

Et les conditions initiales u_0, ..., u_{k-1}. La formule précédente peut s'écrire donc comme suit

$$u_n = \sum_{i=1}^{r} P_i(n)\, \alpha_i^n = \sum_{i=1}^{r} \sum_{j=0}^{n_i-1} p_{ij} n^j \alpha_i^n \tag{3.11}$$

Pour $n = 0,..., k-1$; on obtient un système de k équations linéaires dont son déterminant est

$$\begin{vmatrix} 1 & 0 & . & 1 & 0 & . & 0 \\ \alpha_1 & \alpha_1 & . & \alpha_r & \alpha_r & . & \alpha_r \\ \alpha_1^2 & 2\alpha_1^2 & . & \alpha_r^2 & 2\alpha_r^2 & . & 2^{n_r-1}\alpha_r^2 \\ \alpha_1^3 & 3\alpha_1^3 & . & \alpha_r^3 & 3\alpha_r^3 & . & 3^{n_r-1}\alpha_r^3 \\ . & . & . & . & . & . & . \\ \alpha_1^{k-1} & (k-1)\,\alpha_1^{k-1} & . & \alpha_r^{k-1} & (k-1)\,\alpha_r^{k-1} & . & (k-1)^{n_r-1}\,\alpha_1^{k-1} \end{vmatrix} \tag{3.12}$$

$*$ On va montrer que le déterminant (3.12) n'est pas nul, ce qui signifie que les coéfficients p_{ij} sont uniques. Pour cela, il suffit de démontrer que les lignes de (3.12) sont linéairement indépendantes.

Supposons donc qu'il existe des constantes a_0, ..., a_{k-1} tels que

$$\sum_{l=0}^{k-1} a_l l^i \alpha_j^l = 0;\ \forall\ \overline{j=1,\ r} \text{ et } i = \overline{0,\ n_j - 1} \tag{3.13}$$

En notant

$$C(x) = \sum_{l=0}^{k-1} a_l x^l \tag{3.14}$$

Et en posant $C_0(x) = C(x)$, $C_{i+1}(x) = xC_i'(x)$; $\forall i \geq 0$, on obtient

$$C_i(x) = \sum_{l=0}^{k-1} a_l l^i x^l$$

En effet. Cette relation peut être démontrer par récurrence.
* Pour $i = 0$, on a $\sum_{l=0}^{k-1} a_l l^0 x^l = \sum_{l=0}^{k-1} a_l x^l = C_0(x)$. Soit maintenant $C_i(x) = \sum_{l=0}^{k-1} a_l l^i x^l$ pour quelques i. On a

$$C_{i+1}(x) = xC_i'(x) = x\sum_{l=0}^{k-1} a_l l^i l x^{l-1} = \sum_{l=0}^{k-1} a_l l^{i+1} x^l$$

Donc, par induction on conclut que

$$\boxed{C_i(x) = \sum_{l=0}^{k-1} a_l l^i x^l}$$

Les équations (3.13) s'écrivent $C_i(\alpha_j) = 0$; $\forall\ \overline{j = 1, r}$ et $\overline{i = 0, n_j - 1}$. Le lemme (3.1.5) implique que $C(x)$ est divisible par $(x-\alpha_1)^{n_1}$, $(x-\alpha_2)^{n_2}$, ..., $(x-\alpha_r)^{n_r}$ et on écrit donc

$$C(x) = (x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\ldots(x-\alpha_r)^{n_r} q(x)$$

pour un polynôme $q(x)$. On conclut que, soit *dégré* $(C(x)) \geq n_1 + \ldots + n_r$, soit $C(x) = 0$. D'après (3.14), on a *dégré* $(C(x)) < k$, et on en déduit donc que $C(x) = 0$. ie.,

$$a_0 = a_1 = \ldots = a_{k-1} = 0$$

Le reste de la démonstration de la proposition (3.1.9) repose sur la proposition suivante. ∎

Proposition 3.1.10 *Le déterminant* (3.12) *est, ou bien appartient à* $\mathbb{R}$ *ou bien appartient à* $i\mathbb{R}$.

Preuve. On sait que si α est une racine de $P(x) \in \mathbb{R}[x]$, alors $\overline{\alpha}$ est aussi une racine de $P(x)$ de même multiplicité que celle de α. Notons, maintenant par Δ le déterminant (3.12). Il est clair que $\overline{\Delta}$ s'obtient en prenant les conjugués de toutes les entrées de Δ. D'autre part, si $\alpha_i \in \mathbb{C}$ est une racine de $P(x)$ qui intervient exactement dans s colonnes de Δ; alors il existe s colonnes de Δ qui s'identifient à ces s premières colonnes, en remplaçant α_i par $\overline{\alpha_i}$ (ceci vient du fait que $\alpha_i, \overline{\alpha_i}$ ont la même multiplicité). En échangeant toutes les n_i colonnes où α_i intervient avec celles de $\overline{\alpha_i}$, on peut modifier $\overline{\Delta}$ de telle sorte que les colonnes contenant α_i et $\overline{\alpha_i}$ sont placées comme dans leurs places usuelles dans Δ. En répétant le même procédé avec toutes les racines complexes de $P(x)$; on obtient le même déterminant Δ, puisque les lignes contenant des racines réelles ne s'affectent plus quand on prend les conjugués. Donc s'il y a r racines complexes distinctes $\alpha_1,\ldots, \alpha_r$ de multiplicité respectivement $n_1,\ldots, n_r$; alors ses conjugués $\overline{\alpha_1},\ldots, \overline{\alpha_r}$ sont aussi des racines de même multiplicité $n_1,\ldots, n_r$ et on obtient

$$\overline{\Delta} = (-1)^{n_1+\ldots+n_r}\Delta$$

Ce qui signifie que : si $n_1 + \ ... + n_r$ est pair, alors

$$\Delta = \overline{\Delta} \Longrightarrow \Delta \in \mathbb{R}$$

Et si $n_1 + \ ... + n_r$ est impair, alors

$$\Delta = -\overline{\Delta} \Longrightarrow \Delta \in i\mathbb{R} \qquad \text{(c.q.f.d)}$$

Revenons, maintenant à la démonstration de la proposition (3.1.9). Les coéfficients p_{ij} peuvent être calculer par le principe de Cramer. On sait que $p_{ij} = \frac{\Delta_{ij}}{\Delta}$ où Δ_{ij} est le déterminant obtenu à partir de Δ en remplaçant la colonne $\left(0^j\alpha_i^0, 1^j\alpha_i^1, ..., (k-1)^j\alpha_i^{k-1}\right)^T$ de Δ par $(u_0, u_1, ..., u_{k-1})^T$. Si $\alpha_{i_2} = \overline{\alpha_{i_1}}$, on voit que le déterminant $\Delta_{i_2 j}$ peut être obtenir à partir de $\Delta_{i_1 j}$ en : 1) Prenant le conjugué de chaque entrée de $\Delta_{i_1 j}$.
2) Echangeant $k = n_1 + ... + n_r$ colonnes. Il s'ensuit que $\Delta_{i_2 j} = (-1)^k\overline{\Delta_{i_1 j}}$. De plus, on a $\Delta = (-1)^k\overline{\Delta}$, ce qui donne

$$\overline{p_{i_1 j}} = \frac{\overline{\Delta_{i_1 j}}}{\overline{\Delta}} = \frac{(-1)^k\Delta_{i_2 j}}{(-1)^k\Delta} = \frac{\Delta_{i_2 j}}{\Delta} = p_{i_2 j} \qquad \text{(c.q.f.d)}$$

Maintenant, on va s'intéresser à la structure de l'ensemble des zéros d'une suite linéaire récurrente. ■

Notation 3.1.11 *On note par $\mathbb{Z}(u_n)$ l'ensemble des zéros d'une suite linéaire récurrente. ie.,*

$$\mathbb{Z}(u_n) = \{i \in \mathbb{N} : u_i = 0\}$$

Lemme 3.1.12 Soit $(u_n)_{n\in\mathbb{N}}$ une suite récurrente linéaire à termes entiers, alors les assertions suivantes sont équivalentes.

1) *La suite $(u_n)_{n\in\mathbb{N}}$ est linéaire récurrente d'ordre k.*

2) *Pour $n \geq 1$: $u_n = (M^n)_{1,k}$ où $M \in \mathbb{Z}^{k.k}$ est une matrice carrée d'ordre k dans $\mathbb{Z}$ et $(M^n)_{1,k}$ est l'élément de M^n situé à la première ligne et $k-$ ième colonne.*

3) *$\forall n \geq 1 : u_n = VM^NW^T$ où $V, W \in \mathbb{Z}^k$ et $M \in \mathbb{Z}^{k.k}$ pour quelque k.*

Le théorème suivant donne la structure de l'ensemble $\mathbb{Z}(u_n)$.

Théorème 3.1.13 *(de Skolem-Mahler-Lech) Soit $(u_n)_n \subset \mathbb{C}$ une suite linéaire récurrente et soit $\mathbb{Z}(u_n)$ l'ensemble des zéros de $(u_n)_n$. Alors $\mathbb{Z}(u_n)$ est une réunion finie d'un ensemble fini et d'un nombre fini de progressions arithmétiques où une progression arithmétique désigne un ensemble de la forme $A = \{ax + b, x \in \mathbb{Z}\}$ et a, b des entiers fixés avec $a > 0$.*

Remarque 3.1.14 *Quelques progressions arithmétiques peuvent être de raison nul.*

* *Pour démontrer ce théorème, on va suivre un processus dû à G .Hensel. La preuve de Hensel s'appuie sur le théorème suivant.*

Théorème 3.1.15 *Soit $p \succ 2$ un nombre premier et soit $(a_i)_{i\in\mathbb{N}}$ une suite d'entiers. Posons*

$$b_n = \sum_{i=0}^{n} C_n^i p^i a_i$$

Alors, si $b_n = 0$ pour un nombre fini d'indices n, on aura $b_n = 0$ pour tout n de $\mathbb{N}$.

Pour démontrer le théorème (3.1.15), *on a besoin des lemmes et définition suivants.*

Lemme 3.1.16 *Soit p un nombre premier et $n \in \mathbb{Z}$. Alors,*

$$V_p\left(\frac{p^n}{n!}\right) \geq n\frac{p-2}{p-1}$$

Preuve. D'après le calcul de $V_p(n!)$ (voir chapitre 1), on sait que

$$V_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + ... + ... \leq \frac{n}{p} + \frac{n}{p^2} + ...+ = \frac{n}{p-1}$$

Or

$$V_p\left(\frac{p^n}{n!}\right) = V_p(p^n) - V_p(n!) \geq n - \frac{n}{p-1} = n\,\frac{p-2}{p-1} \qquad \text{(c.q.f.d)}$$

■

Définition 3.1.17 *Soit $P(x) = c_0 + c_1x + ... + c_nx^n \in \mathbb{Q}[x]$ un polynôme et définissons $W_k(P)$ comme suit*

$$W_k(P) = \begin{cases} \min\{V_p(c_i)\,;\ i \geq k\}, & si\ k \leq n \\ \infty, & si\ k > n \end{cases}$$

Remarque 3.1.18 *Pour une valeur fixée $P(t) \in \mathbb{Q}$ ($t \in \mathbb{Z}$), on a*

$$\begin{aligned} V_p(P(t)) &= V_p(c_0 + c_1t + ... + c_nt^n) \\ &\geq \min\{V_p(c_0), V_p(c_1t), ..., V_p(c_nt^n)\} \\ &\geq \min\{V_p(c_0), V_p(c_1), ..., V_p(c_n)\} = W_0(P) \end{aligned}$$

Lemme 3.1.19 *Soit $P(x)$, $r(x)$ des polynômes de $\mathbb{Q}[x]$ et soit n_1,..., $n_k \in \mathbb{Z}$. Supposons que $P(x) = (x - n_1)...(x - n_k)\,r(x)$; alors*

$$W_k(P) \leq W_0(r)$$

Preuve. Il suffit de montrer que, si $P(x) = (x - n_1)\, r(x)$, alors $W_{k+1}(P) \leq W_k(r)$, pour tout k de $\mathbb{N}$. Posons

$$P(x) = p_0 + p_1 x + ... + p_{n+1} x^{n+1} \text{ et } r(x) = r_0 + r_1 x + ... + r_n x^n$$

* On a $P(x) = (x - n_1)\, r(x)$ qui donne $p_{i+1} = r_i - n_1 r_{i+1}$, et par conséquent on obtient

$$r_i = p_{i+1} + n_1\, p_{i+2} + n_1^2\, p_{i+3} + ... + n_1^{n-i}\, p_{n+1}$$

D'où

$$\begin{aligned} V_p(r_i) &= V_p(p_{i+1} + n_1 p_{i+2} + n_1^2 p_{i+3} + ... + n_1^{n-i} p_{n+1}) \\ &\geq \min\{V_p(p_{i+1}), V_p(p_{i+2}), ..., V_p(p_{n+1})\} = W_{i+1}(P) \end{aligned}$$

Il s'ensuit que

$$\begin{aligned} W_k(r) &= \min\{V_p(r_i),\, i \geq k\} \geq \min\{V_p(p_i),\, i \geq k+1\} \\ &\Longrightarrow W_k(r) \geq W_{k+1}(P) \end{aligned}$$

D'autre part, si $r(x) = (x - n_2)\, q(x)$, on obtient encore $W_k(r) \leq W_{k-1}(q)$ et ainsi de suite. On obtient par itération la relation suivante

$$W_{k+1}(P) \leq W_k(r) \leq W_{k-1}(q) \leq ... \leq W_0(r)$$

■

Lemme 3.1.20 *Soit $r(x) \in \mathbb{Q}[x]$ un polynôme défini par $r(x) = \sum_{i=0}^{n} a_i\, p^i\, \frac{x(x-1)...(x-i+1)}{i!}$, $n \in \mathbb{N}$ fixé. Alors*

$$\forall\, k \in \mathbb{N} : W_k(r) \geq k\frac{p-2}{p-1}$$

Preuve. On voit que $r(x)$ peut s'écrire comme suit

$$\begin{aligned} r(x) &= \sum_{i=0}^{n} a_i\, \frac{p^i}{i!}\, x(x-1)...(x-i+1) \\ &= \sum_{i=0}^{n} a_i \frac{p^i}{i!} \sum_{j=0}^{i} b_{ij} x^j = \sum_{j=0}^{n} \sum_{i=j}^{n} a_i \frac{p^i}{i!} b_{ij} x^j \end{aligned}$$

Où b_{ij} sont des entiers appelés *nombres de Stirling* du premier type. Par conséquent, le coéfficient de x^j dans $r(x)$ est donné par $\sum_{i=j}^{n} a_i\, \frac{p^i}{i!}\, b_{ij}$. Et de plus, on a

$$\begin{aligned} V_p(\sum_{i=j}^{n} a_i\, \frac{p^i}{i!}\, b_{ij}) &\geq \min_{i \geq j}\left\{V_p(a_i\, \frac{p^i}{i!}\, b_{ij})\right\} \geq \min_{i \geq j}\left\{V_p(\frac{p^i}{i!})\right\} \\ &\geq \min_{i \geq j}\left\{i\frac{p-2}{p-1}\right\} \geq j\, \frac{p-2}{p-1} \end{aligned}$$

D'où

$$\min_{k>j}\left\{V_p(\sum_{i=k}^{n}a_i\,\frac{p^i}{i!}\,b_{ik})\right\}=W_j(r)\geq j\,\frac{p-2}{p-1}\qquad\text{(c.q.f.d)}$$

■

Preuve. (du théorème 3.1.15) On va montrer que, si $b_n=0$ pour $n\in\{n_1,...,n_r\}$, alors

$$V_p(b_n)\geq k\,\frac{p-2}{p-1},\ \forall\, b_n\in\mathbb{Z}$$

Soit $n=\max\{n_1,...,n_r\}$. Alors, $\forall t\leq n$; on a $r(t)=\sum_{i=0}^{n}C_t^ip^ia_i=\sum_{i=0}^{t}C_t^ip^ia_i=b_t$ et puisque $b_t=0$, $\forall t\in\{n_1,...,n_r\}$; on aura $r(n_1)=...=r(n_r)=0$. ie., $(x-n_1)...(x-n_r)$ divise $r(x)$, ce qui donne

$$r(x)=(x-n_1)...(x-n_r)\,q(x)$$

pour un polynôme $q(x)$. De plus, on a $V_p(r(t))\geq V_p(q(t))$; et on obtient enfin

$$V_p(b_t)=V_p(r(t))\geq V_p(q(t))\geq W_0(q)\geq W_k(r)\geq k\,\frac{p-2}{p-1}\qquad\text{(c.q.f.d)}$$

Maintenant, puisque k peut être choisi infiniment grand ; on en déduit que $V_p(b_n)=\infty$. C'est-à-dire

$$\|b_n\|_p=0,\ \forall b_n\in\mathbb{Z}\implies b_n=0\,;\ \forall\, n\in\mathbb{N}$$

Et donc le théorème (3.1.15) s'ensuit. ■

Preuve. (du théorème de Skolem – Mahler – Lech)

Supposons que $(u_n)_{n\in\mathbf{N}}$ est donnée par la relation de récurrence

$$u_n=c_{k-1}u_{n-1}+c_{k-2}u_{n-2}+...+c_0u_{n-k}\,;\ \forall n\geq k$$

De plus, on peut supposer que $c_0\neq 0$. D'après le lemme (3.1.12), il existe V, $W\in\mathbb{Z}^k$ et une matrice $M\in\mathbb{Z}^{k.k}$ tels que $u_n=VM^nW^T$. De plus, on a $\det(M)=\pm c_0\neq 0$. Choisissons un nombre premier p ne divisant pas c_0. Soit M_p l'image de M dans $F_p^{k.k}$ par la projection $P:\mathbb{Z}\longrightarrow F_p$. ie : $M_p=P(M)$. Puisque $p\nmid c_0$, alors $\det(M_p)\neq 0$. D'autre part, le cardinal du groupe des matrices carrées inversibles d'ordre k sur F_p est au plus p^{k^2}. Alors

$$\exists N\leq p^{k^2}\text{ tel que : }\ M_p^N=I$$

Où M_p est un élément de l'ensemble des matrices inversibles dans F_p. Dans $\mathbb{Z}$, l'équation $M_p^N=I$ implique qu'il existe $N\leq p^{k^2}$ et $M_1\in\mathbb{Z}^{k.k}$ tels que

$$M^N=I+pM_1$$

Soit $n \in \mathbb{N} \Longrightarrow n = mN + r$ (division euclidienne de n par N) ; alors l'équation précédente donne

$$M^n = M^{mN+r} = M^{mN} M^r = (I + pM_1)^m M^r$$

$$\Longrightarrow u_n = V M^n W^T = V (I + pM_1)^m M^r W^T$$

$$\Longrightarrow u_{mN+r} = V (I + pM_1)^m W_r^T$$

Où $W_r^T = M^r W^T$. On peut donc partager la suite $(u_n)_{n\in\mathbb{N}}$ en N sous-suites linéaires récurrentes différentes $u_m^{(r)}$, $\forall r \in \{0, ..., N-1\}$, en définissant

$$u_m^{(r)} = u_{mN+r} = V (I + pM_1)^m W_r^T = \sum_{i=0}^{m} C_m^i p^i V M_1^i W_r^T$$

D'après, le théorème (3.1.15) chaque suite $(u_m^{(r)})_{n\in\mathbb{N}}$ est ou bien identiquement nulle ou bien a un nombre fini de zéros. Pour affirmer que $(u_m^{(r)})_n$ est identiquement nulle, il suffit de calculer ses k premiers termes. On en déduit que

$$\mathbb{Z}(u_n) = E \bigcup_{0\leq r\prec N} \{mN + r\} \text{ où } E \text{ est un ensemble fini} \qquad \text{(c.q.f.d)}$$

Applications : ◘

Exemple 3.1.21 *Soit $(a_n)_{n\in\mathbb{N}}$ une suite définie par $a_0 = a_4 = 8$; $a_1 = a_3 = a_5 = 0$; $a_2 = 9$ et par la relation de récurrence*

$$\forall n \geq 6 : a_n = 6a_{n-2} - 12a_{n-4} + 8a_{n-6}$$

Soit $S_a(x)$ la fonction génératrice donnée par $S_a(x) = 1 - 6x^2 + 12x^4 - 8x^6$. On a

$$S_a(x) = \left(1 - \sqrt{2}\, x\right)^3 \left(1 + \sqrt{2}\, x\right)^3$$

Alors, il existe P_1, $P_2 \in \mathbb{Q}[x]$ avec dégré$(P_1) \leq 2$, dégré$(P_2) \leq 2$ tels que

$$a_n = \left(\sqrt{2}\right)^n P_1(n) + \left(-\sqrt{2}\right)^n P_2(n)$$

Posons $P_1(x) = r_0 + r_1 x + r_2 x^2$ et $P_2(x) = t_0 + t_1 x + t_2 x^2$. On obtient alors le système suivant

$$\begin{cases} r_0 + t_0 = 8 \\ \sqrt{2}\,(r_0 + r_1 + r_2 - t_0 - t_1 - t_2) = 0 \\ 2\,(r_0 + 2r_1 + 4r_2 + t_0 + 2t_1 + 4t_2) = 9 \\ \cdots \\ 4\sqrt{2}\,(r_0 + 5r_1 + 25r_2 - t_0 - 5t_1 - 25t_2) = 0 \end{cases}$$

$$\Longrightarrow \begin{cases} r_0 = 4;\ r_1 = -1;\ r_2 = \frac{1}{16} \\ t_0 = 4;\ t_1 = -1;\ t_2 = \frac{1}{16} \end{cases}$$

$$\Longrightarrow \forall n \in \mathbb{N} : a_n = \left(\sqrt{2}\right)^n (4 - n + \frac{n^2}{16})(1 + (-1)^n)$$

Et par conséquent, on conclut que

$$a_n = 0 \iff \begin{cases} 4 - n + \frac{n^2}{16} = 0 \ ou \\ 1 + (-1)^n = 0 \end{cases} \iff \begin{cases} n = 8 \ ou \\ n = 2p + 1,\ p \in \mathbb{N} \end{cases}$$

$$\iff \mathbb{Z}(a_n) = \{8\} \cup \{1 + 2\mathbb{N}\}$$

Exemple 3.1.22 *Soit $(b_n)_n$ une suite définie par*

$$\begin{cases} \forall n \geq 3 : b_n = -3b_{n-1} + 9b_{n-2} - 54b_{n-3} \\ b_0 = 0,\ b_1 = 3,\ b_2 = 9 \end{cases}$$

La fonction génératrice de $(b_n)_n$ est

$$\begin{aligned} S_b(x) &= 1 + 3x - 9x^2 + 54x^3 \\ &= (1 + 6x)\left(1 - 3\frac{1 + i\sqrt{3}}{2}x\right)\left(1 - 3\frac{1 - i\sqrt{3}}{2}x\right) \end{aligned}$$

Alors

$$\forall n \in \mathbb{N} : b_n = \lambda_1(-6)^n + \lambda_2\left(3\frac{1 + i\sqrt{3}}{2}\right)^n + \lambda_3\left(3\frac{1 - i\sqrt{3}}{2}\right)^n \ où\ \lambda_1, \lambda_2, \lambda_3 \in \mathbb{C}$$

En utilisant les conditions initiales, on obtient le système suivant

$$\begin{cases} \lambda_1 + \lambda_2 + \lambda_3 = 0 \\ -6\lambda_1 + 3\frac{1+i\sqrt{3}}{2}\lambda_2 + 3\frac{1-i\sqrt{3}}{2}\lambda_3 = 3 \\ 36\lambda_1 + \left(3\frac{1+i\sqrt{3}}{2}\right)^2\lambda_2 + \left(3\frac{1-i\sqrt{3}}{2}\right)^2\lambda_3 = 9 \end{cases}$$

$$\Longrightarrow \begin{cases} \lambda_1 = 0 \\ \lambda_2 = -\lambda_3 = -\frac{i\sqrt{3}}{3} \end{cases}$$

$$\begin{aligned} \Longrightarrow \quad b_n &= (-\frac{i\sqrt{3}}{3})\left(3\frac{1 + i\sqrt{3}}{2}\right)^n + (\frac{i\sqrt{3}}{3})\left(3\frac{1 - i\sqrt{3}}{2}\right)^n \\ &= 3^n(\frac{i\sqrt{3}}{3})\left[\left(\frac{1 - i\sqrt{3}}{2}\right)^n - \left(\frac{1 + i\sqrt{3}}{2}\right)^n\right] \end{aligned}$$

Donc

$$\begin{aligned} b_n = 0 &\iff \left(\frac{1-i\sqrt{3}}{2}\right)^n - \left(\frac{1+i\sqrt{3}}{2}\right)^n = 0 \\ &\iff \left[\left(\frac{1+i\sqrt{3}}{2}\right)^5\right]^n - \left(\frac{1+i\sqrt{3}}{2}\right)^n = 0 \\ &\iff \left[\left(\frac{1+i\sqrt{3}}{2}\right)^4\right]^n = 1 \\ &\iff e^{2in\frac{\pi}{3}} = 1 = e^{i2\pi k} \iff 3/n \end{aligned}$$

Ce qui implique que

$$\mathbb{Z}(b_n) = 3\mathbb{N}$$

Exemple 3.1.23 *Soit $(c_n)_{n\geq 0}$ une suite donnée par les valeurs initiales $c_0 = 0$, $c_1 = 0$, $c_2 = 1$, $c_3 = 0$ et la relation de récurrence suivante*

$$\forall n \geq 4 : c_n = 3c_{n-2} - c_{n-4}$$

Sa fonction génératrice est

$$S_c(x) = 1 - 3x^2 + x^4 = (1 - \frac{1+\sqrt{5}}{2}x)(1 - \frac{1-\sqrt{5}}{2}x)(1 + \frac{1+\sqrt{5}}{2}x)(1 + \frac{1-\sqrt{5}}{2}x)$$

$$\begin{aligned} \Longrightarrow c_n &= \frac{1}{2\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n + \left(-\frac{1+\sqrt{5}}{2}\right)^n - \left(-\frac{1-\sqrt{5}}{2}\right)^n\right] \\ &= \frac{1}{2\sqrt{5}}(1+(-1)^n)\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right] \end{aligned}$$

Alors

$$\begin{aligned} c_n = 0 &\iff \begin{cases} 1+(-1)^n = 0 \\ \left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n = 0 \end{cases} \\ &\iff \begin{cases} n = 2p+1\ ,\ p \in \mathbb{N} \\ n = 0 \end{cases} \\ &\iff \mathbb{Z}(c_n) = \{0\} \cup \{2\mathbb{N}+1\} \end{aligned}$$

Corollaire 3.1.24 *Soit $(u_n)_n$ une suite linéaire récurrente d'ordre k dont les racines $\alpha_1, \ldots, \alpha_r$ du polynôme caractéristique de $(u_n)_n$ sont distinctes. S'il existe un i_0, $1 \leq i_0 \leq r$ tel que $\frac{\alpha_j}{\alpha_{i_0}}$ n'est pas une racine de l'unité pour tout $j \neq i_0$, alors $\mathbb{Z}(u_n)$ est fini.*

Preuve. Par le théorème (3.1.2), on sait qu'il existe des polynômes $P_1(x)$, $P_2(x)$,..., $P_r(x) \in \mathbb{C}[x]$ tels que

$$u_n = \sum_{i=1}^{r} P_i(n)\,\alpha_i^n \text{ avec } dégré(P_i) = n_i - 1$$

* En groupant les termes $P_i(x)\,\alpha_i^n$, $P_j(x)\,\alpha_j^n$ tels que $\frac{\alpha_i}{\alpha_j}$ est une racine de l'unité on peut écrire

$$u_n = f_1(n) + ... + f_s(n)$$

Où $f_i(n) = P_{i1}(n)\alpha_{i1}^n + ... + P_{ik_i}(n)\alpha_{ik_i}^n$, $\forall i$; $1 \leq i \leq s$ et $k_1 + ... + k_s = k$. De plus, on a

$$\forall i,\ 1 \leq i \leq s \text{ et } l,\ 1 \leq l \leq k_i\ ;\ \frac{\alpha_{ij}}{\alpha_{i'l}} \text{ est une racine de l'unité} \iff i = i'$$

* Supposons que $u_n = 0$ pour tout n de $A = \{ax + b\}$ où a, b, $x \in \mathbb{Z}$ et $a \succ 0$. Soit $m \in \mathbb{N}$; alors $\left(\frac{\alpha_{ij}}{\alpha_{jl}}\right)^m = 1$ pour tout i, j, l tels que $1 \leq i \leq s$ et $1 \leq j,\ l \leq k_i$. De plus la progression A est une union finie de progressions arithmétiques de la forme $A' = \{amx + b',\ x \in \mathbb{Z}\}$. Etudions un de ces progressions arithmétiques A'.

Si $n \in A'$, alors n s'écrit $n = amx + b' \implies \alpha_{ij}^n = \alpha_{ij}^{b'}\alpha_{ij}^{amx}$. D'où

$$f_i(x) = Q_i(x)\alpha_{ij}^{amx},\ \forall i,\ 1 \leq i \leq s$$

où $Q_i(x) = \sum_{j=1}^{k_i} \alpha_{ij}^{b'} p_{ij}(amx + b')$. Donc $u_n = f_1(n) + ... + f_s(n) = 0$ implique que

$$Q_1(x)\alpha_{11}^{amx} + ... + Q_s(x)\alpha_{s1}^{amx} = 0, \forall x \in \mathbb{Z} \tag{3.15}$$

Puisque $\frac{\alpha_{il}}{\alpha_{i'l}}$ n'est pas une racine de l'unité pour $i \neq i'$; il s'ensuit que $\left(\frac{\alpha_{il}}{\alpha_{i'l}}\right)^{amx}$ n'est plus une racine de l'unité pour $i \neq i'$, et par conséquent les suites linéaires récurrentes $\left(x^l\alpha_{il}^{amx}\right)_{x\in\mathbb{Z}}$; $1 \leq i \leq s$ et $l \geq 0$ sont linéairement indépendantes. Il ressort que (3.15) s'annule, $\forall x \in \mathbb{Z}$ si et seulement si $Q_1 = Q_2 = ... = Q_s = 0$. ie :

$$\forall n \in A' : f_1(n) = ... = f_s(n) = 0 \tag{3.16}$$

Puisque cette relation est valable pour toute progression A', on en déduit donc que (3.16) est vraie pour tout n de A (car A est une réunion finie des A').

Soit α_{i_0} une racine du polynôme caractéristique satisfaisant les conditions du corollaire. Alors, on obtient $f_{i_0}(n) = P_{i_0}(n)\alpha_{i_0}^n$, et par suite $f_{i_0}(n)$ admet au plus n_{i_0} zéros. Par conséquent, la relation (3.16) nous permet de conclure que $\mathbb{Z}(u_n)$ ne peut contenir des progressions arithmétiques. D'après le théorème de Skolem-Mahler-Lech on déduit que $\mathbb{Z}(u_n)$ est fini.

* La contreposée de ce corollaire est le corollaire suivant. ■

Corollaire 3.1.25 *Si $(u_n)_{n\in\mathbb{N}}$ est une suite linéaire récurrente d'ordre k et $u_n = 0$, $\forall n \in \mathbb{N}$. Alors $\forall \alpha_i$, il existe α_j ; $j \neq i$ tel que $\frac{\alpha_i}{\alpha_j}$ est une racine de l'unité.*

Chapitre 4

Présence de carrés parfaits dans une suite linéaire récurrente d'ordre deux

4.1 Carrés dans les suites de Fibonacci et Lucas

Dans ce dernier chapitre, on va aborder un autre problème qui a souvent envié plusieurs passionnants de la mathématique appliquée; à savoir la recherche des carrés parfaits dans une suite linéaire récurrente.

On va premièrement s'intéresser aux suites de Fibonacci et Lucas, en montrant que les seuls carrés parfaits de Fibonacci sont $F_{-1} = F_1 = F_2 = 1$, $F_0 = 0$ et $F_{12} = 144$; cependant ceux de Lucas sont $L_1 = 1$, $L_3 = 4$ et on finit par une généralisation de notre étude au cas des suites de Lucas générales.

Rappel : La suite de Fibonacci $(F_n)_{n\in\mathbb{N}}$ est définie par $F_0 = 0$, $F_1 = 1$ et la relation de récurrence

$$\forall\, n \geq 2 : F_n = F_{n-1} + F_{n-2}$$

De même, celle de Lucas notée $(L_n)_n$ est donnée par les valeurs initiales $L_0 = 2$, $L_1 = M$ et par la relation de récurrence suivante

$$L_{n+2} = ML_{n+1} - NL_n \ ;\ \forall\, n \geq 0$$

Dans le cas où $(M, N) = (1, -1)$, on obtient une suite similaire à celle de Fibonacci définie par

$$\forall\, n \geq 0 : L_{n+2} = L_{n+1} + L_n \ , \ L_0 = 2 \ , \ L_1 = 1$$

De plus, on a vu que les termes généraux de $(F_n)_n$ et $(L_n)_n$ sont donnés par

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = (5)^{\frac{-1}{2}} (\alpha^n - \beta^n) \, ; \, L_n = \alpha^n + \beta^n \text{ respectivement}$$

où $\alpha = \frac{1+\sqrt{5}}{2}$, $\beta = \frac{1-\sqrt{5}}{2}$ sont les racines du polynôme caractéristique $x^2 - x - 1$.

Avant de donner les résultats fondamentaux de notre étude, on va montrer quelques propriétés intéressantes des suites de Lucas et Fibonacci qui s'avèrent importantes dans toute l'étude qui reste.

Propriétés :

1) $F_{-n} = (-1)^{n+1} F_n$ et $L_{-n} = (-1)^{n+1} L_n$.

2) Si $m/n \implies F_m/F_n$.

3) $2F_{m+n} = F_m L_n + F_n L_m$.

4) $2L_{m+n} = 5F_m F_n + L_m L_n$.

5) $L_{2m} = L_m^2 + (-1)^{m+1} 2$.

6) Si $3/n$, alors : $(F_n, L_n) = 2$.

7) Si $3 \nmid n$, alors : $(F_n, L_n) = 1$.

Preuve. 1) On a

$$\begin{aligned} F_{-n} &= 5^{\frac{-1}{2}} \left(\alpha^{-n} - \beta^{-n}\right) = 5^{\frac{-1}{2}} \left(\frac{\beta^n - \alpha^n}{(\alpha\beta)^n}\right) = \\ &= 5^{\frac{-1}{2}} (-1)(-1)^n (\alpha^n - \beta^n) = (-1)^{n+1} F_n \text{ (puisque } \alpha\beta = -1) \end{aligned}$$

D'une façon analogue, on peut montrer que $L_{-n} = (-1)^{n+1} L_n$.

2) Soit m/n et posons $n = km$; alors

$$\begin{aligned} F_n &= 5^{\frac{-1}{2}} \left(\alpha^{km} - \beta^{km}\right) \\ &= 5^{\frac{-1}{2}} (\alpha^m - \beta^m) \underbrace{\left((\alpha^m)^{k-1} + \beta^m (\alpha^m)^{k-2} + \ldots + (\beta^m)^{k-1}\right)}_{\lambda} \\ &= \lambda F_m \end{aligned}$$

Ce qui signifie que F_m/F_n.

3)

$$\begin{aligned} F_mL_n + F_nL_m &= 5^{\frac{-1}{2}}(\alpha^m - \beta^m)(\alpha^n + \beta^n) + 5^{\frac{-1}{2}}(\alpha^n - \beta^n)(\alpha^m + \beta^m) \\ &= 5^{\frac{-1}{2}}\left[\alpha^{n+m} + \alpha^m\beta^n - \alpha^m\beta^n + \alpha^{n+m} + \alpha^n\beta^m - \alpha^n\beta^m - \beta^{n+m}\right] - \beta^{n+m} \\ &= 2.5^{\frac{-1}{2}}\left(\alpha^{n+m} - \beta^{n+m}\right) = 2F_{n+m} \end{aligned}$$

4)

$$\begin{aligned} 5F_mF_n + L_mL_n &= 5.5^{-1}(\alpha^m - \beta^m)(\alpha^n - \beta^n) + (\alpha^m + \beta^m)(\alpha^n + \beta^n) \\ &= 2\left(\alpha^{n+m} + \beta^{n+m}\right) = 2L_{m+n} \end{aligned}$$

5) On a

$$\begin{aligned} L_m^2 + (-1)^{m+1}2 &= (\alpha^m + \beta^m)^2 + (-1)^{m+1}2 \\ &= \alpha^{2m} + \beta^{2m} + 2(\alpha\beta)^m + (-1)^{m+1}2 \\ &= \alpha^{2m} + \beta^{2m} + 2(-1)^m + 2(-1)^{m+1} = \alpha^{2m} + \beta^{2m} \\ &= L_{2m} \end{aligned}$$

6) Un calcul simple donne $L_n^2 - 5F_n^2 = 4(-1)^n$, ce qui signifie que $(F_n, L_n) = 1$ ou 2. Supposons que n est un multiple de 3. (C'est-à-dire : $n = 3k$), on obtient alors

$$\begin{aligned} F_{3k} &= 5^{\frac{-1}{2}}(\alpha^{3k} - \beta^{3k}) \\ &= 5^{\frac{-1}{2}}(\alpha^3 - \beta^3)\underbrace{\left((\alpha^3)^{k-1} + \beta^3(\alpha^3)^{k-2} + \ldots(\beta^3)^{k-1}\right)}_{\lambda} \end{aligned}$$

Or $\alpha^3 = 2 + \sqrt{5}$; $\beta^3 = 2 - \sqrt{5} \implies \alpha^3 - \beta^3 = 2\sqrt{5}$. D'où

$$F_{3k} = 2.\lambda \text{ (ie : } F_{3k} \text{ est divisible par 2)} \qquad (*)$$

D'autre part, on a

$$\begin{aligned} L_{3k} &= (\alpha^{3k} + \beta^{3k}) \\ &= (\alpha^3 + \beta^3)\underbrace{\left((\alpha^3)^{k-1} - \beta^3(\alpha^3)^{k-2} + \ldots - \ldots + (\beta^3)^{k-1}\right)}_{\nu} = 4\nu \qquad (**) \end{aligned}$$

De $*$ et $**$, on conclut que

$$(F_{3k}, L_{3k}) = 2$$

7) Maintenant soit $3 \nmid n$. ie : $n = 3k + 1$ ou $n = 3k + 2$. Puisque $(F_n, L_n) = 1$ ou 2, on en déduit que

$$3 \nmid n \implies (F_n, L_n) = 1 \qquad \text{(c.q.f.d)}$$

Dans l'étude qui reste on a besoin des lemmes suivants. ■

Lemme 4.1.1 *Pour tout k de $\mathbb{N}$, on a*

$$L_{6k} \equiv 2 \pmod 4$$

Preuve. On peut procéder par récurrence.
Pour $k = 1$, on a $L_6 = 18 \equiv 2 \pmod 4$. Supposons que $L_{6k} \equiv 2 \pmod 4$ et montrons que

$$L_{6(k+1)} = L_{6k+6} \equiv 2 \pmod 4$$

D'après (4) ; on a

$$2L_{6k+6} = 5F_{6k}F_6 + L_{6k}L_6 = 40F_{6k} + 18L_{6k}$$

Et par conséquent, on obtient

$$L_{6(k+1)} = 20F_{6k} + 9L_{6k} \equiv 2 \pmod 4$$

On conclut donc par récurrence que $L_{6k} \equiv 2 \pmod 4$ pour tout k de $\mathbb{N}$. ■

Lemme 4.1.2 *Si $k = 2^r$ avec $r \geq 1$, alors*

$$L_k \equiv 3 \pmod 4$$

Preuve. Ce résultat se démontre par récurrence.
En effet. Pour $k = 2$, on a $L_2 = 3 \equiv 3 \pmod 4$. Supposons que $L_{2^i} \equiv 3 \pmod 4$ pour tout $1 \leq i \leq r$. D'après (5), on aura $L_{2^{r+1}} = L_{2.2^r} = L_{2^r}^2 - 2 \equiv 3^2 - 2 \equiv 3 \pmod 4$. On en déduit que

$$L_k \equiv 3 \pmod 4, \forall k = 2^r ; r \geq 1$$

■

Lemme 4.1.3 *Si $k = 2^r$, alors*

$$\begin{cases} i) \left(\frac{-1}{L_k}\right) = -1 \ , \ si\ r \geq 1 \\ ii) \left(\frac{2}{L_k}\right) = +1 \ , \ si\ r \geq 2 \end{cases}$$

Preuve. $i)$ Par le lemme (4.1.2), on a $L_k \equiv 3 \pmod 4$. D'après le critère d'Euler, on aura

$$\left(\frac{-1}{L_k}\right) \equiv (-1)^{\frac{L_k-1}{2}} \equiv -1 \pmod{L_k}$$

Qui signifie que -1 n'est pas un carré modulo L_k.

ii) Soit $k = 2^r$ avec $r \geq 2$. Alors $\frac{1}{2}k$ est pair et d'après la relation (5) on aura

$$\begin{aligned} L_{\frac{1}{2}k}^2 &= L_k + 2 \equiv 2 \pmod{L_k} \\ &\Longrightarrow 2 \equiv L_{\frac{1}{2}k}^2 \pmod{L_k} \Longrightarrow 2 \text{ est un carré modulo } L_k \\ &\Longrightarrow \left(\frac{2}{L_k}\right) = +1 \end{aligned}$$

■

Lemme 4.1.4 *Si $k = 2^r$ et $r \geq 2$; alors $3 \nmid L_k$.*

Preuve. Puisque $k = 2^r$ et $r \geq 2$, on conclut que $4/k$ et par conséquent $F_4 = 3/F_k$ (d'après (2)). Et par la propriété (7) on a $(F_k, L_k) = 1$, on en déduit donc que

$$3 \nmid L_k \qquad \text{(c.q.f.d)}$$

■

Lemme 4.1.5 *Si $k = 2^r$ et $r \geq 1$, alors pour tout m de $\mathbb{N}$, on a*

$$\begin{cases} i)\ F_{m+2k} \equiv -F_m \pmod{L_k} \\ ii)\ L_{m+2k} \equiv -L_m \pmod{L_k} \end{cases}$$

Preuve. *i*) D'après (3), on a

$$\begin{aligned} 2F_{m+2k} &= F_m L_{2k} + F_{2k} L_m = F_m \left(L_k^2 - 2\right) + F_k L_k L_m \\ &\Longrightarrow 2F_{m+2k} \equiv -2F_m \pmod{L_k} \\ &\Longrightarrow F_{m+2k} \equiv -F_m \pmod{L_k} \text{ (puisque : } (L_k, 2) = 1) \end{aligned}$$

ii) D'une façon analogue et par (4), on a

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

■

Théorème 4.1.6 *F_n est un carré parfait seulement pour $n \equiv 0, 1, 2, 6$ ou $11 \pmod{12}$.*

Preuve. Puisque $F_{12} = 144$ et $L_{12} = 322$, alors par (3), on obtient

$$\begin{aligned} F_{n+12} &= 72L_n + 161F_n \\ &\Longrightarrow F_{n+12} - F_n = 72L_n + 160F_n \equiv 0 \pmod 8 \\ &\Longrightarrow F_{n+12} \equiv F_n \pmod 8 \end{aligned}$$

On peut donc considérer 12 comme extrême de la congruence. En examinant les 12 premiers nombres de Fibonacci, on obtient

$$\begin{cases} F_n \equiv 2 \pmod 8, \text{ si } n \equiv 3 \text{ ou } 9 \pmod{12} \\ F_n \equiv 3 \pmod 8, \text{ si } n \equiv 4 \pmod{12} \\ F_n \equiv 5 \pmod 8, \text{ si } n \equiv 5, 7 \text{ ou } 8 \pmod{12} \\ F_n \equiv 7 \pmod 8, \text{ si } n \equiv 10 \pmod{12} \end{cases}$$

Et on voit immédiatement que tous ces cas sont rejetés. ■

Théorème 4.1.7 *F_n n'est pas un carré si $n \equiv 6 \pmod{12}$.*

Preuve. Si $n = 12p + 6$, alors par (3) on aura

$$2F_{12p+6} = F_{12p}L_6 + F_6L_{12p} = 18F_{12p} + 8L_{12p}$$

D'autre part, on a $F_{12} = 144/F_{12p} \Longrightarrow F_{12p+6} = 9F_{12p} + 4L_{12p}$ qui par le lemme (4.1.1) donne

$$F_n = F_{12p+6} \equiv 8 \pmod{16}$$

On en déduit que dans ce cas F_n n'est pas un carré. ■

Théorème 4.1.8 *F_n n'est pas un carré si $n = 12p + q$ avec $p > 0$ et $q \in \{-1, 1, 2\}$.*

Preuve. En effet. Si $p > 0$, On pose $p = 2^{r-1}\alpha$ où $r > 1$ et α est impair. Alors $n = 12p + q = 6k\alpha + q$ où $k = 2^r$, $r \geq 2$. Par le lemme (4.1.5), on obtient

$$F_{6k\alpha+q} \equiv (-1)^{3\alpha} F_q \pmod{L_k} \equiv -F_q \pmod{L_k}$$

Et par le lemme (4.1.3), on en déduit que $\left(\frac{F_n}{L_k}\right) = \left(\frac{-1}{L_k}\right) = -1$. Autrement dit F_n n'est pas un carré parfait. ■

Remarque 4.1.9 *Le théorème précédent signifie que, si $n \equiv 1$, 2 ou 11 (mod 12) ; alors n n'est pas un carré parfait.*

Conclusion 4.1.10 *D'après l'étude précédente, on conclut que les seuls carrés parfait dans la suite de Fibonacci sont* $F_{-1} = F_1 = F_2 = 1$, $F_0 = 0$ *et* $F_{12} = 144$.

Théorème 4.1.11 *Si* $L_n = x^2$, *alors* $n = 1$ *ou* $n = 3$.

Preuve. Si n est pair, on peut écrire $n = 2m$. Et d'après (5), on obtient

$$L_n = L_{2m} = L_m^2 + 2(-1)^{m+1}$$

ie., $L_n = y^2 \pm 2 \neq x^2$, et donc, on en déduit que dans ce cas L_n n'est pas un carré parfait.
Si n est impair, on distingue deux cas.
i) $n \equiv 1 \pmod 4$. Dans ce cas, on voit que $L_1 = 1$ est un carré parfait, mais pour $n \neq 1$, on écrit $n = 1 + 2.3^r.k$ où k est pair non divisible par 3 et $r \in \mathbb{N}$. Donc, par le lemme (4.1.5), on obtient

$$L_n = L_{1+2.3^r.k} \equiv -L_1 \equiv -1 \pmod{L_k}$$

D'autre part, puisque k est pair et d'après le lemme (4.1.2), on a $L_k \equiv 3 \pmod 4$, ce qui signifie que (-1) n'est pas un carré modulo L_k. Et par suite L_n n'est pas un carré parfait.
ii) $n \equiv 3 \pmod 4$, alors pour $n = 3$; on obtient $L_3 = 4 = 2^2$ (ie., L_3 est un carré). Et pour $n \neq 3$, on écrit comme précédemment $n = 1 + 2.3^r.k$; ce qui donne

$$L_n \equiv -L_3 \equiv -4 \pmod{L_k} \Longrightarrow L_n \neq x^2 \qquad \text{(c.q.f.d)}$$

■

4.2 Les carrés dans les suites de Lucas générales

Dans le reste, on va étendre l'étude précédente au cas général des suites entières $(x_n)_{n\in\mathbb{N}}$ d'ordre deux définies seulement par une relation de récurrence de la forme

$$x_{n+2} = Px_{n+1} - Qx_n \ , \ \forall n \geq 0$$

Dans le cas général, la détermination des carrés de telles suites est très délicate. Pour cela, on va restreindre notre étude au cas où P et Q sont impairs avec $(P, Q) = 1$ et le déscriminant $P^2 - 4Q > 0$. Rappelons d'abord que les suites de Lucas du premier et du deuxième type notées respectivement U_n et V_n sont définies par

$$\begin{cases} U_0 = 0 \ , \ U_1 = 1 \text{ et } U_{n+2} = P\ U_{n+1} - Q\ U_n \\ V_0 = 2 \ , \ V_1 = P \text{ et } V_{n+2} = P\ V_{n+1} - Q\ V_n \end{cases}$$

Les résultats de ce dernier paragraphe repose sur les théorèmes suivants.

Théorème 4.2.1 *Soit $(x_n)_{n\geq 0}$ une suite d'entiers positifs définie par*

$$x_{n+2} = Px_{n+1} - Qx_n, \ \forall\, n \in \mathbb{N}$$

Et soit p un diviseur premier impair de V_k. On a

a) Si k est pair, alors

$$\left(\frac{x_{n+2k}}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{x_n}{p}\right)$$

de telle sorte que $\left(\frac{-1}{p}\right) = 1$ si $p \equiv 1 \pmod 4$ et $\left(\frac{-1}{p}\right) = -1$ si $p \equiv -1 \pmod 4$.

3) Si k est impair, on obtient

$$\left(\frac{x_{n+2k}}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{Q}{p}\right)\left(\frac{x_n}{p}\right)$$

Preuve. Soient $\alpha = \frac{P+\sqrt{D}}{2}$ et $\beta = \frac{P-\sqrt{D}}{2}$ (avec $D = P^2 - 4Q$) les racines du polynôme caractéristique $x^2 - Px + Q$ où $D = P^2 - 4Q > 0$. Rappelons d'abord les formules de solutions de $(U_n)_{n\geq 0}$ et $(V_n)_{n\geq 0}$.

$$\begin{cases} U_n = \frac{\alpha^n - \beta^n}{\sqrt{D}} = \frac{\alpha^n - \beta^n}{\alpha - \beta} \\ V_n = \alpha^n + \beta^n \end{cases}$$

On en déduit donc que

$$V_n + U_n\sqrt{D} = 2\alpha^n, \ U_{-n} = \frac{-1}{Q^n}\, U_n \text{ et } V_{-n} = \frac{1}{Q^n}\, V_n$$

Soient y_0 et y_1 deux entiers tels que, $y_1 + x_1\sqrt{D} = \alpha\left(y_0 + x_0\sqrt{D}\right)$, par conséquent ; on aura

$$y_0 = 2x_1 - Px_0; \ y_1 = Px_1 - 2Qx_0$$

Posons $y_n + x'_n\sqrt{D} = \alpha^n\left(y_0 + x_0\sqrt{D}\right)$ et montrons que les suites $(x_n)_n$ et $(x'_n)_n$ sont égales. On a

$$\begin{aligned} y_{n+k} + x'_{n+k}\sqrt{D} &= \alpha^k\alpha^n\left(y_0 + x_0\sqrt{D}\right) = \alpha^k(y_n + x'_n\sqrt{D}) \\ &= \frac{1}{2}\left(V_k + U_k\sqrt{D}\right)(y_n + x'_n\sqrt{D}) \end{aligned}$$

D'où

$$2x'_{n+k} = V_k x'_n + U_k y_n \qquad (*)$$

De même si $n - k \geq 0$, on aura

$$\begin{aligned} y_{n-k} + x'_{n-k}\sqrt{D} &= \alpha^{-k}(y_n + x'_n\sqrt{D}) \\ &= \frac{1}{2}Q^{-k}\left(V_k - U_k\sqrt{D}\right)(y_n + x'_n\sqrt{D}) \end{aligned}$$

$$\Rightarrow 2Q^k x'_{n-k} = V_k x'_n - U_k y_n \qquad (**)$$

Par addition de $*$ et $**$, on obtient $x'_{n+k} + Q^k x'_{n-k} = V_k x'_n$. Pour $k = 1$, cette relation donne

$$x'_{n+1} = Px'_n - Qx'_{n-1}$$

C'est-à-dire : $(x'_n)_{n\geq 0}$ et $(x_n)_{n\geq 0}$ vérifient la même relation de récurrence et puisque $x'_0 = x_0$ et $x'_1 = x_1$, on en déduit que $x_n = x'_n$ pour tout n. D'où $x_{n+k} + Q^k x_{n-k} = V_k x_n$; ce qui donne aussi

$$x_{n+2k} + Q^k x_n = V_k x_{n+k}$$

De cette dernière relation, on conclut que : si p est un diviseur premier impair de V_k ; alors

i Si k est pair, on aura

$$\begin{aligned}\left(\frac{x_{n+2k}}{p}\right) &= \left(\frac{-Q^k x_n}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{Q^k}{p}\right)\left(\frac{x_n}{p}\right) \\ &= \left(\frac{-1}{p}\right)\left(\frac{x_n}{p}\right) \text{ (puisque } k \text{ pair et } Q \text{ impair)} \Rightarrow \left(\frac{Q^k}{p}\right) = 1)\end{aligned}$$

ii) Si k est impair, on obtient

$$\begin{aligned}\left(\frac{x_{n+2k}}{p}\right) &= \left(\frac{-Q^k x_n}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{Q^k}{p}\right)\left(\frac{x_n}{p}\right) \\ &= \left(\frac{-1}{p}\right)\left(\frac{QQ^{k-1}}{p}\right)\left(\frac{x_n}{p}\right)\end{aligned}$$

Puisque k est impair et $k-1$ est pair ; on déduit que $\left(\frac{Q^{k-1}}{p}\right) = 1$. D'où

$$\left(\frac{x_{n+2k}}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{Q}{p}\right)\left(\frac{x_n}{p}\right)$$

■

Théorème 4.2.2 *Soient P et Q deux entiers impairs avec $(P, Q) = 1$. Alors $V_{3.2^j}$ admet un diviseur premier $p \equiv -1 \pmod 4$ et au moins deux pour $j \geq 2$.*

Preuve. Montrons d'abord les formules

$$\begin{cases} i)\ V_{2n} = (V_n^2 - 2Q^n) \\ ii)\ V_{3n} = V_n\,(V_n^2 - 3Q^n) \end{cases}$$

En effet, on a

i)

$$\begin{aligned}V_n^2 - 2Q^n &= (\alpha^n + \beta^n)^2 - 2Q^n = \alpha^{2n} + \beta^{2n} + 2\,(\alpha\beta)^n - 2Q^n \\ &= \alpha^{2n} + \beta^{2n} + 2Q^n - 2Q^n = \alpha^{2n} + \beta^{2n} = V_{2n}\end{aligned}$$

ii)

$$\begin{aligned} V_n\left(V_n^2 - 3Q^n\right) &= \left(\alpha^n + \beta^n\right)\left(\alpha^{2n} + \beta^{2n} - Q^n\right) \\ &= \alpha^{3n} + \beta^{3n} + (\alpha\beta)^n\left(\alpha^n + \beta^n\right) - (\alpha\beta)^n\left(\alpha^n + \beta^n\right) \\ &= \alpha^{3n} + \beta^{3n} = V_{3n} \end{aligned}$$

* *En outre, on peut montrer par récurrence que :* $\forall j \geq 0$ *;* V_{2^j} *est impair.*

En effet. Pour $j = 0$*, on a* $V_{2^0} = V_1 = P$ *qui est impair.*

Supposons que V_{2^i} *est impair,* $\forall i \leq j$ *et montrons que* $V_{2^{j+1}}$ *est impair. On a*

$$V_{2^{j+1}} = V_{2.2^j} = V_{2^j}^2 - 2Q^{2^j}$$

Or $V_{2^j}^2$ *est impair et* $2Q^{2^j}$ *est pair, ce qui implique que* $V_{2^{j+1}}$ *est impair. On en déduit que*

$$\forall\ j \geq 0,\ V_{2^j} \text{ est impair} \qquad \text{(c.q.f.d)}$$

* *De plus, on a*

$$\forall\ j \geq 1,\ V_{2^j} = V_{2.2^{j'}} = V_{2^{j'}}^2 - 2Q^{2^{j'}} \equiv 1 - 2 \equiv -1 \pmod 4 \ (j = j' + 1$$

Puisque $j' \geq 0$ *et* $V_{2^{j'}}$ *est impair. On conclut donc que* V_{2^j} *admet un diviseur premier* $p \equiv -1 \pmod 4$*. L'autre facteur* $V_{2^j}^2 - 3Q^{2^j}$ *de* $V_{3.2^j}$ *est congru à* $1 - 3 \equiv -2 \pmod 8$ *; et donc il peut s'écrire*

$$V_{2^j}^2 - 3Q^{2^j} = 2s \text{ avec } s \equiv -1 \pmod 4$$

Alors comme précédemment il admet un diviseur premier $p' \equiv -1 \pmod 4$*. De plus, on a* $p \neq p'$*, car si* $p = p'$ *; alors* p *divise* V_{2^j} *et* $V_{2^j}^2 - 3Q^{2^j}$*. ie., p divise* V_{2^j} *et* $3Q^{2^j}$ *et comme P est premier à Q et* $V_{n+1} \equiv PV_n \pmod Q$*, alors Q est premier à tous les* V_n *et donc à p aussi. ie.,*

$$p/3Q^{2^j} \text{ et } \left(p, Q^{2^j}\right) = 1 \underset{Gauss}{\Longrightarrow} p = p' = 3 \text{ et } (3, Q) = 1$$

Mais pour n pair, on a $V_{2n} = V_n^2 - 2Q^n$ *et par conséquent* V_{2n} *est premier à 3, ce qui contredit* $p = 3/V_{2^n}$ *lorsque* $2n = 2^j$ *avec* $j \geq 2$*. c.q.f.d* ∎

Remarque 4.2.3 *Le cas* $j = 1$ *peut se produire. Pour* $(P, Q) = (7, 5)$ *; on aura* $V_6 = 2.3^2.13.41$ *et 3 est le seul diviseur premier* $\equiv -1 \pmod 4$ *de* V_6*.*

Théorème 4.2.4 *Soient P et Q deux entiers impairs. Si un* x_a *est un carré et pour tout j,* x_a *est premier à un diviseur premier* $p_j \equiv -1 \pmod 4$ *de* $V_{3.2^j}$*. Alors aucun* x_{a+12p_i}*,* $p \neq 0$ *n'est un carré.*

Preuve. Posons $p = 2^{j-1}p'$ avec p' impair ; $j \geq 1$. On a, d'une part

$$\left(V_{3.2^j} + U_{3.2^j}\sqrt{D}\right)^{p'} = 2^{p'}\left(\alpha^{3.2^j}\right)^{p'} = 2\alpha^{6p} = \left(V_{6p} + U_{6p}\sqrt{D}\right) \qquad (*)$$

D'autre part

$$\left(V_{3.2^j} + U_{3.2^j}\sqrt{D}\right)^{p'} = \sum_{k=0}^{p'} C_{p'}^k V_{3.2^j}^k \left(U_{3.2^j}\sqrt{D}\right)^{p'-k}$$

On sait que. *i*) Si k est pair, alors $p' - k$ est impair et donc $\left(U_{3.2^j}\sqrt{D}\right)^{p'-k} = \lambda\sqrt{D}$, $\lambda \in \mathbb{Z}$. *ii*) Si k est impair (c'est-à-dire $p' - k$ est pair), il s'ensuit que

$$\left(V_{3.2^j} + U_{3.2^j}\sqrt{D}\right)^{p'} = C_{p'}^0\lambda_1\sqrt{D} + C_{p'}^1 V_{3.2^j}^1\delta_1 + C_{p'}^2 V_{3.2^j}^2\lambda_2\sqrt{D} + C_{p'}^3 V_{3.2^j}^3\delta_2 + \ldots$$

En identifiant avec $*$, on conclut que

$$V_{6p} = V_{3.2^j}\left(p'\delta_1 + C_{p'}^3 V_{3.2^j}^3\delta_2 + \ldots + \ldots\right)$$

Ce qui signifie que $V_{3.2^j}/V_{6p}$, et donc tout diviseur premier $p_j \equiv -1 \pmod 4$ de $V_{3.2^j}$ est aussi un diviseur premier de V_{6p}. En appliquant la partie (α) du théorème (4.2.1) avec $n = a$ et $s = 6p$, on déduit que

$$\left(\frac{x_{a+12p}}{p_j}\right) = \left(\frac{-1}{p_j}\right)\left(\frac{x_a}{p_j}\right)$$

Et puisque x_a est un carré, alors $\left(\frac{x_a}{p_j}\right) = 1$. De plus $p_j \equiv -1 (\mathrm{mod}\, 4) \implies \left(\frac{-1}{p_j}\right) = -1$. D'où

$$\left(\frac{x_{a+12p}}{p_j}\right) = -1$$

Autrement dit x_{a+12p} n'est pas un carré modulo p_j et ne peut être donc un carré. ∎

Remarque 4.2.5 *i) Soit r le radical de x_a. ie., $r = \sqrt{x_a}$. Si $r = 2$, il est évidemment premier à tous les p_j de l'énoncé. De plus, si r est premier et s'il y a plusieurs diviseurs premiers $p_j \equiv -1 \pmod 4$ de $V_{3.2^j}$ (vrai pour $j \geq 2$ par le théorème (4.2.2)); alors r est premier à chacun d'eux et la condition du théorème (4.2.4) est satisfaite.*
ii) Pour r premier, on voit que le seul mauvais cas est $r = 3$, $j = 1$ et 3 est le seul diviseur premier $\equiv -1 \pmod 4$ de V_6. Dans ce cas, si x_a est un carré; alors x_{a+12n} peut lui même être un carré.

Exemple 4.2.6 *Définissons $(x_n)_n$ par*

$$\begin{cases} x_0 = 81,\ x_1 = 146735 \\ x_{n+2} = 7x_{n+1} - 11x_n\ ,\forall\ n \geq 0 \end{cases}$$

On a $V_6 = 2.3^6.61$ et on voit que $x_0 = 81$ (un carré), et par suite $x_{12} = 2482587^2$ est aussi un carré.

Remarque 4.2.7 *Supposons que pour tout j, il y ait un diviseur premier impair p_j de $V_{3.2^j}$ qui soit premier au carré x_a et qu'on ait, ou bien $p_j \equiv -1 \pmod 4$ et $\left(\frac{Q}{p_j}\right) = 1$ ou bien $p_j \equiv 1 \pmod 4$ et $\left(\frac{Q}{p_j}\right) = -1$. Alors par le théorème (4.2.1) (partie (β)) aucun x_{a+6p}, $p \neq 0$ n'est un carré.*

Corollaire 4.2.8 *Une suite de Lucas généralisée $(x_n)_n$, définie seulement par la relation de récurrence*

$$x_{n+2} = Px_{n+1} - Qx_n, \forall\ n \geq 0$$

ne contient qu'un nombre fini de carrés. Il en est de même pour les multiples de carrés (doubles, triples de carrés...)

Preuve. En effet. Par le théorème (4.2.4), il en est ainsi pour chaque classe d'indices modulo 12. Pour les multiples de carrés, supposons par exemple que $x_n = 3a^2$, qui donne $3x_n = 9a^2$. ie., 3 x_n est un carré et on est ainsi ramené aux carrés dans la suite $(3x_n)_{n\geq 0}$.

■

4.3 Une méthode de recherche des carrés

Soit $(x_n)_n$ la suite de Lucas généralisée définie par

$$x_{n+2} = Px_{n+1} - Qx_n\ ;\ \forall n \geq 0$$

Où P, Q sont impairs et premiers entre eux. Cherchons à trouver tous les carrés dans la suite $(x_n)_n$.

* On commence par chercher des entiers b tels que $x_{n+12} \equiv x_n \pmod b$ ou $\frac{x_{n+12}}{b} \equiv \frac{x_n}{b} \pmod b$, si b est premier.

* Soit alors I l'ensemble des indices a ; $0 \leq a \leq 12$ tels que x_a soit un carré modulo tous ces entiers b.

−Ainsi, si x_n est un carré ; il existe alors $a \in I$ tel que $n \equiv a \pmod{12}$.

−Cela fait et si x_a est un carré, alors si la condition du théorème (4.2.4) est satisfaite, on en déduit que la sous-suite (x_{a+12n}) ne contient aucun carré. Sinon (ie., si la condition du théorème (4.2.4) n'est pas satisfaite, alors x_{a+12n} est un carré éventuel et on teste x_a modulo les diviseurs premiers de V_6, V_{12}, V_{24},..., $V_{3.2^j}$. On distingue quatre cas.

A) S'il existe un diviseur premier $p \equiv 1 \pmod 4$ de V_6 et si x_a est un non carré modulo p, autrement dit : $\left(\frac{x_a}{p}\right) = -1$; alors par le théorème (4.2.1), on obtient $\left(\frac{x_{a+12n}}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{x_a}{p}\right) =$

-1, qui signifie qu'aucun x_{a+12n} n'est un carré.

$-$S'il n'existe pas un diviseur premier $p \equiv 1 \pmod 4$ de V_6, alors tous les diviseurs premiers impairs p_j de V_6 sont tels que $p_j \equiv -1 \pmod 4$ et on distingue trois cas.

B) Il y a deux diviseurs premiers $p, p' \equiv -1 \pmod 4$ de V_6 tels que $\left(\frac{x_a}{p}\right)$ et $\left(\frac{x_a}{p'}\right)$ sont opposés. Alors par le théorème (4.2.1) ; on déduit que $\left(\frac{x_{a+12n}}{p}\right)$ et $\left(\frac{x_{a+12n}}{p'}\right)$ sont opposés et aucun x_{a+12n} n'est un carré.

C) x_a est un carré modulo tous les diviseurs premiers $p \equiv -1 \pmod 4$ de V_6. Alors, on teste x_a encore une fois modulo les diviseurs premiers de V_{12} et on répète le même processus qu'avec V_6.

D) x_a est un non carré modulo tous les diviseurs premiers $p \equiv -1 \pmod 4$ de V_6. Dans ce cas, on teste x_{a+12} ou x_{a-12} modulo les diviseurs premiers de V_{12}.

Et ainsi de suite. On effectue des tests modulo les diviseurs premiers de V_6, V_{12}, V_{24},... jusqu'à ce qu'on se trouve dans une bonne situation (A ou B) ou jusqu'à ce qu'un carré soit découvert.

$*$ Cette méthode est forte éfficace et la plupart des suites étudiées n'ont pu résister au test V_6.

Exemple **4.3.1** *Soit la suite* $(x_n)_{n\geq 0}$ *définie par* $x_{n+2} = 5x_{n+1} - 3x_n$. *On a* $V_6 = 2.19.167$ *et* $V_{12} = 2.7^3.47.1249$.

i) Si $x_0 = 1$ *et* $x_1 = 5$ *; alors les congruences modulo* 3, 5 *et* 8 *impliquent que* $a \equiv 0$ *ou* 4 (mod 12).

$-$*Pour* $a \equiv 0 \pmod{12}$, *on a* $x_0 = 1$ *qui est premier à tous les diviseurs premiers* p_j *de* $V_{3.2^i}$ *vérifiant* $p_j \equiv -1 \pmod 4$. *Donc d'après le théorème* (4.2.4) *aucun* $x_{0+12n} = x_{12n}$ *n'est un carré.*

$-$*Pour* $a \equiv 4 \pmod{12}$, *on a* $x_4 = 409$ *et par conséquent* $\left(\frac{409}{19}\right) = -1$ *;* $\left(\frac{409}{167}\right) = 1$, *ce qui correspond au cas* (B). *Autrement dit aucun* x_{4+12n} *n'est un carré.*

Conclusion **4.3.2** x_0 *est le seul carré dans la suite* $(x_n)_{n\geq 0}$.

Maintenant si les termes initiaux sont tels que $x_0 = 1$, $x_1 = 13$ *; les congruences demandent alors*

$$a \equiv 0, 7, 11 \pmod{12}$$

$-$*Comme précédemment le cas* $a \equiv 0 \pmod{12}$ *est réglé par le théorème* (4.2.4). *Mais pour* $a \equiv 7 \pmod{12}$, *on a* $x_7 = 93169$ *et par suite* $\left(\frac{93169}{19}\right) = -1; \left(\frac{93169}{167}\right) = 1$ *qui correspond au cas* (B). *C'est-à-dire : aucun* x_{7+12n} *n'est un carré.*

Pour $a \equiv 11 \pmod{12}$, *on a* $x_{11} = 3723516$ *qui est un carré modulo* 19 *et* 167. *Donc on le passe au test* V_{12}. *On voit que* x_{11} *est un non carré modulo* 1249 *où* $1249 \equiv 1 \pmod 4$, *ce qui correspond au cas* (A). *Alors aucun* x_{11+12n} *n'est un carré.*

Conclusion 4.3.3 $x_0 = 1$ *est le seul carré dans la suite* $(x_n)_{n\geq 0}$.

Exemple 4.3.4 *Soit la suite* $(x_n)_{n\geq 0}$ *telle que* $x_{n+2} = 7x_{n+1} - 3x_n$; $\forall\, n \in \mathbb{N}$. *On a* :
$D = 7^2 - 4.3 = 37$; $V_6 = 2.43.911$ *et* $V_{12} = 2.431.1831.3889$.

* *Si* $x_0 = 1$, $x_1 = 4$; *alors les congruences modulo* 3, 5, 7, 8 *impliquent que les valeurs de a sont telles que* $a \equiv 0, 1, 2, 8, 11 \pmod{12}$.

$-$*Pour* $a \equiv 0 \pmod{12}$, *on a* $x_0 = 1$ *qui satisfait la condition du théorème* (4.2.4). *Et par conséquent aucun* $x_{0+12n} = x_{12n}$ *n'est un carré.*

$-$*Pour* $a \equiv 1 \pmod{12}$ *et puisque* $x_1 = 4$ *est premier à* 43 *et* 911 ; *le théorème* (4.2.4) *indique qu'aucun* x_{1+12n} *n'est un carré.*

$-$*Le cas* $a \equiv 2 \pmod{12}$ *est également réglé par le théorème* (4.2.4) (*car* $x_2 = 25 = 5^2$ *et* 5 *est premier à tous les* V_n.

$-$*Pour* $a \equiv 8 \pmod{12}$; *on a* $\left(\frac{x_8}{43}\right) = \left(\frac{x_8}{911}\right) = 1$, *ce qui correspond au cas* (C), *mais* $\left(\frac{x_8}{3889}\right) = -1$. *C'est-à-dire :* x_8 *est un non carré modulo* 3889 *qui correspond au cas* (A). *Alors aucun* x_{8+12n} *n'est un carré.*

$-$*Enfin, au lieu de calculer* x_{11}, *on calcule* x_{-1} *et on trouve* $x_{-1} = 1$, *qui est un carré qui satisfait la condition du théorème* (4.2.4). *Alors, aucun* $x_{-1+12n} = x_{11+12n}$ *n'est un carré, et par conséquent la suite contient juste* 4 *carrés qui sont* 1, 1, 4 *et* 25.

* *Maintenant si la suite commence par* $x_0 = 1$, $x_1 = 3$; *les congruences demandent* $a \equiv 0, 4, 6, 10 \pmod{12}$.

$-$*Pour* $a \equiv 0 \pmod{12}$, *on applique le théorème* (4.2.4) *comme précedemment et on déduit que* $x_{0+12n} = x_{12n}$ *n'est plus un carré.*

$-$*Si* $a \equiv 6 \pmod{12}$, *on a* $x_6 = 9.3637$ *qui est un carré modulo* 43 *et* 911 ; *mais un non carré modulo* 3889 ; *ce qui correspond au cas* (A). *D'où aucun* x_{6+12n} *n'est un carré.*

$-$ *Pour* $n \equiv 4 \pmod{12}$ *et* $n \equiv 10 \pmod{12}$, *on voit que* x_4 *et* x_{10} *sont des non carrés modulo* 43 *et* 911 *(cas* (D)*). On doit donc passer* x_{16} *et* x_{22} *(ou* x_{-8} *et* x_{-2}*) au test* V_{12}. *On voit que* $\left(\frac{x_{-8}}{3889}\right) = -1$; $\left(\frac{x_{-2}}{3889}\right) = -1$ *avec* $3889 \equiv 1 \pmod 4$ *qui correspond au cas* (A). *On conclut enfin que* $x_0 = 1$ *est le seul carré dans la suite* $(x_n)_{n\geq 0}$.

Conclusion générale

Les suites linéaires récurrentes constituent une partie fondamentale en théorie des nombres. L'un des passionnant sujets évoquant celles-ci est le problème de multiplicité. Dans ce mémoire, on a abordé une étude approfondie de deux principaux problèmes relatifs aux suites linéaires récurrentes. Le premier concerne la multiplicité d'une suite linéaire récurrente d'ordre deux, à termes entiers et le deuxième consiste à rechercher les carrés parfaits dans de telles suites.Généralement les résultats obtenus sont :

1) **Pour la multiplicité d'une suite linéaire récurrente :**

Soit$(a_n)_{n\geq 0} \subset \mathbb{Q}$ une suite linéaire récurrente définie par la relation de récurrence

$$a_{n+2} = Ma_{n+1} - Na_n, \forall n \geq 0 \text{ où } M, N \in \mathbb{Z}$$

Pour $\omega \in \mathbb{Q}$. Désignons par s le plus petit dénominateur commun à a_0 et a_1. Alors on voit que $(sa_n)_{n\geq 0} \subset \mathbb{Z}$ et donc la ω-multiplicité de $(a_n)_{n\geq 0}$ est équivalente à la $s\omega$-multiplicité de $sa_n)_{n\geq 0}$. Par suite on peut restreindre notre étude au suites entières.

Notons aussi que $p.g.c.d\,(a_0, a_1)\,/a_n$ pour tout $n \geq 0$ et on peut donc supposer que $(a_0, a_1) = 1$ et $a_0 \geq 0$. D'autre part, sans perdre de généralité, on peut supposer que $a_0 = \omega$ et il suffit donc de borner le cardinal de l'ensemble $\{n \geq 0 : a_n = a_0\}$.

De plus, on sait généralement que la multiplicité de $(a_n)_{n\geq 0}$ est au plus 5 et dans le cas particulier si $(M, N) = 1$; alors la multiplicité est au plus égale à 4.

***En s'appuyant sur des arguments p-adiques, on retrouve les résultats suivants :**

−Si $(a_0, a_1) = 1$, $M = 1$ et $N = 2$ (respectivement $M = -1$ et $N = 2$) ; alors, la multiplicité de $(a_n)_{n\geq 0}$ est au plus égale à 3 (respectivement au plus égale à 4).

* De plus, si $N \neq \pm 1$ et $(a_0, a_1) = 1$; alors :

1) Si $M = 1$, les solutions de $a_n = a_0$ avec $n > 0$ appartiennent toutes à la même classe d'équivalence modulo N.

2) Si $M = -1$ et $N \neq \pm 1, \pm 2$; alors les solutions de $a_n = a_0$ avec $n > 0$ sont toutes de même parité.

* En imposant quelques autres fortes conditions ; on obtient les résultats suivants :

−Si $(a_0, a_1) = 1$ et $2 \nmid MN$; alors la multiplicité de $(a_n)_{n\geq 0}$ est au plus égale à 5.

* Si $M = 2M'$ $(M' \neq 0))$, $2 \nmid Na_0$, $M^2 - 4N < 0$ et $(a_0, a_1) = 1$; on en déduit que :

−Si M' est impair, $N \equiv 3 \pmod 4$; alors $m\,(a_0) \leq 3$ (respectivement $m\,(a_0) \leq 4$ si $N \equiv 1 \pmod 4$).

−Si M' est pair ; alors $m\,(a_0) \leq 3$, si $N \equiv 1 \pmod 4$ (respectivement $m\,(a_0) \leq 4$, si $N \equiv 3$

(mod 4).

–Enfin, si $(M, N) = 1$ et $(a_0, a_1) = 1$, alors la multiplicité est ou bien infinie ou bien bornée supérieurement par 4.

2) La multiplicité en utilisant des arguments algébriques :

Soit $(a_n)_{n\geq 0}$ une suite linéaire récurrente entière définie par

$$a_{n+2} = c_1 a_{n+1} + c_2 a_n$$

Et soient α_1, α_2 les racines du polynôme caractéristique $x^2 - c_1 x - c_2$. En posant $\lambda_1 = a_1 - \alpha_2 a_0$ et $\lambda_2 = a_1 - \alpha_1 a_0$, on voit que $(a_n)_{n\geq 0}$ est donnée par

$$a_n = \frac{\lambda_1 \alpha_1^n - \lambda_2 \alpha_2^n}{\alpha_1 - \alpha_2}$$

Par conséquent l'étude de la multiplicité de $(a_n)_{n\geq 0}$ revient à résoudre l'équation

$$\lambda_1 \alpha_1^n - \lambda_2 \alpha_2^n = \pm (\lambda_1 - \lambda_2)$$

Dans le cas particulier si $\Delta = c_1^2 + 4c_2 < 0$, on a $\lambda_2 = \overline{\lambda_1}$ et $\alpha_2 = \overline{\alpha_1}$; donc l'équation précédente peut s'écrire comme suit

$$\lambda \alpha^n - \overline{\lambda}\overline{\alpha}^n = \pm (\lambda - \overline{\lambda})$$

Et par conséquent, on a les résultats suivants :

* Soient $\mathbb{k}$ un corps quadratique imaginaire et α, λ des entiers algébriques dans $\mathbb{k}$ avec $0 < \arg \alpha < \frac{\pi}{2}$: $0 < \arg \lambda < \pi$ et $\frac{\alpha}{\overline{\alpha}}$ n'est pas une racine de l'unité ; alors toutes les solutions des équations $\lambda \alpha^n - \overline{\lambda}\overline{\alpha}^n = \pm (\lambda - \overline{\lambda})$ sont déterminées. De plus, on a :

–Si $(\alpha, \lambda) = \left(\frac{1+\sqrt{-7}}{2}, \frac{1+\sqrt{-7}}{2}\right)$, alors $n = 0, 1, 2, 4, 12$, qui signifie que $m(a_0) + m(-a_0) = 5$.

–Si $(\alpha, \lambda) = \left(1 + \sqrt{-2}, \sqrt{-2}\right)$, alors $n = 0, 1, 2, 5$, qui signifie que $m(a_0) + m(-a_0) = 4$.

–Si $(\alpha, \lambda) = \left(\frac{1+\sqrt{-11}}{2}, \frac{1+\sqrt{-11}}{2}\right)$; alors $n = 0, 1, 4$, qui signifie que $m(a_0) + m(-a_0) = 3$.

–Si $(\alpha, \lambda) = \left(\frac{1+\sqrt{-11}}{2}, \frac{-3+\sqrt{-11}}{2}\right)$; alors $n = 0, 1, 3$, qui signifie que $m(a_0) + m(-a_0) = 3$.

–Si $(\alpha, \lambda) = \left(\frac{1+\sqrt{-15}}{2}, \frac{-3+\sqrt{-15}}{2}\right)$; alors $n = 0, 1, 3$, qui signifie que $m(a_0) + m(-a_0) = 3$.

–Si $(\alpha, \lambda) = \left(\frac{1+\sqrt{-19}}{2}, \frac{1+\sqrt{-19}}{2}\right)$; alors $n = 0, 1, 6$, qui signifie que $m(a_0) + m(-a_0) = 3$.

D'autre part, si $(a_0, a_1) = 1$, $c_1 \geq 0$ et $\Delta = c_1^2 + 4c_2 < 0$; alors l'équation $\lambda \alpha^n - \overline{\lambda}\overline{\alpha}^n = \pm (\lambda - \overline{\lambda})$ a plus de trois solutions pour les valeurs de (λ, α) suivantes :

$$\left(\frac{1+\sqrt{-7}}{2}, \frac{1+\sqrt{-7}}{2}\right), \left(\frac{-1+\sqrt{-7}}{2}, \frac{3+\sqrt{-7}}{2}\right), \left(\frac{-3+\sqrt{-7}}{2}, \frac{1+\sqrt{-7}}{2}\right),$$
$$\left(\frac{-3+\sqrt{-11}}{2}, \frac{1+\sqrt{-11}}{2}\right), \left(\frac{-3+\sqrt{-15}}{2}, \frac{1+\sqrt{-15}}{2}\right) \text{ et } \left(\sqrt{-2}, 1+\sqrt{-2}\right)$$

Enfin si $(a_n)_{n\geq 0}$ est non dégénérée telle que $a_0 > 0$, $(a_0, a_1) = 1$, $c_1 \geq 0$ et $\Delta = c_1^2 + 4c_2 \geq 0$; alors, l'équation $a_n = \pm a_0$ a au plus trois solutions. ie., $m(a_0) + m(-a_0) \leq 3$ sauf si $c_1 = c_2 = 1$, $a_0 = 1$ et $a_1 = -1$ où dans ce cas les solutions sont $n = 0, 1, 3, 4$.

3)Concernant l'étude des carrés parfaits : les principaux résultats sont :

–Les seuls carrés parfaits dans une suite de Fibonacci sont $F_0 = 0$, $F_{-1} = F_1 = F_2 = 1$ et $F_{12} = 144$.

–Les seuls carrés parfaits dans une suite de Lucas vérifiant $(P, Q) = (1, -1)$ sont $L_1 = 1$ et $L_3 = 4$.

* Le cas des suites de Lucas généralisées est un peu compliqué, pour cela, on a restreint l'étude au cas où P, Q sont impairs, premiers entre eux et vérifiant $P^2 - 4Q > 0$. La méthode de recherche des carrés parfaits se fait en suivant les étapes suivantes :

–On cherche des entiers b tels que $x_{n+12} \equiv x_n \pmod b$.

Soit I l'ensemble des indices a , $0 \leq a < 12$, tels que x_a soit un carré modulo tous ces entiers b.

–Si x_a $(0 \leq a < 12)$ est un carré et si pour tout $j \geq 1$, x_a est premier à un diviseur premier $p_j \equiv -1 \pmod 4$ de $V_{3.2^j}$; alors aucun x_{a+12n} $(n \neq 0)$ n'est un carré. Sinon, i.e., si x_a est un carré modulo les entiers b, mais un non-carré parfait, alors x_{a+12n} peut être un carré. Dans ce cas, on commence à tester x_a modulo les diviseurs premiers de V_6. On distingue quatre cas.

a) S'il existe un diviseur premier $p \equiv 1 \pmod 4$ de V_6, et si x_a est un non carré modulo p; alors aucun x_{a+12n} n'est un carré. Sinon :

*b.*1) S'il n'existe pas de diviseur premier $p \equiv 1 \pmod 4$ de V_6, et s'il y a deux diviseurs premiers p, $p' \equiv -1 \pmod 4$ de V_6 tels que $\left(\frac{x_a}{p}\right)$ et $\left(\frac{x_a}{p'}\right)$ sont opposés; alors aucun x_{a+12n} n'est un carré.

*b.*2) Si x_a est un carré modulo tous les diviseurs premiers $p \equiv -1 \pmod 4$ de V_6, alors on passe x_a au test V_{12} et on reprend le même processus précédent.

*b.*3) Si x_a est un non carré modulo tous les diviseurs premiers $p \equiv -1 \pmod 4$ de V_6 ; alors on test x_{a+12} ou x_{a-12} modulo tous les diviseurs premiers de V_{12} et on reprend les mêmes étapes appliquées à V_6... et ainsi de suite.

Bibliographie

[1] Alter and K. K. Kubota, multiplicities of second order linear recurrences.

[2] Y. Amice, Les nombres p-adiques. Colledtion sup, no 14, Les presses universitaires de France, Paris 1975.

[3] J. Berstel, sur le calcul des termes d'une suite récurrente linéaire, exposé fait à l'I.R.R.I.A (Rocquencourt) en mars 1974.

[4] Berstel and M. Mignotte; deux propriétés décidables des suites récurrentes linéaires. Bull. Soc. Math. France. 104, pp 175-184 (1976).

[5] F. Beukers, the multiplicity of binary recurrences. Composito math. 40 (1980), pp 251-267.

[6] F. Beukers, The zero multiplicity of ternary recurrences. Composito Math. 77 (1991), pp 165-177.

[7] F. Beukers and R. Tijdeman, on the multiplicities of binary complex recurrences. Composito math. 51 (1984), pp 193-213.

[8] Z. I. Borevitch et I. R. Chafarevitch, Théorie des nombres, Gauthier-Villars, Paris. 1967.

[9] P. Borwein and T. Erdelyi, polynomials and polynomial inequalities. Springer (1995).

[10] L. Cerlienco, M. Mignotte et F. Piras, Suites récurrentes linéaires. Propriétés algébriques et arithmétiques, L'enseignement Mathématiques 33 (1987), pp 67-108.

[11] P. Chowla, S. Chowla, M. Dunton and D. J. Lewis, some diophantine equations in quadratic number fields, Norsk vid. Selsk. Forth.31 (1958), pp 181-183.

[12] S. Chowla, M. Dunton and D. J. Lewis, linear recurrences of order two, pacific J. Math. 11 (1961), pp 833-843.

[13] H. Cohen : A course in computational algebraic number theory. Springer (1993).

[14] J. H. E. Cohn, On square Fibonacci numbers, J. London Math. Soc. 39 (1964), pp 537-541.

[15] J. H. E. Cohn, The diophantine equation $x^2 - Dy^2 = 1$, Acta Arith. 78 (1997), pp 401-403.

[16] D. Duverney, Théorie des nombres (cours et exercices corrigés), 2e édition-Paris, Dunod, impr. 2007.

[17] V. Halava, T. Harju, M. Hirvensalo and J. Karhumaki : Skolem's porblem on the border between decidability and undecidability. Tucs Tech. Report no 683, April 2005.

[18] G. Hansel. Une demonstration simple du théorème de Skolem-Mahler-Lech. Theoret. Comput. Sci.43, pp 1-10 (1986).

[19] S. Katok, real and p-adic analysis, course notes for Math 497 C, Mass Program, Fall 2000 (2001).

[20] K. K. Kubota, On a conjecture of Morgan Ward. I, II. Acta Arith. 33 (1977), pp 11-28, 29-48.

[21] R. R. Laxton, Linear recurrences of order two, J. Austral Math. Soc. 7 (1967), pp 108-114.

[22] M. Mignotte. Suites récurrentes linéaires, Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 15, no 2 (1973-1974), exp no G 14, pp 1-9.

[23] L. J. Mordell. Diophantine equations, Academic press, London, 1969.

[24] P. Robba, Zéros de suites récurrentes linéaires, Groupe de travail ultramétrique, tome 5 (1977-1978), exp no 13, pp 1-5.

[25] P. Samuel, Les carrés dans des généralisations des suites de Lucas. Tome 16, no 3 (2004), pp 693-703.

[26] H. P. Schlickewei, Multiplicities of recurrence sequences, Acta. Math. 176 (1996), pp 171-243.

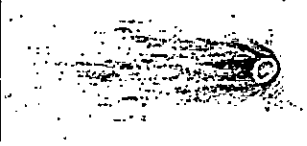
[27] H . P. Schlickewei and A. J. Van der Poorten, Zeros of recurrence sequences, Bull. Austral. Math. Soc. 44 (1991), pp 215-223.

[28] W. M. Schmidt, The zero multiplicity of linear recurrence sequences, Acta. Math. 182 (1999), pp 243-282 .

[29] W. M. Schmidt, zeros of linear recurrence sequences, publ. Math. Debrecen. 56 (2000), pp 609-630.

[30] R. Tijdeman, Multiplicities of binary recurrences. Sémin. Théorie de nombres, Univ. Bordeaux 1, 1980-1981. Exp. 29, 11 p.

[31] N. K. Vereshchagin, Occurrence of zero in a linear recursive sequence, Vestnik Moskov. Univ. Math. Vol 41 (1986).



ملخص

خلال هذا البحث قمنا بدراسة مسالة التعددية في متتالية تراجعية خطية من الرتبة الثانية.استعملنا في البداية طرق بياديكية للبرهان علي أن تعددية أي متتالية تراجعية خطية صحيحة من الرتبة الثانية لا تتعدي خمسة. وباستعمال طرق أخرى جبرية قمنا بتحسين هذا الحد حيث برهنا أن هذه التعددية لا تتعدى عموما ثلاثة. من جهة أخرى قمنا بتحديد صيغة صريحة تعطي الحد العام لأي متتالية تراجعية خطية كيفية بدلالة جذور كثير الحدود المميز. وفي الأخير عملنا علي دراسة حالة خاصة للتعددية تتمثل في البحث عن المربعات التامة في ممتاليات فيبوناتشي و ليكا و أوجدنا طريقة فعالة للبحث عن هذه المربعات.

Abstract

In this work, we give some of the major results concerning the multiplicity of binary linear recurrence sequences. We use first p-adic arguments to prove that the multiplicity of any integer binary linear recurrences does not exceed five, by using algebraic ones; we improve this bound to be at most three. We also determined a closed form representing the general term for any linear recurrence sequence in term of the roots of the characteristic polynomial. Finally, we studied an other problem of presence of perfect squares in Fibonacci and Lucas sequences which represent a particular case of multiplicity, and we found an effective method for searching this squares.

Résumé

Le but de ce travail est de présenter quelques résultats intéressants concernant la multiplicité des suites linéaires récurrentes d'ordre deux. On a utilisé premièrement des arguments p-adiques pour prouver que la multiplicité de toute suite linéaire récurrente binaire à termes entiers ne dépasse pas cinq. En utilisant des méthodes algébriques, on peut améliorer cette borne à trois. On détermine aussi une formule explicite représentant le terme général de toute suite linéaire récurrente quelconque. Enfin, on a étudié un autre problème qui consiste à chercher les carrés parfaits dans les suites de Fibonacci et Lucas, ceci représente un cas particulier du problème de multiplicité, et on a établi une méthode efficace pour la recherche de ces carrés.