N° d'ordre : 03/2020-D/MT

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université des Sciences et de la Technologie Houari Boumediène

Faculté de MATHEMATIQUES

THESE

Présentée pour l'obtention du **grade** de **DOCTEUR EN SCIENCES**

En : **MATHEMATIQUES**

Spécialité : **Algèbre et théorie des nombres**

Par : **ABCHICHE Mourad**

Sujet

Aspects p-adiques et combinatoires liés aux suites récurrentes linéaires

Soutenue publiquement le 05/03/2020 à 14h00, devant le jury composé de :

M. Abdelaziz BELLAGH	Maître de conférences/ A à l'U.S.T.H.B	Président
M. Kamel BETINA	Professeur à l'U.S.T.H.B	Directeur de thèse
M. Hacène BELBACHIR	Professeur à l'U.S.T.H.B	Co-directeur de thèse
M. Ahmed AIT MOKHTAR	Maître de conférences/ A à l'E.N.S (Kouba)	Examinateur
M. Abdelkader BOUYAKOUB	Professeur à l'université Oran 1	Examinateur
M. Abdellah DERBAL	Professeur à l'E.N.S (Kouba)	Examinateur

Remerciements

En premier lieu, je remercie sincérement mon directeur de thèse Kamel BETINA pour sa disponibilité, son soutien, son aide et ses encouragements durant ces longues années de collaboration.

J'exprime ma reconnaissance et ma gratitude envers mon codirecteur de thèse Hacène BELBACHIR pour m'avoir initié à la combinatoire et intégré dans son équipe. Son soutien, sa gentillesse et son amitié me touchent beaucoup.

Ma reconnaissance et mes remerciements à Abdelkader NECER pour le travail qu'on a réalisé ensemble, pour son accueil chaleureux et pour tout le temps qu'il m'a consacré durant chacun de mes stages à l'université de Limoges. Ma profonde gratitude pour sa patience et pour l'amitié qu'il m'a toujours témoignée.

Un grand merci à Abdelaziz BELLAGH pour m'avoir fait l'honneur d'accepter de présider le jury de cette thèse.

J'adresse aussi mes vifs remerciements à Ahmed AIT MOKHTAR de l'E.N.S de Kouba, à Abdellah DERBAL également de l'E.N.S de Kouba et à Abdelkader BOUYAKOUB de l'université Oran 1 pour avoir accepté de faire partie du jury et de donner de leur temps pour examiner ce travail.

Merci à tous les collègues et amis de la faculté de Mathématiques qui m'ont soutenu, conseillé et encouragé.

A mon épouse Djamila, à mes enfants Ghiles et Sara et à toute ma famille, merci pour tout.

Table des matières

Introduction

Ce travail s'inscrit dans le cadre de l'étude des suites récurrentes linéaires (s.r.l) qui prennent leur origine en 1202 avec l'exemple donné par Fibonacci de la célèbre suite $1, 1, 2, 3, 5, 8, 13, ...$ qui porte son nom (voir [66] et [43]). C'est un domaine riche et varié dont le champ d'applications est divers (cryptographie, codes correcteurs d'erreurs, informatique, algorithmique, combinatoire, théorie des nombres etc.). Une très abondante littérature lui est consacrée voir par exemple [19], [46], [63], [48], [60] etc.

La thèse et centrée sur deux notions : la notion de congruence dans les s.r.l, avec l'utilisation de l'outil p-adique, et la notion d'étude combinatoire, consacrée aux polynômes bivariés généralisés de Fibonacci et de Lucas, aux polynômes de Chebyshev et à la généralisation de la formule de congruence de Lucas.

Le document est divisé en cinq chapitres. Le premier est consacré au rappel de quelques définitions et principaux résultats utiles pour les besoins du chapitre 2. Il s'agit notamment de généralités sur les s.r.l, de suites d-extraites d'une s.r.l et de leurs polynômes caractéristiques, qui joueront un rôle central dans la problématique qui nous occupera dans le chapitre suivant. Puis de la notion de corps valués ultramétriques et de la construction, pour un nombre premier p, du corps $\mathbb{Q}_p$ des nombres p-adiques comme complété de $\mathbb{Q}$ par rapport à sa valeur absolue p-adique. Nous aborderons aussi la notion de valuation, d'extension de $\mathbb{Q}_p$, d'uniformisante, de corps résiduel etc.

Le second chapitre consiste en l'établissement de congruences entre les termes d'une suite récurrente linéaire $u = (u_n)_n$ vérifiant $u_{n+m} = a_{m-1}u_{n+(m-1)} + \cdots + a_1u_{n+1} + a_0u_n$, où les a_i sont des entiers avec a_0 non nul. Plus précisément, étant donné un nombre premier p, l'objectif est de déterminer tous les entiers naturels non nuls d pour lesquels la congruence $u_{n+md} \equiv a_{m-1}u_{n+(m-1)d} + \cdots + a_1u_{n+d} + a_0u_n \bmod p$ est réalisée quel que soit n dans $\mathbb{N}$. Pour ce faire, l'idée est qu'au lieu d'agir directement sur les termes de cette suite, on passe plutôt par son polynôme caractéristique $f(X) = X^m - a_{m-1}X^{m-1} - \cdots - a_1X - a_0 \in \mathbb{Z}[X]$ et le polynôme caractéristique f_d de ses suites d-extraites.

Ce qui a motivé ce travail est un article de H.T. Freitag [32] paru en 1984, dans lequel l'auteure a montré que, pour le cas de la suite $(F_n)_n$ de Fibonacci, on a $F_{n+2d} \equiv F_{n+d} + F_n \bmod 10$ pour tout n, si et seulement si $d \equiv 1$ ou $5 \bmod 12$. Ce résultat a connu plusieurs généralisations à d'autres s.r.l voir [33], [34], [74]. Seulement les conditions données sur l'entiers d sont à chaque fois des conditions nécessaires et non suffisantes.

Dans cette partie il est montré que l'on peut ramener le problème à des congruences entre polynômes caractéristiques. L'avantage de cette approche est d'avoir obtenu sur les exemples traités, au moyen de l'outil p-adique, des conditions nécessaires et suffisantes sur d pour que

les congruences en question se réalisent. L'un de nos principaux résultats concerne la suite de Fibonacci et généralise le résultat de Freitag. Ce dernier a traité le cas $p = 2$ et $p = 5$, le résultat que nous avons obtenu le fait pour une multitude de nombres premiers.

Certaines suites étudiées au chapitre 2, telles que les suites de Fibonacci, de Lucas, de Pell, font partie d'une famille plus générale de suites récurrentes linéaires que nous avons appelées suites de polynômes bivariés généralisés de Fibonacci et de Lucas. Les suites de polynômes de Catalan, de Lucas, de Jacobsthal, de Byrd,... en sont aussi des cas particuliers. L'objet du chapitre 3 est l'étude des propriétés de cette famille de polynômes. Nous exhiberons, notamment, un lien avec les polynômes de Chebyshev, ce qui permet une transition au chapitre suivant.

Le quatrième chapitre consiste à étendre une certaine étude faite sur les polynômes de Chebyshev de première et deuxième espèce définis, respectivement, par les relations de récurrences linéaires $T_n = 2XT_{n-1} - T_{n-2}$ avec $T_0 = 1, T_1 = X$ et $U_n = 2XU_{n-1} - U_{n-2}$ avec $U_0 = 1, U_1 = 2X$ aux polynômes généralisés de Chebyshev obtenus en remplaçant dans les récurrences précédentes, le monôme $2X$ par un polynôme $h(X)$ de degré supérieur ou égal à 1 à coefficients réels et distinct du monôme aX avec a rationnel. Il s'agit dans un premier temps d'en donner les formules explicites et d'identifier l'espace vectoriel $\mathbb{E}_n[X]$ auquel ils appartiennent ainsi que sa base canonique. On munit ensuite $\mathbb{E}_n[X]$ de deux nouvelles bases dont l'une contient les polynômes T_n et l'autre les U_n puis on détermine les coordonnées des polynômes généralisés de Chebyshev dans ces nouvelles bases. L'objectif étant de mettre la lumière sur l'intéraction existante entre ces polynômes, à travers les écritures obtenues.

Il est important de souligner que les résultats obtenus ne s'appliquent pas au cas $h(X) = aX$ avec a rationnel (et en particulier à $h(X) = 2X$) ce qui justifie l'emploi délibéré de l'expression "étendre l'étude à h" au lieu de " généraliser l' étude à h", utilisée au début du paragraphe.

Le cinquième chapitre est consacré à la formule de congruence de Lucas qui se trouve dans son fascicule intitulé "Théorie des fonctions numériques simplement périodiques" paru dans la revue "American journal of mathematics" en 1878 (voir [51]) et dans lequel il démontre que pour p premier, si $n = n_0 + n_1p + \cdots + n_mp^m$ et $k = k_0 + k_1p + \cdots + k_mp^m$ sont les écritures des entiers n et k en base p, alors $\binom{n}{k} \equiv \binom{n_0}{k_0}\binom{n_1}{k_1}\cdots\binom{n_m}{k_m} \bmod p$.

Après un aperçu non exhaustif des nombreux développements qu'a connus cette formule, tirés essentiellement du papier d'Andrew Granville [37] publié en 1997 et du livre de L. E. Dickson [26] "History of the theory of numbers", nous proposons une généralisation de cette formule de Lucas aux coefficients bi^{s}nomiaux qui sont une généralisation naturelle des coefficients binomiaux et qui correspondent aux coefficients des x^k issus du développement de $(1 + x + x^2 + \cdots + x^s)^n$ en puissances de x.

Chapitre 1

Suites récurrentes linéaires, nombres p-adiques et loi de réciprocité quadratique

Dans ce chapitre nous traiterons d'abord des suites récurrentes linéaires dans leurs généralités, ensuite nous aborderons quelques notions sur les nombres p-adiques et terminerons par rappeler la loi de réciprocité quadratique.

1.1 Suites récurrentes linéaires

Les suites récurrentes linéaires sont nées en 1202 avec la célèbre suite $1, 1, 2, 3, 5, 8, 13, \cdots$ donnée par le mathématicien italien Leonardo Fibonacci $(1175 - 1250)$ (voir [43] et [66]), qui porte son nom et dans laquelle chaque terme est la somme des deux termes qui le précédent.

L'étude des suites récurrentes est un domaine si riche et varié dont le champ d'applications est divers que, de l'avis des spécialistes, il est impossible de réaliser une bibliographie complète sur le sujet. Les lecteurs trouveront néanmoins, dans [19], [46], [63], [48], [60] une bonne présentation des suites récurrentes linéaires, qu'elles soient définies sur des anneaux, des corps ou des modules. Une bibliographie très intéresssante y est jointe.

Dans ce travail, nous allons considérer les suites récurrentes linéaires à valeurs dans un corps commutatif K et nous nous contenterons de donner les propriétés qui nous seront utiles pour les besoins de ce mémoire. L'essentiel des preuves se trouve dans [19].

1.1.1 Définitions et propriétés

Soit K un corps commutatif. On note par $S(K)$ l'ensemble des suites à valeurs dans K. Un élément de $S(K)$ sera noté $u = (u(n))_{n\geq 0}$ ou $u = (u_n)_{n\geq 0}$.

$K[X]$ désigne l'algèbre des polynômes à coefficients dans K.

Pour $u = (u(n))_{n\geq 0} \in S(K)$ et $P(X) = \sum_{0\leq i\leq d} a_i X^i \in K[X]$ avec d dans $\mathbb{N}$, on définit le "produit" Pu par

$$(Pu)(n) = \sum_{0\leq i\leq d} a_i u(n+i).$$

Ce produit Pu peut aussi être défini grâce à l'opérateur schift E qui associe à une suite $u = (u(n))_n$ la suite décalée $E(u) = (u(n+1))_n$. Dans ce cas $Pu = P(E)(u) = \sum_{0\leq i\leq d} a_i E^i(u)$ défini pour tout entier n par

$$(Pu)(n) = \sum_{0\leq i\leq d} a_i u(n+i).$$

Les opérations somme des suites et la multiplication Pu confèrent à $S(K)$ une structure de $K[X]$-module. Il est bon de noter aussi que $S(K)$ est un K-espace vectoriel par rapport à la somme de suites et la multiplication par un scalaire (élément de K).

Pour $u \in S(K)$, on désigne par I_u l'idéal annulateur de u dans $K[X]$,
$I_u = \{P \in K[X];\ Pu = 0\}$.

Suites récurrentes linéaires

On dit qu'une suite u est une suite récurrente linéaire (en abrégé s.r.l) si I_u est non nul. L'idéal I_u est alors appelé "l'idéal caractéristique de u " et les polynômes unitaires de I_u sont appelés "les polynômes caractéristiques de u ". L'anneau $K[X]$ étant principal, l'idéal I_u est engendré par un polynôme unitaire de degré minimal d appelé "le polynôme minimal de la s.r.l u ". C'est donc le polynôme caractéristique dont le degré est le plus bas. On dit alors que u est de longueur (ou de rang) d.

Dans le cas général où K est juste un anneau commutatif (voir [63]), une suite u est une s.r.l si son idéal annulateur contient un polynôme unitaire.

Somme de suites récurrentes linéaires

Si $u = (u_n)_n$ et $v = (v_n)_n$ sont deux s.r.l de polynômes caractéristiques respectifs P et Q alors leur somme $u + v = (u_n + v_n)_n$ est une s.r.l de polynôme caractéristique PQ.

Produit par un polynôme

Si $u = (u_n)_n$ est une s.r.l admettant $G(X) = P(X)Q(X)$ pour polynôme caractéristique alors la suite Pu ou $P(E)u$ est une s.r.l de polynôme caractéristique Q.

Espace des suites récurrentes linéaires

L'ensemble des suites récurrentes linéaires sur K, noté SR(K), est un $K[X]$-module (par rapport aux opérations définies plus haut qui font de $S(K)$ un $K[X]$-module).

Soit $P(X) = X^m - a_{m-1}X^{m-1} - \cdots - a_0 \in K[X]$. On considère l'ensemble SR_P de toutes les s.r.l de polynôme caractéristique P. Un élément u de SR_P est déterminé de manière unique

par ses m premiers termes $u_0, u_1, ..., u_{m-1}$. Chaque autre terme est une combinaison linéaire de ceux-ci. Il en résulte que SR_P est un sous-espace vectoriel de $S(K)$ de dimension m. Une base étant formée par les suites $v^{(i)} = (v_n^{(i)})_{n\geq 0}$, $0 \leq i \leq m-1$ de SR_p définies par les conditions initiales $v_j^{(i)} = \delta_j^i$, $0 \leq j \leq m-1$ où δ_j^i est le symbole de Kronecker qui vaut 1 si $i = j$ et 0 sinon. Sur cette base un élément u de SR_P s'écrit $u = u_0 v^{(0)} + u_1 v^{(1)} + \cdots + u_{m-1} v^{(m-1)}$.

Terme général

Soit $u = (u_n)_n$ une suite récurrente linéaire de polynôme caractéristique

$$P(X) = X^m - a_{m-1}X^{m-1} - \cdots - a_1 X - a_0 \in K[X],$$

définie par

$$u_{n+m} = a_{m-1}u_{n+(m-1)} + \cdots + a_1 u_{n+1} + a_0 u_n, \tag{1.1}$$

où les a_i sont dans K avec $a_0 \neq 0$.

La détermination du terme général de cette suite est possible pourvu que l'on soit capable de calculer les puissances de la matrice compagnon de la suite (voir plus bas) ou de factoriser le polynôme P dans une extention convenable de K.

Considérons la suite définie par $v_n = {}^t(u_n, u_{n+1}, ..., u_{n+(m-1)})$ où ${}^t v$ désigne le vecteur tansposé du vecteur v. La relation (1.1) induit alors sur la suite (v_n) la relation $v_{n+1} = Av_n$ où

$$A = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ a_0 & a_1 & \cdots & a_{m-1} \end{pmatrix}$$

est la matrice compagnon de la suite u, de polynôme caractéristique $P(X)$.

Lorsque le calcul de la puissance n-ème de la matrice A s'effectue sans réelle difficulté, le terme v_n s'obtient par $v_n = A^n\ v_0$.

Soit le m-uplet $\alpha = (1, 0, ..., 0)$. Le terme général de la suite u est alors, pour tout n dans $\mathbb{N}$,

$$u_n = \alpha\ A^n\ v_0.$$

Il se trouve que ce n'est pas toujours le cas (i.e. A^n n'est pas toujours facile à calculer). D'où l'intérêt de chercher à factoriser le polynôme P.

Dans le corps L de décomposition de P sur K

$$P(X) = \prod_{i=1}^{s} (X - \alpha_i)^{m_i},$$

avec $s \in \mathbb{N}^*$, m_i la multiplicité de la racine α_i et $\sum_{i=1}^{s} m_i = m$.

Il existe alors des polynômes $P_i \in L[X]$ $(1 \leq i \leq s)$ de degré $\leq m_i - 1$ tels que

$$u_n = \sum_{1 \leq i \leq s} P_i(n)\alpha_i^n. \tag{1.2}$$

Écriture explicite des P_i $(1 \leq i \leq s)$

La série génératrice formelle $S(X) = \sum_{n \geq 0} u_n X^n$ de la suite récurrente linéaire u est une fraction rationnelle. Il existe donc deux polynômes $A, B \in K[X]$ tels que $S(X) = \dfrac{A(X)}{B(X)}$ avec $B(X) = X^m P(\dfrac{1}{X})$ et $B(0) \neq 0$ (voir [19]).

Dans $L[X]$, le polynôme $B(X)$ s'écrit

$$B(X) = -a_0 \prod_{i=1}^{s} (X - \omega_i)^{m_i},$$

où $\omega_i = \dfrac{1}{\alpha_i}$ $(1 \leq i \leq s)$.

La décomposition en éléments simples de la fraction $\dfrac{A(X)}{B(X)}$ donne

$$\frac{A(X)}{B(X)} = Q(X) + \sum_{i=1}^{s} \sum_{j=1}^{m_i} \frac{a_{ij}}{(X - \omega_i)^j},$$

où $Q(X)$ est un polynôme à coefficients dans K et $a_{ij} \in L$.

L'identité formelle

$$\frac{1}{(x - \omega)^j} = (-1)^j \omega^{-j} \sum_{n \geq 0} \binom{n + j - 1}{j - 1} (x\omega^{-1})^n,$$

entraîne

$$S(X) = Q(X) + \sum_{n \geq 0} \sum_{i=1}^{s} \sum_{j=1}^{m_i} (-1)^j a_{ij} \alpha_i^{n+j} \binom{n + j - 1}{j - 1} X^n.$$

D'où l'on déduit qu'à partir de $n_0 = d^\circ Q$,

$$u_n = P_1(n)\alpha_1^n + \cdots + P_s(n)\alpha_s^n,$$

avec

$$P_i(n) = \sum_{j=1}^{m_i} (-1)^j a_{ij} \alpha_i^j \binom{n + j - 1}{j - 1}.$$

A titre d'exemples, voir la preuve du théorème 3.5, page 60.

1.1.2 Suites d-extraites

Soit $u = (u_n)_n$ une s.r.l vérifiant (1.1) de matrice compagnon A et de polynôme caractéristique $P(X) = X^m - a_{m-1}X^{m-1} - \cdots - a_1X - a_0 \in K[X]$. Les sous-suites $u^{(0)}, u^{(1)}, ..., u^{(d-1)}$ définies pour tout entier naturel non nul d et tout entier naturel n par $u_n^{(j)} = u_{dn+j}$ s'appellent suites d-décimées ou suites d-extraites de la suite u.

Les suites d-extraites de la s.r.l u sont elles-mêmes des s.r.l ; de plus si dans une extension convenable du corps K

$$P(X) = \prod_{i=1}^{s}(X - \alpha_i)^{m_i},$$

alors

$$Q(X) = \prod_{i=1}^{s}(X - \alpha_i^d)^{m_i}$$

est un polynôme caractéristique des suites d-extraites de la suite u (voir [19]), c'est aussi le polynôme caractéristique de la matrice A^d.

L'application qui associe à une suite récurrente linéaire u le d-uplet de ses suites d-extraites $(u^{(0)}, u^{(1)}, .., u^{(d-1)})$ est un isomorphisme d'espaces vectoriels. Son inverse est l'opérateur d'emboîtement qui consiste à construire à partir d'un d-uplet de suites récurrentes linéaires $(u^0, u^1, \cdots, u^{d-1})$ une s.r.l u dont les suites d-extraites sont justement les u^j. Il suffit de poser pour tout $n \geq 0$:

$$u_{dn} = u_n^0, \quad u_{dn+1} = u_n^1, ..., u_{d(n+1)-1} = u_n^{d-1}.$$

1.2 Le corps des nombres p-adiques

La découverte des nombres p-adiques remonte à 1897 par le mathématicien Kurt Hensel $(1861 - 1941)$. Sa première motivation était d'utiliser les techniques des séries entières pour résoudre des problèmes de théorie des nombres. Aujourd'hui la théorie des nombres p-adiques dépasse largement ce cadre, elle fournit un outil puissant pour arriver à bout de problèmes dans diverses branches des mathématiques. Déjà en 1975 dans sa préface à l'ouvrage de Y. Amice [3], Charles Pisot a prédit que le progrès dans le p-adique aura des répercussions sur l'ensemble des mathématiques.

Il y'a plusieurs approches (équivalentes) pour la construction du corps $\mathbb{Q}_p$ des nombres p-adiques. Nous invitons les lecteurs à consulter les ouvrages de Y. Amice [3], Z. I. Borevitch et I. R. Chafarevitch [15], P. Colmez [22], N. Koblitz [42], A. M. Robert [68],... Une bibliographie très riche y est jointe.

Pour notre part, nous avons choisi la méthode analytique qui consiste à voir $\mathbb{Q}_p$ comme le complété de $\mathbb{Q}$ pour la valeur absolue p-adique. Nous rappelerons les notions dont nous nous servirons pour cette construction et nous donnerons les propriétés qui nous seront utiles pour les besoins cette thèse.

Les définitions, résultats et preuves se trouvent dans les références citées plus haut.

1.2.1 Notion de valeur absolue sur un corps commutatif

Une valeur absolue sur un corps commutatif K est une application $|\ .\ |$ de K dans $\mathbb{R}^+$ vérifiant, pour tous $(x, y) \in K^2$, les propriétés suivantes :

1. $|\ x\ | = 0 \Leftrightarrow x = 0$,
2. $|\ xy\ | = |\ x\ |\ |\ y\ |$,
3. $|\ x + y\ | \leq |\ x\ | + |\ y\ |$ (inégalité triangulaire).

Un corps muni d'une valeur absolue est dit corps valué.

Exemples de valeurs absolues dans le cas $K = \mathbb{Q}$

Valeur absolue triviale

Elle est définie par $|\ 0\ | = 0$ et pour tout $x \in \mathbb{Q}^*$ par $|\ x\ | = 1$.

Valeur absolue usuelle ou ordinaire de $\mathbb{Q}$

Elle est définie pour tout $x \in \mathbb{Q}$ par

$$|\ x\ | = \max(x, -x) = \begin{cases} x & \text{si } x \geq 0, \\ -x & \text{si } x < 0. \end{cases}$$

La valeur absolue usuelle de $\mathbb{Q}$ est souvent notée $|\ .\ |_\infty$.

Valeur absolue p-adique de $\mathbb{Q}$

Soit p un nombre premier. Tout $x \in \mathbb{Q}^*$ s'écrit de manière unique $x = p^k \dfrac{a}{b}$ avec $(k, a, b) \in \mathbb{Z}^3$ et a, b premiers entre eux, non divisibles par p. On pose alors

$$|\ x\ |_p = p^{-k},$$

avec la convention $|\ x\ |_p = 0$ si et seulement si $x = 0$.

L'application $|\ .\ |_p$ ainsi définie, est une valeur absolue sur $\mathbb{Q}$ appelée valeur absolue p-adique de $\mathbb{Q}$.

Valeur absolue ultramétrique

Une valeur absolue ultramétrique sur un corps commutatif K est une application $|\ .\ |$ de K dans $\mathbb{R}^+$ vérifiant, pour tous x, y dans K :

1. $|\ x\ | = 0 \Leftrightarrow x = 0$,

2. $\mid xy \mid = \mid x \mid \mid y \mid$,
3. $\mid x+y \mid \leq \max(\mid x \mid, \mid y \mid)$ (inégalité ultramétrique).

Il est clair que :
- l'inégalité ultramétrique entraîne l'inégalité triangulaire,
- si $\mid x \mid \neq \mid y \mid$ alors $\mid x+y \mid = \max(\mid x \mid, \mid y \mid)$, (pour la valeur absolue ultramétrique),
- la valeur absolue p-adique est une valeur absolue ultramétrique sur $\mathbb{Q}$.

Valeur absolue et topologie

Soit K un corps valué (muni d'une valeur absolue $\mid . \mid$). L'application d sur $K \times K$ définie, pour x et y dans K, par $d(x,y) = \mid x-y \mid$ est une distance sur K et définit donc une topologie sur K.

Deux valeurs absolues sur K sont dites équivalentes si leurs distances associées induisent la même topologie (i.e. les ouverts pour l'une sont les ouverts pour l'autre).

Proposition 1.1. *Deux valeurs absolues $\mid . \mid_1$ et $\mid . \mid_2$ sur K sont équivalentes si et seulement s'il existe $\alpha \in \mathbb{R}_+^*$ tel que $\forall x \in K$, $\mid x \mid_1 = \mid x \mid_2^{\alpha}$.*

Proposition 1.2. *Soient p et q deux nombres premiers. Deux valeurs absolues p-adique et q-adique $\mid . \mid_p$ et $\mid . \mid_q$ sur $\mathbb{Q}$ sont équivalentes si et seulement si p et q sont égaux.*

Théorème 1.3. *(Ostrowski)*
Toute valeur absolue non triviale sur $\mathbb{Q}$ est équivalente soit à la valeur absolue ordinaire $\mid . \mid_\infty$ soit à la valeur absolue p-adique $\mid . \mid_p$ où p est un nombre premier.

1.2.2 Corps valué ultramétrique ou non archimédien

Un corps valué est dit ultramétrique ou non archimédien s'il est muni d'une valeur absolue ultramétrique. Il est dit archimédien sinon.

Quelques propriétés des corps valués ultramétriques ou non archimédiens

Soit $(K, \mid . \mid)$ un corps valué ultramétrique.

1. Une suite $(x_n)_n$ d'éléments de K est une suite de Cauchy si et seulement si $\mid x_n - x_{n+1} \mid$ tend vers zéro quand n tend vers $+\infty$.
2. Si une suite $(x_n)_n$ d'éléments de K converge vers $x \in K^*$ alors il existe n_0 tel que $\forall n \geq n_0$, $\mid x_n \mid = \mid x \mid$.

3. Si K est complet, une série $\sum_{n\geq 0} x_n$ converge dans K si et seulement si $\mid x_n \mid$ tend vers zéro quand n tend vers $+\infty$.
4. Tout triangle dans K est isocèle.
5. Tout point d'une boule de K en est le centre.
6. Deux boules sont soit disjointes soit l'une est contenue dans l'autre.
7. Soient $A = D^+(0,1) = \{x \in K \ / \ \mid x \mid \leq 1\}$ la boule fermée de centre zéro et de rayon 1 et $\mathfrak{M} = D^-(0,1) = \{x \in K \ / \ \mid x \mid < 1\}$ la boule ouverte de centre zéro et de rayon 1. On a
   (a) A est un anneau et tout élément de K est soit dans A soit son inverse est dans A (on dit alors que A est un anneau de valuation).
   (b) A est un anneau local (i.e. possède un unique idéal maximal) d'idéal maximal $\mathfrak{M}$. A s'appelle l'anneau des entiers de K.
   (c) $\mathcal{U} = \{x \in K \ / \ \mid x \mid = 1\}$ est le groupe des unités de A (c'est un sous-groupe du groupe multiplicatif K^*).
   Nous avons la partition $A = \mathcal{U} \cup \mathfrak{M}$.
   (d) L'anneau quotient $k = \dfrac{A}{\mathfrak{M}}$ est un corps appelé le corps résiduel de K.

1.2.3 Valuation

Une valuation sur K est une application v de K dans $\mathbb{R} \cup \{+\infty\}$ vérifiant, pour tous x, y dans K, les conditions suivantes :

1. $v(x) = +\infty \Leftrightarrow x = 0$,
2. $v(xy) = v(x) + v(y)$,
3. $v(x+y) \geq \min(v(x), v(y))$.

Remarque 1.4. *1. Si K est un corps muni d'une valeur absolue ultramétrique $\mid . \mid$ et si $\lambda < 0$ alors l'application v définie sur K par $v(x) = \lambda \log |x|$ pour $x \in K^*$ et $v(0) = +\infty$ est une valuation sur K (*log *désigne le logarithme népérien).*

2. Réciproquement, étant donnés une valuation v sur K et un réel $0 < a < 1$, alors $|x| = a^{v(x)}$ est une valeur absolue ultramétrique sur K.

Il est donc équivalent de raisonner en termes de valuation ou en termes de valeur absolue ultramétrique. Ainsi, il vient de la propriété (7) des corps non archimédiens que l'anneau des entiers d'un corps valué ultramétrique $(K, \mid . \mid)$ est $A = \{x \in K \ / \ v(x) \geq 0\}$ où v est la valuation associée à $\mid . \mid$ définie dans le (1) de la remarque 1.4. A est un anneau local dont l'unique idéal maximal est $\mathfrak{M} = \{x \in K \ / \ v(x) > 0\}$ et le groupe des unités de K est $\mathcal{U} = \{x \in K \ / \ v(x) = 0\}$.

On peut rajouter aussi que l'anneau A est intègre et que son corps des fractions est K.

1.2.4 Valuation discrète - Uniformisante

D'après la deuxième condition de la définition d'une valuation (voir paragraphe 1.2.3), une valuation v est un morphisme du groupe multiplicatif K^* dans le groupe additif $\mathbb{R}$. Il s'ensuit que $v(K^*)$ est un sous-groupe de $\mathbb{R}$. La valuation v est dite discrète si $v(K^*)$ est un sous-groupe discret de $\mathbb{R}$ i.e. de la forme $a\mathbb{Z}$ avec $a \in \mathbb{R}_+^*$. Elle est dite normalisée si $v(K^*) = \mathbb{Z}$.

Puisque le produit d'une valuation v par tout $\lambda > 0$ reste une valuation sur K, on peut normaliser toute valuation v en la multipliant par $\frac{1}{a}$ tout en maintenant inchangés A, $\mathfrak{M}$ et $\mathcal{U}$.

Dans le cas d'une valuation normalisée v, un élément $\pi \in A$ tel que $v(\pi) = 1$ est appelé une uniformisante et tout élément $x \in K$ admet une écriture unique de la forme

$$x = \pi^m \ u,$$

avec $m = v(x) \in \mathbb{Z}$ et $u \in \mathcal{U}$.

1.2.5 Complétion d'un corps valué

Soit $(K, |\ .\ |)$ un corps valué. On note par $C(K)$ l'ensemble des suites de Cauchy à valeurs dans K et par $\mathcal{M}(K)$ l'ensemble des suites convergentes vers zéro. On montre que $C(K)$ est un anneau (unitaire) et $\mathcal{M}(K)$ est un idéal maximal de $C(K)$. Par conséquent, l'anneau quotient $\widehat{K} = \dfrac{C(K)}{\mathcal{M}(K)}$ est un corps.

La valeur absolue $|\ .\ |$ de K s'étend à $\widehat{K}$ (et se note de la même manière) en posant pour $\widehat{a} = (a_n)_n + \mathcal{M}(K) \in \widehat{K}$, $|\ \widehat{a}\ | = \lim\limits_{n\to\infty} |\ a_n\ |$.

Proposition 1.5. *Le corps $\widehat{K}$ est un corps complet pour la valeur absolue $|\ .\ |$ et contient K comme sous-corps dense. De plus $|\ \widehat{K}\ | = |\ K\ |$.*

1.2.6 Le corps des nombres p-adiques

Le complété de $\mathbb{Q}$ pour la valeur absolue usuelle $|\ .\ |_\infty$ est le corps $\mathbb{R}$ des nombres réels.

Le complété de $\mathbb{Q}$ pour la valeur absolue ultramétrique $|\ .\ |_p$ (ou p est nombre premier) est le corps $\mathbb{Q}_p$ des nombres p-adiques.

Soient p un nombre premier et $x = p^k \ \dfrac{n}{m}$ un rationnel non nul avec k, n, m dans $\mathbb{Z}$ et $pgcd(n, p) = pgcd(m, p) = 1$. La valeur absolue p-adique de x est $|\ x\ |_p = p^{-k}$. L'application v_p qui à $x \neq 0$ associe $v_p(x) = k$ est une valuation appelée la valuation p-adique de x (on peut le vérifier directement ou prendre $\lambda = -\dfrac{1}{\log p}$ dans la remarque 1.4). Donc $|\ x\ |_p = p^{-v_p(x)}$.

La valuation de $\mathbb{Q}_p$ qui prolonge la valuation p-adique de $\mathbb{Q}$ est telle que pour tout x dans $\mathbb{Q}_p^*$, $v_p(x) = -\log_p |x|_p \in \mathbb{Z}$ et $| x |_p = p^{-v_p(x)}$ ($\log_p$ est le logarithme en base p).

Développement de Hensel

Etant donné un nombre premier p, tout entier naturel n possède un développement en base p de la forme $n = n_0 + n_1 p + \cdots + n_m p^m$, où les $0 \leq n_i \leq p-1$. Dans le cas de $\mathbb{Q}_p$, tout nombre p-adique admet un développement infini en puissances de p donné par le théorème suivant :

Théorème 1.6. *(Développement de Hensel)*
Tout élément $a \in \mathbb{Q}_p$ admet un développement unique sous-forme de série convergente dans $\mathbb{Q}_p$,

$$a = \sum_{n \geq n_0} a_n \, p^n,$$

où $n_0 \in \mathbb{Z}$ et les a_n sont dans $\mathbb{N}$ tels que $0 \leq a_n \leq p-1$ pour tout $n \geq n_0$.

La valuation du nombre p-adique a ci-dessus est

$$v_p(a) = \inf\{n \in \mathbb{Z} \ / \ a_n \neq 0\},$$

elle vaut donc n_0 si $a_{n_0} \neq 0$. Sa valeur absolue est $| a |_p = p^{-v_p(a)}$.

Cette valuation est une valuation discrète normalisée sur $\mathbb{Q}_p$ d'uniformisante p.

L'anneau des entiers de $\mathbb{Q}_p$ noté $\mathbb{Z}_p$ est d'après ce qui précède

$$\mathbb{Z}_p = \{a \in \mathbb{Q}_p \ / \ | a |_p \leq 1\} = \{a \in \mathbb{Q}_p \ / \ v_p(a) \geq 0\} = \left\{ \sum_{n \geq 0} a_n \, p^n \ / \ 0 \leq a_n \leq p-1 \right\}.$$

$\mathbb{Z}_p$ est un anneau local, principal, d'idéal maximal

$$p\mathbb{Z}_p = \{a \in \mathbb{Q}_p \ / \ | a |_p < 1\} = \{a \in \mathbb{Q}_p \ / \ v_p(a) > 0\} = \left\{ \sum_{n \geq 1} a_n \, p^n \ / \ 0 \leq a_n \leq p-1 \right\}.$$

et les idéaux de $\mathbb{Z}_p$ sont $\{0\}$ et les $p^k \, \mathbb{Z}_p$ avec k dans $\mathbb{N}$.

Tout élément $x \in \mathbb{Q}_p$ s'écrit de manière unique $x = p^k \, u$ où $k \in \mathbb{Z}$ et $u \in \mathcal{U}$.

Le groupe des unités de $\mathbb{Z}_p$ est

$$\mathcal{U}_p = \{a \in \mathbb{Q}_p \ / \ | a |_p = 1\} = \{a \in \mathbb{Q}_p \ / \ v_p(a) = 0\} = \left\{ \sum_{n \geq 0} a_n \, p^n \ / \ 0 \leq a_n \leq p-1 \text{ et } a_0 \neq 0 \right\}.$$

Le corps résiduel $\dfrac{\mathbb{Z}_p}{p\mathbb{Z}_p}$ est isomorphe à $\mathbb{F}_p$ (le corps fini à p éléments).

De manière générale, si K est un corps valué ultramétrique et $\widehat{K}$ son complété alors K et $\widehat{K}$ ont même corps résiduel.

Notons que la suite $(x_n)_n$ définie par $x_n = \sum_{k=0}^{n} p^{2^k}$ où p est un nombre premier, est une suite de Cauchy de $(\mathbb{Q}, |\ .\ |_p)$ car $|\ x_n - x_{n+1}\ |_p = |\ p^{2^{n+1}}\ |_p = \dfrac{1}{p^{2^{n+1}}}$ tend vers zéro quand n tend vers l'infini. Cette suite est convergente dans $\mathbb{Q}_p$ vers le nombre p-adique $\sum_{n\geq 0} p^{2^n}$ qui n'est pas dans $\mathbb{Q}$. La suite $(x_n)_n$ est un exemple d'une suite de Cauchy non convergente dans $(\mathbb{Q}, |\ .\ |_p)$.

Il faut savoir qu'un nombre p-adique est rationnel si et seulement si son développement de Hensel est périodique à partir d'un certain rang, ce qui n'est pas le cas du nombre p-adique $\sum_{n\geq 0} p^{2^n}$.

Remarque 1.7. *Le développement de Hensel reste vrai dans le cas de tout corps valué ultramétrique K de valuation discrète normalisée v dont π est une uniformisante.*

Soit A l'anneau de entiers de K d'idéal maximal πA et $\mathcal{U}$ le groupe des unités de A. Soit S un système de représentants des éléments du corps résiduel $\dfrac{A}{\pi A}$ contenant zéro. Alors tout élément $a \in K$ s'écrit de façon unique sous-forme d'une série convergente

$$a = \sum_{n\geq n_0} a_n\ \pi^n,$$

où les a_n sont dans S pour tout $n \geq n_0$ et $n_0 \in \mathbb{Z}$.

Tout élément x de K s'écrit $x = \pi^n\ u$ avec $n \in \mathbb{Z}$ et $u \in \mathcal{U}$.

1.2.7 Extensions algébriques

Soit K un corps muni d'une valeur absolue $|\ .\ |$ et L une extension finie de K. La norme d'un élément α de L noté $N_{L|K}(\alpha)$ est le déterminant de l'endomorphisme φ_α du K-espace vectoriel L défini par $\varphi_\alpha(x) = \alpha x$.

Si $P(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0 \in K[X]$ désigne le polynôme minimal de α sur K alors

$$N_{L|K}(\alpha) = ((-1)^m\ a_0)^{[L:K(\alpha)]},$$

où $[L : K(\alpha)]$ est le degré de l'extension L de $K(\alpha)$.

Dans le cas où $L = K(\alpha)$, on a $N_{L|K}(\alpha) = (-1)^m\ a_0$.

Théorème 1.8. *Soit $(K, |\ .\ |)$ un corps valué ultramétrique complet.*

Toute extension finie L de K possède une unique valeur absolue qui prolonge celle de K que l'on note encore $|\ .\ |$.

De plus, si $P(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0 \in K[X]$ est le polynôme minimal de $x \in L$ et $n = [L : K]$ alors

$$|\ x\ | = |\ N_{L|K}(x)\ |^{\frac{1}{n}} = |\ P(0)\ |^{\frac{1}{m}} = |\ a_0\ |^{\frac{1}{m}}\ .$$

En termes de valuation, on écrira $v(x) = \dfrac{1}{[L : K]}\, v(N_{L|K}(x)) = \frac{1}{m}\, v(P(0)) = \frac{1}{m}\, v(a_0)$.

La proposition suivante nous donne une information sur le polynôme minimal des éléments de l'anneau des entiers de l'extension L du théorème précédent ainsi qu'une indication sur le corps résiduel de L par rapport à celui de K.

Proposition 1.9. *Soit $(K, |\ .\ |)$ un corps valué ultramétrique complet.*

Soient L une extension finie de K et $|\ .\ |$ l'unique valeur absolue de L prolongeant celle de K. Soient $A(L) = \{x \in L\ /\ |\ x\ | \leq 1\}$ l'anneau des entiers de L et $\mathfrak{M}(L) = \{x \in L\ /\ |\ x\ | < 1\}$ l'unique idéal maximal de $A(L)$.

Alors $A(L)$ est l'ensemble des éléments x de L dont le polynôme minimal $P(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_0 \in A[X]$ où A est l'anneau des entiers de K.

Le corps résiduel $\dfrac{A(L)}{\mathfrak{M}(L)}$ de L est une extension finie du corps résiduel $\dfrac{A}{\mathfrak{M}}$ de K de degré inférieur ou égal à $[L : K]$.

Rappelons enfin le résultat suivant :

Proposition 1.10. *Soit p un nombre premier.*

Toute extension finie du corps des nombres p-adiques $\mathbb{Q}_p$ est de valuation discrète.

Considérons une extension finie K de $\mathbb{Q}_p$ de corps résiduel k et $|\ .\ |_p$ (resp. v_p) l'unique valeur absolue (resp. valuation) de K prolongeant la valeur absolue $|\ .\ |_p$ (resp. valuation v_p) p-adique de $\mathbb{Q}_p$. D'après la proposition 1.10, K est un corps de valuation discrète. Soit π une uniformisante.

Il vient de la proposition 1.9 que k est une extension finie du corps résiduel $\mathbb{F}_p$ de $\mathbb{Q}_p$. Donc $k = \mathbb{F}_q$ (corps à q éléments) où $q = p^f$. L'entier f est égal à

$$f = [k : \mathbb{F}_p] = \dim_{\ \mathbb{F}_p} k$$

et s'appelle le degré résiduel de l'extension $K \mid \mathbb{Q}_p$.

Tout élément $a \in K$ s'écrit de manière unique

$$a = \pi^m \, b \quad \text{avec } m \in \mathbb{Z} \text{ et } \mid b \mid_p = 1 \text{ (ou } v_p(b) = 0).$$

En particulier $p = \pi^e \, b$ avec $e \in \mathbb{Z}$ et $\mid b \mid_p = 1$. Par suite $\mid p \mid = \mid p \mid_p = \dfrac{1}{p} = \mid \pi \mid^e$ ou encore $v(p) = v_p(p) = 1 = e \; v(\pi)$, d'où $\mid \pi \mid = p^{-\frac{1}{e}}$ ou encore $v(\pi) = \dfrac{1}{e}$. On déduit que $e \in \mathbb{N}^*$ et $v(K^*) = \dfrac{1}{e}\,\mathbb{Z}$. L'entier naturel e s'appelle l'indice de ramification de l'extension K de $\mathbb{Q}_p$. Il est égal à l'indice du sous-groupe $v(\mathbb{Q}_p^*)$ dans le sous-groupe $v(K^*)$ du groupe additif $\mathbb{R}$ (c'est aussi l'indice du sous-groupe $\mid \mathbb{Q}_p^* \mid$ dans le sous-groupe $\mid K^* \mid$ du groupe multiplicatif $\mathbb{R}^*$).

On montre que si l'extension finie $K \mid \mathbb{Q}_p$ est de degré n alors $n = e \; f$.

1.3 Loi de réciprocité quadratique, symbole de Legendre

L'introduction du symbole de Legendre obéit à notre besoin d'utilisation de cet outil, dans le chapitre suivant, pour nous permettre de déduire l'irréductibilité de certains polynômes.

Le symbole de Legendre indique dans quels cas un entier est un résidu quadratique modulo un nombre premier p donné. Il a été introduit par le mathématicien francais Adrien-Marie Legendre $(1752 - 1833)$ au cours de ses efforts pour démontrer la loi de réciprocité quadratique conjecturée par le mathématicien suisse Leonhard Euler $(1707 - 1783)$. A l'origine la loi de réciprocité quadratique s'énonçait autrement, c'est à Legendre qu'on doit sa formulation actuelle.

Les définitions et résultats énoncés dans cette section sont tirés de l'ouvrage de Pierre Samuel [71] "Théorie algébrique des nombre" et de celui de Jean-Pierre Serre [72] "Cours d'arithmétique". Le lecteur y trouvera toutes les preuves.

Résidu quadratique

Soit p un nombre premier. Un élément $a \in \mathbb{Z} \setminus p\mathbb{Z}$ est un carré modulo p ou un résidu quadratique modulo p s'il existe $b \in \mathbb{Z} \setminus p\mathbb{Z}$ tel que $a \equiv b^2 \bmod p$. Il revient au même de dire que $\bar{a} = \bar{b}^2$ dans le groupe $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$.

Le cas $p = 2$ étant trivial, on suposera dans toute cette section que p est impair.

L'application de $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ dans $\{-1, 1\}$ qui à x associe 1 si x est un résidu quadratique modulo p et -1 sinon est un morphisme de groupes multiplicatifs.

Grâce au premier théorème d'isomorphime, son noyau est un sous-groupe d'indice 2 de $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$. On déduit que le nombre de carrés dans $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ est $\frac{p-1}{2}$.

Par exemple, $\text{Card}(\{\text{résidus quadratiques modulo } 11\}) = \text{Card}(\{1,3,4,5,9\}) = 5$.

Il convient de noter que le produit de deux éléments x, y de $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ est un carré si et seulement si, soit x et y sont tous deux des carrés, soit x et y ne sont pas des carrés.

Symbole de Legendre

Soient p un nombre premier et a dans $\mathbb{Z}$. Le symbole de Legendre $\left(\frac{a}{p}\right)$ est défini par :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \mid a. \\ 1 & \text{si } p \nmid a \text{ et } a \text{ résidu quadratique modulo } p. \\ -1 & \text{si } p \nmid a \text{ et } a \text{ non résidu quadratique modulo } p. \end{cases}$$

Les propriétés suivantes se déduisent immédiatement de la définition.
Pour tous a, b dans $\mathbb{Z}$:

- $\left(\frac{a}{p}\right) = \left(\frac{a \bmod p}{p}\right)$,
- $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$,
- $\left(\frac{a^2}{p}\right) = 1$ pourvu que $p \nmid a$.

Critère d'Euler

Théorème 1.11. *Soit p un nombre premier impair. on a :*

$$\forall a \in \mathbb{Z}, \quad \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p.$$

Par exemple : $\left(\frac{-1}{13}\right) = 1$, $\left(\frac{-1}{19}\right) = -1$ et pour tout nombre premier impair p on a

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

$$= \begin{cases} 1 & \text{si } p \equiv 1 \bmod 4, \\ -1 & \text{sinon.} \end{cases}$$

Loi de réciprocité quadratique

Le résultat fondamental qui suit, appelé loi de réciprocité quadratique, à été conjecturé indépendamment par Euler, Legendre et Gauss. Il a été démontré par Legendre dans certains cas et complétement démontré par Gauss en 1801 dans ses Disquisitiones Arithmeticae.

Théorème 1.12. *Soient p et q deux nombres premiers impairs, on a*

$$\left(\frac{p}{q}\right)\ \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\ \frac{q-1}{2}}.$$

En d'autres termes

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \ \Leftrightarrow\ p \equiv 1 \bmod 4 \text{ ou } q \equiv 1 \bmod 4.$$

Le résultat concernant le cas $\left(\frac{2}{p}\right)$, qui n'est pas prévu par la loi de réciprocité quadratique, porte le nom de loi complémentaire et est donné par la proposition suivante :

Proposition 1.13. *Soit p un nombre premier impair. On a*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

En d'autres termes, 2 est un résidu quadratique modulo p si et seulement si $p \equiv \pm 1 \bmod 8$.

Quelques exemples

Soit p un nombre premier impair. On a :

- 3 est un résidu quadratique modulo p si et seulement si $p = 3$ ou $p \equiv \pm 1 \bmod 12$.
- 5 est un résidu quadratique modulo p si et seulement si $p = 5$ ou $p \equiv \pm 1 \bmod 5$.
- 7 est un résidu quadratique modulo p si et seulement si $p = 7$ ou $p \equiv \pm 1,\ \pm 3,\ \pm 9 \bmod 28$.

Chapitre 2

Congruences dans les décimations de suites récurrentes linéaires

L'objet de ce chapitre est l'étude de congruences dans les suites récurrentes. De manière plus précise, il s'agit, étant donné un nombre premier p et une suite récurrente linéaires $(u_n)_n$ vérifiant, pour tout entier n, la relation $u_{n+h} = a_{h-1}u_{n+(h-1)} + \cdots + a_1u_{n+1} + a_0u_n$, de déterminer les entiers naturels d pour lesquels $u_{n+hd} \equiv a_{h-1}u_{n+(h-1)d} + \cdots + a_1u_{n+d} + a_0u_n \bmod p$.

2.1 Introduction

Soit $u = (u_n)_{n\geq 0}$ une suite récurrente linéaire d'ordre $h \in \mathbb{N}^*$ à valeurs dans un corps commutatif K, qu'on suppose de caractéristique nulle, définie par la donnée de ses h premiers termes et par la relation de récurrence

$$u_{n+h} = a_{h-1}u_{n+(h-1)} + \cdots + a_1u_{n+1} + a_0u_n$$

où les coefficients a_i $(0 \leq i \leq h-1)$ sont dans K avec $a_0 \neq 0$ et de polynôme caractéristique

$$f(X) = X^h - a_{h-1}X^{h-1} - \cdots - a_1X - a_0.$$

Nous allons nous intéresser, dans ce chapitre, aux suites d-extraites de la suite u et plus précisément à leur polynôme caractéristique f_d. Ce sont les sous-suites $u^{(0)}, u^{(1)}, \ldots, u^{(d-1)}$ de u définies, pour tout entier non nul d et tout entier n, par $u_n^{(j)} = u_{dn+j}$ appelées aussi suites d-décimées de la suite u.

Lorsque le polynôme f se factorise, dans une extention convenable de K, de la manière suivante

$$f(X) = \prod_{i=1}^{s}(X - \alpha_i)^{m_i}, \tag{2.1}$$

alors les suites d-extraites $u^{(j)}$, qui sont aussi des suites récurrentes linéaires, ont

$$f_d(X) = \prod_{i=1}^{s}(X - \alpha_i^d)^{m_i} \tag{2.2}$$

pour polynôme caractéristique.

Le problème que nous cherchons à résoudre peut être formulé de la manière suivante : en considérant un polynôme unitaire f à coefficients dans $\mathbb{Z}$, à quelles conditions sur d, a-t-on $f_d = f$ (resp. $f_d = f$ modulo un idéal de $\mathbb{Z}$) ?

Notons d'emblée le résultat suivant :

Proposition 2.1. *Soit f un polynôme unitaire à coefficients dans $\mathbb{Z}$ tel que $f(0) \neq 0$. Les assertions suivantes sont équivalentes :*

1. *Il existe d dans $\mathbb{N}^*$ tel que $f_d = f$.*
2. *Les racines de f sont des racines de l'unité.*

Preuve.

L'implication (1) $\Rightarrow$ (2) s'obtient en remarquant que si α est racine de f alors α^d l'est aussi (puisque α^d est par définition racine de f_d et $f_d = f$). Par conséquent α^{d^2}, $\alpha^{d^3}, \ldots$ sont des racines de f. Comme il y'a un nombre fini de racines, il existe alors s, t dans $\mathbb{N}$ avec $s < t$ tels que $\alpha^{d^t} = \alpha^{d^s}$ et donc $\alpha^{d^t - d^s} = 1$.

Réciproquement, si les racines de f sont des racines de l'unité alors il existe un entier naturel m (le ppcm des ordres des racines de f) tel que pour tout α racine de f, $\alpha^m = 1$. En posant $d = m + 1$ et en désignant par R l'ensemble des racines distinctes de f nous avons alors

$$\begin{aligned} f_d(X) &= \prod_{\alpha \in R} (X - \alpha^d)^{m_i} \\ &= \prod_{\alpha \in R} (X - \alpha^{m+1})^{m_i} \\ &= \prod_{\alpha \in R} (X - \alpha)^{m_i} \\ &= f(X). \end{aligned}$$

□

On sait donc que modulo un nombre premier p, un tel d existe. Il s'agit ensuite de le décrire en fonction de p.

Pour comprendre les motivations de ce travail, rappelons quelques résultats dûs à H.T. Freitag, G.M. Phillips et L. Somer qui, dans les années quatre-vingts, partant d'une suite récurrente linéaire de la forme $u_{n+h} = a_{h-1}u_{n+(h-1)} + \cdots + a_1 u_{n+1} + a_0 u_n$, ce sont intéressés au problème de la détermination des entiers d et m pour lesquels

$$u_{n+hd} \equiv a_{h-1}u_{n+(h-1)d} + \cdots + a_1 u_{n+d} + a_0 u_n \bmod m.$$

Dans [32], H.T. Freitag à montré le théorème suivant

Théorème 2.2. *Si (F_n) désigne la suite de Fibonacci alors, pour tout n dans $\mathbb{N}$,*

$$F_{n+2d} \equiv F_{n+d} + F_n \bmod 10$$

si et seulement si $d \equiv 1$ ou $5 \bmod 12$.

H. T. Freitag, G. M. Fillips ont démontré, respectivement dans [33] et [34], les théorème 2.3 et théorème 2.4 suivants

Théorème 2.3. *Soit (u_n) une suite récurrente d'entiers à coefficients dans $\mathbb{Z}$ d'ordre 2 définie par*

$$u_{n+2} = au_{n+1} + bu_n,$$

alors pour tout p premier ≥ 3 et tout entier n

$$u_{n+2p} \equiv au_{n+p} + bu_n \bmod 2p.$$

Théorème 2.4. *Soit (u_n) une suite récurrente linéaire d'entiers d'ordre h définie par*

$$u_{n+h} = a_{h-1}u_{n+(h-1)} + \cdots + a_1u_{n+1} + a_0u_n, \qquad \text{avec } a_i \in \mathbb{Z},$$

alors, pour tout nombre premier p et tout n dans $\mathbb{N}$,

$$u_{n+hp} \equiv a_{h-1}u_{n+(h-1)p} + \cdots + a_1u_{n+p} + a_0u_n \bmod p.$$

Ce théorème a été généralisé par L. Somer dans [74] en prouvant que

Théorème 2.5. *Soit (u_n) une suite récurrente linéaire d'entiers d'ordre h définie par*

$$u_{n+h} = a_{h-1}u_{n+(h-1)} + \cdots + a_1u_{n+1} + a_0u_n, \qquad \text{avec } a_i \in \mathbb{Z},$$

alors, pour tout nombre premier p et pour tout entier non nul b, on a

$$u_{n+hp^b} \equiv a_{h-1}u_{n+(h-1)p^b} + \cdots + a_1u_{n+p^b} + a_0u_n \bmod p.$$

Il a montré aussi dans le même article que

Théorème 2.6. *Soit (u_n) une suite récurrente linéaire d'entiers d'ordre h définie par*

$$u_{n+h} = a_{h-1}u_{n+(h-1)} + \cdots + a_1u_{n+1} + a_0u_n, \qquad \text{avec } a_i \in \mathbb{Z}.$$

Soit p un nombre premier ne divisant par a_0 et soit $b \in \mathbb{N}^*$. Alors il existe un entier g tel que pour tout $d \equiv p^b \bmod g$

$$u_{n+hd} \equiv a_{h-1}u_{n+(h-1)d} + \cdots + a_1u_{n+d} + a_0u_n \bmod p.$$

Toutes ces conguences s'expriment naturellement, comme nous allons le voir sur l'exemple particulier de la suite de Fibonacci, en termes de congruences entre polynômes sous la forme $f_d(X) \equiv f(X) \bmod p$ où f est le polynôme caractéristique $f(X) = X^h - a_{h-1}X^{h-1} - \cdots - a_0$ de la suite récurrente linéaire u d'ordre h vérifiant $u_{n+h} = a_{h-1}u_{n+(h-1)} + \cdots + a_1u_{n+1} + a_0u_n$ et f_d le polynôme défini par l'équation (2.1) qui est un polynôme caractéristique des suites d-extraites de la suite u.

Précisons que $f_d(X) \equiv f(X) \bmod p$ signifie que les coefficients des deux polynômes sont congrus deux à deux modulo p.

Soit donc $(F_n)_n$ la suite de Fibonacci. Supposons qu'il existe un entier d tel que pour tout entier n,

$$F_{n+2d} \equiv F_{n+d} + F_n \bmod 10.$$

Soit $(F_n^{(j)})_n$ la j-ème suite d-extraite de la suite $(F_n)_n$. Nous avons

$$F_n^{(j)} = F_{dn+j}, \qquad F_{n+1}^{(j)} = F_{dn+j+d} \text{ et } F_{n+2}^{(j)} = F_{dn+j+2d}$$

Par suite, en posant $dn + j = m$,

$$F_{m+2}^{(j)} \equiv F_{m+1}^{(j)} + F_m^{(j)} \bmod 10$$

Ce qui signifie que, modulo 10, le polynôme caractéristique f_d de la suite $(F_n^{(j)})_n$ est égal à f.

C'est à dire

$$f_d(X) \equiv f(X) \bmod 10.$$

Réciproquement si $f_d(X) \equiv f(X) \bmod 10$ alors pour tout n,

$$F_{n+2}^{(j)} \equiv F_{n+1}^{(j)} + F_n^{(j)} \bmod 10.$$

Par suite

$$F_{dn+2d+j} \equiv F_{dn+d+j} + F_{dn+j} \bmod 10.$$

En posant encore $m = dn + j$, nous obtenons pour tout m

$$F_{m+2d} = F_{m+d} + F_m \bmod 10$$

Ce qui montre que la congruence $F_{n+2d} \equiv F_{n+d} + F_n \bmod 10$ est équivalente à

$$f_d(X) \equiv f(X) \bmod 10.$$

2.2 Résultats généraux

Les résultats que nous allons énoncer dans ce paragraphe sont une version, en termes de polynômes, de ceux que nous avons donnés dans l'introduction et qui se trouvent dans [74]. Ce sont des résultats généraux valables pour tout polynôme unitaire f à coefficients entiers. Ils indiquent que, sous certaines conditions sur l'entier naturel d, la congruence $f_d \equiv f \bmod p$ est réalisée (p étant un nombre premier donné). Nous verrons sur les exemples particuliers que nous avons choisis d'étudier que ces conditions sont nécessaires mais loin d'être suffisantes.

2.2.1 Cadre de travail

Commençons par définir le cadre dans lequel nous allons nous placer pour établir les preuves des résultats qui vont suivre.

Considérons f un polynôme unitaire à coefficients dans $\mathbb{Z}$, p un nombre premier, $\mathbb{K}$ le corps de décomposition de f sur le corps $\mathbb{Q}_p$ des nombres p-adiques. $\mathbb{K}$ est une extension finie de $\mathbb{Q}_p$ de degré $n = e\ t$ où e est l'indice de ramification de l'extension et t son degré résiduel. Désignons par v le prolongement de la valuation discrète p-adique de $\mathbb{Q}_p$ à $\mathbb{K}$, $\mathbb{A}$ l'anneau de valuation de $\mathbb{K}$ formé par les x de $\mathbb{K}$ de valuation ≥ 0. $\mathbb{A}$ est un anneau local d'idéal maximal $\mathfrak{M} = \pi A$ où π est une uniformisante de v. Les éléments de $\mathfrak{M}$ sont les x de valuation > 0. Le goupe des unités de $\mathbb{A}$ est $\mathcal{U}(\mathbb{A})$ dont les éléments sont de valuation nulle. Notons enfin, par $k = \dfrac{\mathbb{A}}{\mathfrak{M}}$ le corps résiduel de $\mathbb{K}$ qui est isomorphe au corps fini $\mathbb{F}_{p^t}$.

2.2.2 Quelques lemmes

Les lemmes suivants nous sont utiles pour démontrer les théorèmes que nous allons énoncer plus loin.

Lemme 2.7. *Soient $a \in \mathbb{Z}$ et $m \in \mathbb{N}$. On a*

$$a \equiv 0 \mod \pi^{me+1} \Rightarrow a \equiv 0 \mod p^{m+1}.$$

En particulier, si $a \in \pi\mathbb{A}$ alors $a \in p\mathbb{Z}$.

Preuve. Soient $m \in \mathbb{N}$ et $a \in \mathbb{Z}$ tels que $a \equiv 0 \mod \pi^{me+1}$ alors $a = \pi^{me+1}x$ avec $x \in \mathbb{A}$. Comme $p = \pi^e u$ avec $v(u) = 0$ alors $a = p^m u^{-m} y$ avec $y = \pi x \in \mathfrak{M}$. Par suite $v(a) > m$. Il en résulte que $v(a) \geq m + 1$ et donc $a = p^{m+1}b$ avec $b \in \mathbb{Z}$ d'où $a \equiv 0 \mod p^{m+1}$.

□

Lemme 2.8. *Soient $\alpha \in \mathbb{A}$ et $s \in \mathbb{N}$. On suppose que $p \geq e + 1$. Alors*

$$\alpha \equiv 1 \mod \pi \Rightarrow \alpha^{p^s} \equiv 1 \mod \pi^{se+1}$$

.

En particulier, si l'extention $\mathbb{K}$ est totalement ramifiée i.e. $e = 1$ alors le Lemme 2.8 est vrai pour tout nombre premier p.

Preuve. La preuve du lemme se fait par récurrence sur s.

Pour $s = 0$ évident.

Pour $s = 1$, posons $\alpha = 1 + \pi a$ avec $a \in \mathbb{A}$. Par la formule du binôme

$$\alpha^p = 1 + \sum_{i=1}^{p} \binom{p}{i} \pi^i a^i.$$

Or pour tout $1 \leq i \leq p-1$, le coefficient binomial $\binom{p}{i}$ est divisible par p. Il peut donc s'écrire $\pi^e a_i$ avec $a_i \in \mathbb{A}$.

Nous avons alors

$$\alpha^p = 1 + \pi^p a^p + \pi^e \sum_{i=1}^{p-1} \pi^i b_i,$$

où $b_i = a_i \ a^i \ \in \mathbb{A}$.

En posant $b = \pi^{p-(e+1)} a^p + \sum_{i=1}^{p-1} \pi^{i-1} b_i$, nous obtenons

$$\alpha^p = 1 + \pi^{e+1} b.$$

Supposons la propriété vraie à l'ordre s et posons $\alpha^{p^s} = 1 + \pi^{se+1} a$ avec $a \in \mathbb{A}$. Nous avons

$$\alpha^{p^{s+1}} = (1 + \pi^{se+1} a)^p.$$

Comme nous l'avons fait plus haut, par la formule du binôme

$$\alpha^{p^{s+1}} = 1 + \sum_{i=1}^{p-1} \binom{p}{i} \pi^{(se+1)} a^i + \pi^{(se+1)p} a^p = 1 + \pi^{(s+1)e+1} b,$$

avec $b \in \mathbb{A}$. Par suite

$$\alpha^{p^{s+1}} \equiv 1 \bmod \pi^{(s+1)e+1}.$$

□

2.2.3 Quelques théorèmes

Les résultats qui suivent décrivent certaines situations où, étant donné un polynôme unitaire f à coefficients dans $\mathbb{Z}$, la congruence $f_d(X) \equiv f(X) \bmod p$ est réalisée.

Théorème 2.9. *Soient p un nombre premier et f un polynôme unitaire à coefficients dans $\mathbb{Z}$. Pour tout $b \in \mathbb{N}^*$, $f_{p^b}(X) \equiv f(X) \mod p$.*

Preuve. Soit h le degré de f et soient α_i $(1 \leq i \leq h)$ les racines de f comptées avec leur multiplicité dans une cloture algébrique $\overline{\mathbb{F}}_p$ de $\mathbb{F}_p$.

Nous avons dans $\overline{\mathbb{F}}_p[X]$

$$f(X) = \prod_{i=1}^{h}(X - \alpha_i).$$

Pour $d = p^b$ avec $b \in \mathbb{N}$,

$$f_d(X) = \prod_{i=1}^{h}(X - {\alpha_i}^d) = \prod_{i=1}^{h}(X - F_r^b(\alpha_i)),$$

F_r étant le frobenius qui est le $\mathbb{F}_p$-automorphisme de $\overline{\mathbb{F}}_p$ qui à x associe x^p et qui permute les racines α_i de f.

Il s'ensuit que $f_d(X) = f(X)$ sur $\overline{\mathbb{F}}_p$ et donc sur $\mathbb{F}_p$.

□

Théorème 2.10. *Soient $b \in \mathbb{N}$, f un polynôme unitaire à coefficients dans $\mathbb{Z}$ avec $f(0) \neq 0$ et p un nombre premier $\geq e+1$ et ne divisant pas $f(0)$. Alors il existe un entier naturel non nul g tel que pour tout $d \equiv 1 \mod g$ on ait $f_d(X) \equiv f(X) \mod p^b$.*

Preuve. La condition p ne divise pas $f(0)$ signifie que les racines α_i de f sont des unités π-adiques. En effet, d'après le lemme 2.7, $f(0)$ n'est pas dans $\mathfrak{M}$ et donc $\prod_{i=1}^{h}\alpha_i = f(0)$ est inversible dans $\mathbb{A} = \mathcal{U}(\mathbb{A}) \cup \mathfrak{M}$. Par suite $\sum_{i=1}^{h} v(\alpha_i) = 0$. Or les α_i sont des entiers de $\mathbb{K}$ donc leur valuation est ≥ 0. Par conséquent $v(\alpha_i) = 0$ pour tous $1 \leq i \leq h$.

Dans le corps k, qui est un corps fini de cardinal p^t, nous avons $\overline{\alpha_i}^{p^t-1} = \overline{1}$. Autrement dit

$$\alpha_i^{p^t-1} \equiv 1 \mod \pi.$$

Nous déduisons du lemme 2.8 que

$$\alpha_i^{(p^t-1)p^b} \equiv 1 \mod \pi^{be+1}.$$

Soit $g = p^b(p^t - 1)$. Pour tout $k \in \mathbb{N}$

$$\alpha_i^{kg+1} \equiv \alpha_i \mod \pi^{be+1}.$$

Donc pour tout $d \equiv 1 \mod g$,

$$\alpha_i^d \equiv \alpha_i \mod \pi^{be+1}.$$

Comme f et f_d sont dans $\mathbb{Z}[X]$ et $p = \pi^e\, u$ avec u inversible alors

$$f_d(X) \equiv f(X) \mod p^b \qquad \text{(voir lemme 2.7).}$$

□

Comme conséquence des théorèmes 2.9 et 2.10 nous avons le résultat suivant

Corollaire 2.11. *Soient $f \in \mathbb{Z}[X]$ unitaire avec $f(0) \neq 0$ et p un nombre premier ne divisant pas $f(0)$, alors il existe $g \in \mathbb{N}^*$ tel que pour tout $b \in \mathbb{N}$ si $d \equiv p^b \mod g$ alors $f_d(X) \equiv f(X) \mod p$.*

Preuve.

D'après le théorème 2.10, $\alpha_i^{p^t-1} \equiv 1 \mod \pi$.

Soient $g = p^t - 1$ et $b, d, k \in \mathbb{N}$ tels que $d = kg + p^b$. Nous avons $d \equiv p^b \mod g$ et $\alpha_i^d \equiv \alpha_i^{p^b} \mod \pi$.

Comme f_d et f_{p^b} sont dans $\mathbb{Z}[X]$, d'après le lemme 2.7

$$f_d(X) \equiv f_{p^b}(X) \bmod p.$$

Par le théorème 2.9, $f_d(X) \equiv f(X) \mod p$.

□

Remarque 2.12. *Dans la suite de ce travail, nous nous retrouverons souvent dans la situation où l'indice de ramification de l'extension $\mathbb{K}$ de $\mathbb{Q}_p$ est égal à 1 (auquel cas $p = \pi\ u$ avec $u \in \mathcal{U}$). Alors si $a \in \mathbb{K}$ et $m \in \mathbb{Z}$, la congruence $a \equiv m \bmod \pi$ qui signifie que $a = m + \pi\mathbb{A}$, peut aussi s'écrire $a \equiv m \bmod p$; écriture qui se justifie par le fait que $m + \pi\mathbb{A} = m + p\mathbb{A}$.*

Remarque 2.13. *Nous déduisons de la démonstration du corollaire 2.11 que l'ordre d'une racine α du polynôme caractéristique $f(X) = X^2 - X - 1$ de la suite de Fibonacci est un diviseur de $p - 1$ où p est un nombre premier congru à ± 1 modulo 5. En effet le polynôme f est, dans ce cas, réductible sur $\mathbb{F}_p$, par suite $t = 1$ et donc modulo p, $\alpha^{p-1} = 1$.*

Ce résultat est connu, voir par exemple [77] et [38].

2.3 Résultats particuliers

Dans cette partie, nous allons donner une généralisation du théorème 2.2 de H.T. Freitag relatif à la suite de Fibonacci de polynôme caractéristique $f(X) = X^2 - X - 1$ et étudier aussi les cas des suites récurrentes linéaires d'ordre 2 de polynôme caractéristique de la forme $f(X) = X^2 + \epsilon_1 X + \epsilon_2$ avec ϵ_1 et ϵ_2 dans $\{-1, 1\}$. Nous terminerons par l'étude des suites récurrentes linéaires de polynôme caractéristique le polynôme cyclotomique
$f(X) = X^{q-1} + X^{q-2} + \cdots + X + 1$ et enfin les suites récurrentes de polynôme caractéristique $f(X) = X^{q-1} - X^{q-2} + \cdots - X + 1$ avec q premier impair.

Notre objectif étant de décrire complétement les entiers d pour lequels $f_d(X) \equiv f(X) \mod p$ où p est un nombre premier donné. Nous donnerons la forme de d selon les différentes valeurs de p.

Désignons par

$(u_n)_n$ la suite correspondant à $\epsilon_1 = -1$ et $\epsilon_2 = 1$,
$(v_n)_n$ la suite correspondant à $\epsilon_1 = \epsilon_2 = 1$,
$(F_n)_n$ la suite de Fibonacci correspondant à $\epsilon_1 = \epsilon_2 = -1$,
$(w_n)_n$ la suite correspondant à $\epsilon_1 = 1$ et $\epsilon_2 = -1$.

2.3.1 Suites de polynôme caractéristique $f(X) = X^2 - X + 1$

Pour la suite $(u_n)_n$ nous avons obtenu le résultat suivant, indépendamment du choix de ces deux premiers termes.

Théorème 2.14. *Soient $d \in \mathbb{N}^*$, p un nombre premier et $f(X) = X^2 - X + 1$. Alors*

$$f_d(X) \equiv f(X) \bmod p \Leftrightarrow d = \begin{cases} 3n \pm 1 & \text{si } p = 2, \\ 2n + 1 & \text{si } p = 3, \\ \dfrac{6n + 3 - (-1)^n}{2} & \text{si } p \neq 2 \text{ et } p \neq 3. \end{cases}$$

où $n \in \mathbb{N}$.

Preuve. Soit p un nombre premier et soient α, β les racines de f sur $\mathbb{Q}_p$.

Dans $\mathbb{F}_2[X]$ (ie pour $p = 2$), le polynôme f est irréductible. Il s'ensuit que le degré résiduel de l'extension $\mathbb{K} = \mathbb{Q}_2(\alpha)$ sur $\mathbb{Q}_2$ est $t = 2$. On sait, du corollaire 2.11, que si $d \equiv 2^b \mod 3$ alors $f_d(X) \equiv f(X) \mod 2$ pour tout b dans $\mathbb{N}^*$.

Or $2^b \equiv 1$ ou $2 \mod 3$, donc si $d \equiv 1$ ou $2 \mod 3$ alors $f_d(X) \equiv f(X) \mod 2$.

Réciproquement, la congruence $f_d(X) \equiv f(X) \mod 2$ équivaut au système

$$\begin{cases} \alpha^d + \beta^d \equiv \alpha + \beta \bmod 2, \\ \alpha^d \ \beta^d \equiv \alpha\beta \bmod 2. \end{cases}$$

En remarquant que $X^3+1=(X+1)(X^2-X+1)$, alors $\alpha^3=-1$. Par suite $\alpha^3\equiv 1 \mod 2$. Comme $\alpha+\beta=\alpha\beta=1$ alors en écrivant $d=3n+r$, nous déduisons que $r=1$ ou $r=2$.

Nous aurions pu déduire que $\alpha^3\equiv 1 \mod 2$ de la preuve du théorème 2.10, puisqu'il y est établi que $\alpha^{p^t-1}\equiv 1 \bmod \pi$ avec, dans notre cas, $t=2$, $e=1$ et $p=2=\pi^e\ u=\pi\ u$ où $u\in\mathcal{U}$.

Modulo 3, $f(X)=(X-2)^2$. Comme $2^2\equiv 1 \bmod 3$ alors en écrivant $d=2n+r$, nous avons

$$f_d(X)\equiv f(X) \bmod 3 \ \Leftrightarrow\ 2^r\equiv 2 \bmod 3 \ \Leftrightarrow\ r=1.$$

Supposons, maintenant, que $p>3$, la condition $d=\dfrac{6n+3-(-1)^n}{2}$ équivaut à $d\equiv 1$ ou $5 \mod 6$.

Nous avons $\alpha^6=\beta^6=1$, $\alpha^{-1}=1-\alpha$ et $\beta^{-1}=1-\beta$.
Par suite
si $d\equiv 1 \mod 6$ alors $\alpha^d+\beta^d=\alpha+\beta$
si $d\equiv 5 \mod 6$ alors $\alpha^d+\beta^d=\alpha^5+\beta^5=\alpha^{-1}+\beta^{-1}=\alpha+\beta$.
Dans ces deux cas $f_d(X)\equiv f(X) \mod p$.

Réciproquement,
si $d\equiv 0 \mod 6$ alors $\alpha^d+\beta^d=2$,
si $d\equiv 1$ ou $4 \mod 6$ alors $\alpha^d+\beta^d=-1$,
si $d\equiv 3 \mod 6$ alors $\alpha^d+\beta^d=-2$.
Dans chacun de ces cas $\alpha^d+\beta^d\not\equiv\alpha+\beta \bmod p$ donc $f_d(X)\not\equiv f(X) \bmod p$.

□

Remarque 2.15. *Pour p premier supérieur ou égal à 5, le polynôme f est irréductible sur $\mathbb{F}_p$ si et seulement si p n'est pas un résidu quadratique modulo 3, c'est à dire si et seulement si $p\equiv 2 \mod 3$. Par suite $t=2$.*

Le corollaire 2.11 affirme que si $d\equiv p^b \mod (p^2-1)$ c'est à dire si $d\equiv 1$ ou $p \mod (p^2-1)$ alors $f_d(X)\equiv f(X) \mod p$.

Notons que $d\equiv 1$ ou $p \mod (p^2-1)$ implique $d\equiv 1$ ou $5 \mod 6$ mais la réciproque est inéxacte. Donc le corollaire 2.11 est une conséquence du théorème 2.14.

Le théorème 2.14, comme nous pouvons le constater, nous fournit d'autres d en plus de ceux prévus par le corrolaire 2.11.

Par exemple pour $p=5$, d'après le corollaire 2.11

$$d\equiv 1 \text{ ou } 5 \bmod 24 \ \Rightarrow\ f_d(X)\equiv f(X) \bmod 5,$$

alors que d'après le théorème 2.14

$$f_d \equiv f \bmod 5 \;\Leftrightarrow\; d \equiv 1 \text{ ou } 5 \bmod 6.$$

Donc, d'après le théorème 2.14, les $d = 7, 11, 13, 17, 19, 31, 35, 37, 41, 45, \ldots$ *réalisent la congruence* $f_d(X) \equiv f(X) \bmod 5$ *mais ne sont pas prévus par le corollaire 2.11.*

Le cas réductible se présente lorsque $p \equiv 1 \mod 3$. *Dans ce cas* $t = 1$. *D'après le corollaire 2.11, si* $d \equiv p^b \mod (p-1)$ *(autrement dit, si* $d \equiv 1 \mod (p-1)$*) alors* $f_d(X) \equiv f(X) \mod p$.

Notons là aussi que la condition $d \equiv 1 \mod (p-1)$ *entraine* $d \equiv 1 \bmod 6$. *Ce qui permet de dire que le corollaire 2.11 est une conséquence du théorème 2.14.*

Mais cette condition ne fournit pas tous les d *du théorème 2.14.*

Par exemple pour $p = 13$, *d'après le corollaire*

$$d \equiv 1 \bmod 12 \;\Rightarrow\; f_d(X) \equiv f(X) \bmod 13$$

tandis que le théorème 2.14 énonce que

$$f_d \equiv f \bmod 13 \;\Leftrightarrow\; d \equiv 1 \text{ ou } 5 \bmod 6.$$

Donc les $d = 7, 11, 17, 19, 23, 29, \ldots$ *réalisent la congruence* $f_d(X) \equiv f(X) \bmod 13$ *mais ne sont pas comptabilisés par le corollaire.*

Remarque 2.16. *Nous allons donner, dans cette remarque, la traduction du résultat précédent sur les termes de la suite* $(u_n)_n$.

Soient $d \in \mathbb{N}^*$, p *un nombre premier et* $(u_n)_n$ *la suite définie par* $u_{n+2} = u_{n+1} - u_n$ *alors pour tout* n

$$u_{n+2d} \equiv u_{n+d} - u_n \bmod p \Leftrightarrow d \equiv \begin{cases} \pm 1 \bmod 3 & \text{si } p = 2, \\ 1 \bmod 2 & \text{si } p = 3, \\ \pm 1 \bmod 6 & \text{si } p \neq 2 \text{ et } p \neq 3. \end{cases}$$

2.3.2 Suites de polynôme caractéristique $f(X) = X^2 + X + 1$

Comme nous le verrons plus loin, le résultat concernant cette suite $(v_n)_n$ se généralise à tout polynôme cyclotomique d'ordre premier impair.

Théorème 2.17. *Soient* $d \in \mathbb{N}^*$, p *un nombre premier et* $f(X) = X^2 + X + 1$.

1. *Si* $p = 3$ *alors* $\forall d \in \mathbb{N}^*, \quad f_d(X) \equiv f(X) \mod 3$.
2. *Si* $p \neq 3$, *alors* $f_d(X) \equiv f(X) \mod p$ *si et seulement si* d *n'est pas multiple de* 3.

Preuve. Les racines α et β de f vérifient $\alpha+\beta=-1$, $\alpha\beta=1$ et $\alpha^3=\beta^3=1$.
Nous avons $\alpha^3=\beta^3=1$ car $X^3-1=(X-1)(X^2+X+1)$.
Si d n'est pas multiple de 3 alors $\alpha^d+\beta^d=\alpha+\beta$.
Si d est multiple de 3 alors $\alpha^d+\beta^d=2$ est congru à -1 modulo p si et seulement si $p=3$. □

Remarque 2.18. *Le théorème 2.17 se traduit de la manière suivante*

Soient $d\in\mathbb{N}^*$, p un nombre premier et (v_n) la suite définie par $v_{n+2}=-v_{n+1}-v_n$

1. *Si $p=3$ alors $\forall d\in\mathbb{N}^*$ et $\forall n\in\mathbb{N}$, $v_{n+2d}\equiv -v_{n+d}-v_n \bmod 3$.*
2. *Si $p\neq 3$ alors $\forall n\in\mathbb{N}$, $v_{n+2d}\equiv -v_{n+d}-v_n \bmod p$ si et seulement si d n'est pas multiple de 3.*

2.3.3 Suite de Fibonacci

Soient p un nombre premier et α une racine du polynôme caractéristique $f(X)=X^2-X-1$ de la suite de Fibonacci $(F_n)_n$ sur $\mathbb{F}_p$. Un des problèmes qui demeure encore ouvert concernant la suite de Fibonacci est celui de la détermination de l'ordre de la racine α (dans le groupe multiplicatif $\mathbb{F}_{p^2}\setminus\{-1\}$ (voir Corollaire 2.11)). Il est équivalent à la détermination de la plus petite période $T(p)$ de la suite $(F_n)_n$ lorsqu'elle est réduite modulo p (exception faite pour $p=5$ où l'ordre de α est 4 est la période $T(5)$ est 20). Dans [66] figure une liste des valeurs de $T(m)$ pour m entier compris entre 2 et 1000 (nous l'avons mise en annexe à la fin de ce mémoire). Mais on ne connait pas de formule qui donne $T(m)$ de manière générale. Il est connu, cependant (voir [77] et [38]), que lorsque p est congru à 2 ou 3 modulo 5, l'ordre de α (donc $T(p)$) est un diviseur de $2(p+1)$ et que c'est un diviseur de $p-1$ lorsque p est congru à ± 1 modulo 5. Le lemme 2.19 et la preuve du théorème 2.10 donnent une démonstration de ce résultat.

Nous avons constaté sur les 168 nombres premiers, qui sont entre 2 et 1000, que l'ordre de α est maximal (i.e. atteint $2(p+1)$ ou $p-1$) dans près de 70 pour cent des cas.

Nous allons présenter les résultats concernant la suite de Fibonacci dans les cas précisément où l'ordre de α est maximal, en distinguant le cas où f est réductible de celui où il est irréductible.

Cas irréductible :

Le polynôme f est irréductible modulo le nombre premier p si et seulement si le discriminant de f, qui est égal à 5, n'est pas un résidu quadratique modulo p. En d'autres termes si et seulement si p est congru à 2 ou 3 modulo 5.

Le lemme suivant nous sera utile pour la démonstration du théorème relatif au cas irréductible.

Lemme 2.19. *Soit $(F_n)_n$ la suite de Fibonacci et soit α une racine de son polynôme caractéristique $f(X) = X^2 - X - 1$. Nous avons les propriétés suivantes :*

1. *Pour tout $n \in \mathbb{N}^*$, $\alpha^n = \alpha F_n + F_{n-1}$.*
2. *Pour tout nombre premier p congru à 2 ou 3 modulo 5,*

$$F_{p+1} \equiv 0 \mod p, \quad F_p \equiv -1 \mod p \text{ et } \alpha^{p+1} \equiv -1 \mod p.$$

Donc l'ordre de α est un diviseur de $2(p+1)$.

Preuve.

1. Se démontre par récurrence sur n.

2. Pour $p = 2$ on a $F_2 = 1 \equiv -1 \mod 2$ et $F_3 = 2 \equiv 0 \mod 2$.

Pour p impair, le $(p+1)$-ème terme de la suite de Fibonacci est donné par la formule de Binet

$$F_{p+1} = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^{p+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{p+1} \right].$$

D'où

$$2^{p+1}\sqrt{5}F_{p+1} = (1+\sqrt{5})^{p+1} - (1-\sqrt{5})^{p+1}.$$

À l'aide de la formule du binôme

$$\begin{aligned} 2^{p+1}\sqrt{5}F_{p+1} &= \left(1+\sqrt{5}\right) \left[\sum_{k=o}^{p} \binom{p}{k} (\sqrt{5})^k \right] - \left(1-\sqrt{5}\right) \left[\sum_{k=o}^{p} \binom{p}{k} (-1)^k (\sqrt{5})^k \right] \\ &= 2\sqrt{5} \left[\sum_{\substack{k=0 \\ k \text{ impair}}}^{p} \binom{p}{k} 5^{\frac{k-1}{2}} + \sum_{\substack{k=0 \\ k \text{ pair}}}^{p} \binom{p}{k} 5^{\frac{k}{2}} \right]. \end{aligned}$$

Comme p divise $\binom{p}{k}$ $(1 \leq k \leq p-1)$, on obtient modulo p

$$2^p F_{p+1} \equiv 5^{\frac{p-1}{2}} + 1. \tag{2.3}$$

Il suffit donc de montrer que

$$5^{\frac{p-1}{2}} + 1 \equiv 0 \mod p$$

pour tout p premier impair congru à 2 ou 3 modulo 5.

Désignons par $\left(\frac{\cdot}{\cdot}\right)$ le symbôle de Legendre. Par le critère d'Euler

$$\left(\frac{5}{p}\right) \equiv 5^{\frac{p-1}{2}} \mod p.$$

Comme $5 \equiv 1 \mod 4$ alors

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right).$$

Par ailleurs p n'est pas un résidu quadratique modulo 5, il s'ensuit que $\left(\frac{p}{5}\right) = -1$ et donc

$$5^{\frac{p-1}{2}} \equiv -1 \mod p.$$

Grâce à l'intégrité du corps $\mathbb{F}_p$, nous déduisons de (2.3), que

$$F_{p+1} \equiv 0 \mod p.$$

De la même manière, à partir de la formule du binôme

$$2^{p-1}F_p \equiv 5^{\frac{p-1}{2}} \mod p \equiv -1 \mod p.$$

D'après le petit théorème de Fermat, $2^{p-1} \equiv 1 \mod p$ donc $F_p \equiv -1 \mod p$.

□

Avant d'établir le résultat concernant la suite de Fibonacci, nous avons effectué des calculs sur les premiers nombres premiers p congrus à 2 ou 3 modulo 5 et nous avons remarqué certaines propriétés que nous avons consignées dans la proposition suivante et qui se sont avérées utiles pour faire la preuve de notre résultat.

Proposition 2.20. *Soient p un nombre premier congru à 2 ou 3 modulo 5, α et β les racines du polynôme caractéristique $f(X) = X^2 - X - 1$ de la suite de Fibonacci sur $\mathbb{Q}_p$. Nous avons :*

1. $\forall k,\ 0 \leq k \leq p-1, \quad \alpha^{2p-(2k+1)} + \beta^{2p-(2k+1)} = -\alpha^{2k+3} - \beta^{2k+3}$,
2. $\alpha^{2p+1} + \beta^{2p+1} \equiv -1 \bmod p$,
3. $\alpha^{p+2} + \beta^{p+2} \equiv -1 \bmod p$,
4. $\forall k,\ 0 \leq k \leq p-1, \quad \alpha^{(p+1)-(2k+1)} + \beta^{(p+1)-(2k+1)} = \alpha^{2k+1} + \beta^{2k+1}$.

Preuve.

La preuve de (1) se fait par récurrence sur k.

Pour $k = 0$ nous avons modulo p

$$\begin{aligned} \alpha^{2p-1} + \beta^{2p-1} &= \alpha^{2(p+1)-3} + \beta^{2(p+1)-3} \\ &= (\alpha^{p+1})^2\alpha^{-3} + (\beta^{p+1})^2\beta^{-3} \\ &= \alpha^{-3} + \beta^{-3} \quad (Lemme 2.19 \\ &= -\alpha^3 - \beta^3, \end{aligned}$$

car $\alpha\beta = -1$ donc $\alpha^{-1} = -\beta$ et $\beta^{-1} = -\beta$.

Supposons la propriété vraie jusqu'à l'ordre k. Au rang suivant

$$\begin{aligned}
\alpha^{2p-(2k+3)} + \beta^{2p-(2k+3)} &= \alpha^{2p-(2k+1)}\alpha^{-2} + \beta^{2p-(2k+1)}\beta^{-2} \\
&= \alpha^{-2}(\alpha^{2p-(2k+1)} + \beta^{2p-(2k+1)}) - \alpha^{-2}\beta^{2p-(2k+1)} \\
&\quad +\beta^{-2}(\alpha^{2p-(2k+1)} + \beta^{2p-(2k+1)}) - \beta^{-2}\alpha^{2p-(2k+1)} \\
&= (-\alpha^{2k+3} - \beta^{2k+3})(\alpha^{-2} + \beta^{-2}) - \alpha^{-2}\beta^{-2}\beta^{2p-(2(k-1)+1)} \\
&\quad -\alpha^{-2}\beta^{-2}\alpha^{2p-(2(k-1)+1)}.
\end{aligned}$$

Comme $\alpha^{-2} + \beta^{-2} = \alpha^2 + \beta^2$ (car $\alpha\beta = -1$), alors

$$\begin{aligned}
\alpha^{2p-(2k+3)} + \beta^{2p-(2k+3)} &= (-\alpha^{2k+3} - \beta^{2k+3})(\alpha^2 + \beta^2) - \beta^{2p-(2(k-1)+1)} - \alpha^{2p-(2(k-1)+1)} \\
&= -\alpha^{2k+5} - \beta^{2k+5} - \beta^{2k+1} - \alpha^{2k+1} + \beta^{2k+1} + \alpha^{2k+1} \\
&= -\alpha^{2k+5} - \beta^{2k+5}.
\end{aligned}$$

Les propriétés (2) et (3) proviennent du lemme 2.19.

Preuve de (4) : Nous avons
Pour tout $1 \leq k \leq p-1$,

$$\begin{aligned}
\alpha^{(p+1)-(2k+1)} + \beta^{(p+1)-(2k+1)} &= -(\alpha^{p+1}\alpha^{(p+1)-(2k+1)} + \beta^{p+1}\beta^{(p+1)-(2k+1)}) \\
&= -(\alpha^{2(p+1)-(2k+1)} + \beta^{2(p+1)-(2k+1)}) \\
&= -(\alpha^{2p-(2k-1)} + \beta^{2p-(2k-1)}) \\
&= \alpha^{2k+1} + \beta^{2k+1}.
\end{aligned}$$

□

Nous pouvons maintenant énoncer le théorème concernant la suite de Fibonacci.

Notons d'abord que, pour p premier congru à 2 ou 3 modulo 5 son polynôme caractéristique $f(X) = X^2 - X - 1$ est irréductible sur $\mathbb{F}_p$, donc le degré résiduel du corps de décomposition de f sur $\mathbb{Q}_p$ est égal à 2. On sait alors du corollaire 2.11, que si $d \equiv 1$ ou $p \mod (p^2-1)$ alors $f_d(X) \equiv f(X) \mod p$. Cependant, comme l'affirme le théorème qui suit, cette condition, à l'exception de $p = 2$, ne fournit pas tous les d qui réalisent cette dernière congruence.

Théorème 2.21. *Soient d un entier naturel, p un nombre premier congru à 2 ou 3 modulo 5 et $(F_n)_n$ la suite de Fibonacci de polynôme caractéristique $f(X) = X^2 - X - 1$. On suppose que p est tel que les racines de f sont d'ordre $2(p+1)$. Alors*

$$f_d(X) \equiv f(X) \mod p \Leftrightarrow d = \begin{cases} 3n \pm 1 & si\ p = 2, \\ (p+1)n + (-1)^n & si\ p \neq 2. \end{cases}$$

où $n \in \mathbb{N}$.

Preuve.

Soit p un nombre premier congru à 2 ou 3 modulo 5. Notons que $f_d(X) \equiv f(X) \mod p$ équivaut au système

$$\begin{cases} \alpha^d + \beta^d & \equiv & \alpha + \beta \mod p, \\ \alpha^d \beta^d & \equiv & \alpha\beta \mod p, \end{cases}$$

α et β sont, bien entendu, les racines de f. Elles vérifient $\alpha + \beta = 1$ et $\alpha\beta = -1$.

Examinons, d'abord, les cas $p = 2$ et $p = 3$.

Pour $p = 2$, en écrivant $d = 3m + r$ avec $m \in \mathbb{N}$ et $0 \leq r \leq 2$, nous vérifions facilement que le système est réalisé si et seulement si $r \neq 0$.

Pour $p = 3$, la condition $d = 4n + (-1)^n$ équivaut à $d \equiv 1$ ou $3 \bmod 8$. Ecrivons alors $d = 8m + r$ avec $m \in \mathbb{N}$ et $0 \leq r \leq 7$. Il s'agit de monter que le système est réalisé si et seulement si $r = 1$ ou $r = 3$.

Puisque $\alpha\beta = -1$ nous ne devons considérer que les valeurs impaires de r.

D'après le lemme 2.19, $\alpha^4 = -1$ (modulo 3) donc

$$\alpha^{8n+1} + \beta^{8n+1} = \alpha + \beta \text{ et } \alpha^{8n+3} + \beta^{8n+1} = \alpha + \beta.$$

Alors que

$$\alpha^{8n+5} + \beta^{8n+5} = -\alpha - \beta \text{ et } \alpha^{8n+7} + \beta^{8n+7} = -\alpha - \beta$$

et

$$-\alpha - \beta \not\equiv \alpha + \beta \bmod 3.$$

Soit, maintenant, p un nombre premier ≥ 5 et congru à 2 ou 3 modulo 5.

Chercher les entiers d qui vérifient

$$f_d(X) \equiv f(X) \mod p$$

revient à chercher les d impaires qui réalisent

$$\alpha^d + \beta^d \equiv (\alpha + \beta) \mod p.$$

Vérifions que les $d = (p+1)n + (-1)^n$ $(n \in \mathbb{N})$ conviennent.

Nous avons d'après le lemme 2.19

$$\begin{aligned} \alpha^d + \beta^d &= (\alpha^{p+1})^n (\alpha)^{(-1)^n} + (\beta^{p+1})^n (\beta)^{(-1)^n} \\ &\equiv (-1)^n (\alpha)^{(-1)^n} + (-1)^n (\beta)^{(-1)^n} \mod p. \end{aligned}$$

Que n soit pair ou impair

$$\alpha^d + \beta^d \equiv \alpha + \beta \mod p.$$

Par suite

$$f_d(X) \equiv f(X) \bmod p.$$

Réciproquement, montrons que si d est impair et

$$d \neq (p+1)n + (-1)^n$$

alors

$$f_d(X) \not\equiv f(X) \bmod p$$

Nous pouvons écrire $d = 2(p+1)m + r$ avec $m \in \mathbb{N}$, r impair, $r \neq p$ et $3 \leq r \leq 2p+1$. Comme $\alpha^{p+1} \equiv -1 \bmod p$ (lemme 2.19) alors

$$\begin{aligned} \alpha^d + \beta^d &= (\alpha^{2(p+1)})^n \alpha^r + (\beta^{2(p+1)})^n \beta^r \\ &\equiv \alpha^r + \beta^r \bmod p. \end{aligned}$$

Il s'agit donc de montrer que si r est impair, $r \neq p$ et $3 \leq r \leq 2p+1$ alors

$$\alpha^r + \beta^r \not\equiv 1 \bmod p.$$

Par exemple, pour $p = 17$, $r \in \{3, 5, 7, 9, 11, 13, 15, 19, 21, 23, 25, 27, 29, 31, 33, 35\}$

et $\alpha^r + \beta^r$ est congru modulo 17 à :

$$4, 11, 12, 8, 12, 11, 4, -1, -4, -11, -12, -8, -12, -11, -4, -1.$$

A l'instar de cet exemple, nous avons observé pour les nombres premiers testés, qu'effectivement $\alpha^r + \beta^r$ n'est pas congru à 1 modulo p mais surtout, chose importante, que les valeurs de $\alpha^r + \beta^r$, prises dans l'ordre, présentent deux symétries. D'abord une première symétrie au niveau de $r = p+2$ où on a les mêmes valeurs de part et d'autre de -1 avec des signes opposés. Puis une seconde symétrie lorsque $3 \leq r \leq p-2$ avec des valeurs identiques.

Ce sont ces constatations qui ont fait l'objet de la proposition 2.20.

Compte tenu de ces symétries, il s'agit de démontrer que pour tout r impair tel que $3 \leq r \leq \frac{p+1}{2}$, nous avons

$$\alpha^r + \beta^r \not\equiv \pm 1 \bmod p$$

ou de manière équivalente pour tout $1 \leq k \leq \lfloor \frac{p-1}{4} \rfloor$,

$$\alpha^{2k+1} + \beta^{2k+1} \not\equiv \pm 1 \bmod p.$$

Comme $\beta = -\alpha^{-1}$ alors

$$\alpha^{2k+1} + \beta^{2k+1} = \alpha^{2k+1} - \alpha^{-(2k+1)}.$$

Supposons que

$$\alpha^{2k+1} + \beta^{2k+1} \equiv 1 \bmod p.$$

Nous aurons

$$(\alpha^{2k+1})^2 - \alpha^{2k+1} - 1 \equiv 0 \mod p.$$

Donc, modulo p, α^{2k+1} est racine de f. On distingue alors deux cas :

Si $\alpha^{2k+1} \equiv \alpha \mod p$ alors $\alpha^{2k} \equiv 1 \mod p$. Donc l'ordre de α dans le groupe multiplicatif $\mathbb{F}_{p^2} - \{0\}$ divise $2k$. Par suite $2p + 2 \leq 2k$. Nous obtenons alors $k \geq p + 1$ ce qui n'est pas le cas.

Si $\alpha^{2k+1} \equiv -\alpha^{-1} \mod p$ alors $\alpha^{4k+4} \equiv 1 \mod p$. Le raisonnement précédent nous conduit à $k \geq \dfrac{p-1}{2}$ ce qui n'est pas le cas non plus.

Supposons, à présent, que

$$\alpha^{2k+1} + \beta^{2k+1} \equiv -1 \bmod p.$$

En remplaçant β par $-\alpha^{-1}$ nous aboutissons à

$$(\alpha^{2k+1})^2 + \alpha^{2k+1} - 1 \equiv 0 \mod p.$$

Dans ce cas α^{2k+1} est racine, modulo p du polynôme $X^2 + X - 1 = (X + \alpha)(X + \beta)$. Là aussi nous observons deux cas :

Si $\alpha^{2k+1} \equiv -\alpha \mod p$ alors $\alpha^{4k} \equiv 1 \mod p$. Ce qui entraine $k \geq \dfrac{p+1}{2}$ qui n'est pas vraie.

Si $\alpha^{2k+1} \equiv \alpha^{-1} \mod p$ alors $\alpha^{2k+2} \equiv 1 \mod p$. D'où nous déduisons $k \geq p$ qui est faux.

□

Remarque 2.22. *Le corollaire 2.11 qui affirme, dans le cas où $f(X) = X^2 - X - 1$ est irréductible, que si $d \equiv 1$ ou $p \bmod (p^2 - 1)$ alors $f_d(X) \equiv f(X) \bmod p$ est une conséquence du théorème 2.21. En effet pour $p \neq 2$,*

$$\begin{array}{rcll} d \equiv 1 \bmod (p-1)^2 & \Rightarrow & d = 1 + (p+1)m(p-1) & \textit{avec } m \in \mathbb{N} \\ & \Rightarrow & d = (p+1)n + (-1)^n & \textit{avec } n = m(p+1) \textit{ pair} \\ & \Rightarrow & f_d(X) \equiv f(X) \bmod p & \end{array}$$

De même

$$\begin{array}{rcll} d \equiv p \bmod (p-1)^2 & \Rightarrow & d = -1 + (p+1) + (p+1)m(p-1) & \textit{avec } m \in \mathbb{N} \\ & \Rightarrow & d = (p+1)n + (-1)^n & \textit{avec } n = (p-1)m + 1 \textit{ impair} \\ & \Rightarrow & f_d(X) \equiv f(X) \bmod p & \end{array}$$

Cas réductible

Nous nous proposons de compléter le théorème 2.21 par l'étude du cas où le polynôme caractèristique $f(X) = X^2 - X - 1$ de la suite de Fibonacci est réductible sur $\mathbb{F}_p$. Cette situation se présente lorsque le discriminant de f, qui est 5, est un résidu quadratique modulo le nombre premier p c'est à dire lorsque $p = 5$ ou p est congru à ± 1 modulo 5.

Comme dans le cas irréductible, nous allons d'abord établir une proposition qui nous sera utile pour la suite.

Proposition 2.23. *Soit p un nombre premier congru à ± 1 modulo 5 et k un entier tel que $3 \leq k \leq \frac{p-3}{2}$. Nous avons les assertions suivantes :*

1. $\alpha^{p-2} + \beta^{p-2} \equiv -1 \bmod p$.
2. $\alpha^{(p-1)-(2k+1)} + \beta^{(p-1)-(2k+1)} = -(\alpha^{2k+1} + \beta^{2k+1})$.
3. *Si p n'est pas congru à 1 modulo 4 alors* $\alpha^{\frac{p-1}{2}} + \beta^{\frac{p-1}{2}} \equiv 0 \bmod p$.
4. *Si p est congru à 1 modulo 4 alors* $\alpha^{\frac{p-3}{2}} + \beta^{\frac{p-3}{2}} \equiv \pm 1 \bmod p$.

   De plus

   si $\alpha^{\frac{p-3}{2}} + \beta^{\frac{p-3}{2}} \equiv 1 \bmod p$ *alors* $\alpha^{\frac{p+1}{2}} + \beta^{\frac{p+1}{2}} \equiv -1 \bmod p$

   si $\alpha^{\frac{p-3}{2}} + \beta^{\frac{p-3}{2}} \equiv -1 \bmod p$ *alors* $\alpha^{\frac{p+1}{2}} + \beta^{\frac{p+1}{2}} \equiv 1 \bmod p$.

Preuve.

1. Comme modulo p, $\alpha^{p-1} = 1$ et $\alpha\beta = -1$ alors

$$\alpha^{p-2} + \beta^{p-2} = \alpha^{p-1}\ \alpha^{-1} + \beta^{p-1}\ \beta^{-1} = \alpha^{-1} + \beta^{-1} = -(\alpha + \beta) = -1.$$

2. Pour les mêmes raisons

$$\alpha^{(p-1)-(2k+1)} + \beta^{(p-1)-(2k+1)} = \alpha^{-(2k+1)} + \beta^{-(2k+1)} = -\beta^{2k+1} - \alpha^{2k+1}.$$

3. Comme $\alpha^{\frac{p-1}{2}} + \beta^{\frac{p-1}{2}} = F_{\frac{p-1}{2}} + 2F_{\frac{p-3}{2}}$, il s'agit alors de montrer que

$$F_{\frac{p-1}{2}} + 2F_{\frac{p-3}{2}} \equiv 0 \bmod p.$$

   Soit $\varphi = \dfrac{1+\sqrt{5}}{2}$ le nombre d'or et $\overline{\varphi}$ son conjugué. Nous avons

$$\varphi + \overline{\varphi} = 1, \quad \varphi - \overline{\varphi} = \sqrt{5} \quad \text{et} \quad \varphi\,\overline{\varphi} = -1.$$

   D'après la formule de Binet

$$\begin{aligned} F_{\frac{p-1}{2}} + 2F_{\frac{p-3}{2}} &= \frac{1}{\sqrt{5}}\left[\left(\varphi^{\frac{p-1}{2}} - \overline{\varphi}^{\frac{p-1}{2}}\right) + 2\left(\varphi^{\frac{p-3}{2}} - \overline{\varphi}^{\frac{p-3}{2}}\right)\right] \\ &= \frac{1}{\sqrt{5}}\left[\varphi^{\frac{p-1}{2}} - \overline{\varphi}^{\frac{p-1}{2}} - 2\varphi\,\overline{\varphi}\,\varphi^{\frac{p-3}{2}} + 2\varphi\,\overline{\varphi}\,\overline{\varphi}^{\frac{p-3}{2}}\right] \\ &= \frac{1}{\sqrt{5}}\left[\varphi^{\frac{p-1}{2}} - \overline{\varphi}^{\frac{p-1}{2}} - 2\overline{\varphi}\,\varphi^{\frac{p-1}{2}} + 2\varphi\,\overline{\varphi}^{\frac{p-1}{2}}\right] \\ &= \frac{1}{\sqrt{5}}\left[\varphi^{\frac{p-1}{2}}(1-2\overline{\varphi}) - \overline{\varphi}^{\frac{p-1}{2}}(1-2\varphi)\right] \\ &= \varphi^{\frac{p-1}{2}} + \overline{\varphi}^{\frac{p-1}{2}} \end{aligned}$$

Par suite

$$\left(F_{\frac{p-1}{2}} + 2F_{\frac{p-3}{2}}\right)^2 = \varphi^{p-1} + \overline{\varphi}^{p-1} + 2(-1)^{\frac{p-1}{2}}.$$

En remplaçant φ et $\overline{\varphi}$ par leur valeur et en développant par la formule du Binôme nous aboutissons, après calculs, à

$$2^p\left(F_{\frac{p-1}{2}} + 2F_{\frac{p-3}{2}}\right)^2 = (-1)^{\frac{p-1}{2}}\ 2^{p+1} - 1 + 5^{\frac{p-1}{2}}\ 5.$$

Comme $p \equiv \pm 1 \bmod 5$ alors

$$5^{\frac{p-1}{2}} \equiv 1 \bmod p,$$

D'après le critère d'Euler, $2^{\frac{p-1}{2}} \equiv (\frac{2}{p}) \bmod p \equiv \pm 1 \bmod p$. Par suite

$$2^p = 2\ \left(2^{\frac{p-1}{2}}\right)^2 \equiv 2 \bmod p,$$

où $(\frac{\cdot}{\cdot})$ désigne le symbôle de Legendre.
Par conséquent

$$\left(F_{\frac{p-1}{2}} + 2F_{\frac{p-3}{2}}\right)^2 \equiv 2\ (-1)^{\frac{p-1}{2}} + 2 \bmod p.$$

Ce qui implique que si p n'est pas congru à 1 mod 4 alors

$$F_{\frac{p-1}{2}} + 2F_{\frac{p-3}{2}} \equiv 0 \bmod p.$$

4. En procédant de la même manière que dans (3) nous aurons

$$(\alpha^{\frac{p-3}{2}} + \beta^{\frac{p-3}{2}})^2 \equiv -2 + 5 + 2(-1)^{\frac{p-3}{2}} \bmod p.$$

Donc si $p \equiv 1 \bmod 4$ alors $\frac{p-3}{2}$ est impair ce qui donne

$$\alpha^{\frac{p-3}{2}} + \beta^{\frac{p-3}{2}} \equiv \pm 1 \bmod p.$$

Nous avons $\frac{p+1}{2} = p - 1 - \frac{p-3}{2}$ avec $\frac{p-3}{2}$ impair. D'après (2) :

si $\alpha^{\frac{p-3}{2}} + \beta^{\frac{p-3}{2}} \equiv 1 \bmod p$ alors $\alpha^{\frac{p+1}{2}} + \beta^{\frac{p+1}{2}} \equiv -1 \bmod p$

si $\alpha^{\frac{p-3}{2}} + \beta^{\frac{p-3}{2}} \equiv -1 \bmod p$ alors $\alpha^{\frac{p+1}{2}} + \beta^{\frac{p+1}{2}} \equiv 1 \bmod p$.

□

Voici maintenant le résultat concernant la suite de Fibonacci lorsque son polynôme caractéristique $f(X) = X^2 - X - 1$ est réductible modulo p.

On se place dans le cas où les racines de f sont d'ordre $p - 1$.

Théorème 2.24. *Soient d un entier naturel, p un nombre premier égal à 5 ou congru à ± 1 modulo 5 et $f(X) = X^2 - X - 1$ le polynôme caractéristique de la suite de Fibonacci. On suppose que p est tel que les racines de f sont d'ordre $p - 1$. Alors*

1. *Si $p = 5$ ou p n'est pas congru à 1 modulo 4 alors*

$$f_d(X) \equiv f(X) \mod p \Leftrightarrow d \equiv 1 \mod (p-1).$$

2. *Si $p \neq 5$ est congru à 1 modulo 4 alors*

$$f_d(X) \equiv f(X) \mod p \Leftrightarrow d \equiv \begin{cases} \text{soit à } 1 \text{ ou } \dfrac{p-3}{2} \mod (p-1) \\ \text{soit à } 1 \text{ ou } \dfrac{p+1}{2} \mod (p-1) \end{cases}$$

Preuve. Puisque f est un polynôme réductible modulo p alors le degré résiduel t du corps de décomposition de f sur $\mathbb{Q}_p$ est égal à 1. Par le corollaire 2.11, chaque fois que d est congru à 1 modulo $(p-1)$ nous avons $f_d(X) \equiv f(X) \mod p$.

La condition suffisante se déduit du corollaire 2.11 et du (4) de la proposition 2.23.

Réciproquement, la congruence $f_d(X) \equiv f(X) \mod p$ équivaut au système

$$\begin{cases} \alpha^d + \beta^d &= \alpha + \beta \mod p \\ \alpha^d \beta^d &= \alpha\beta \mod p \end{cases}$$

α, β étant les racines de f sur $\mathbb{Q}_p$.

Cas où $p = 5$:

Comme $\alpha^4 \equiv 1 \bmod 5$ alors en écrivant $d = 4n + r$ avec $0 \leq r \leq 3$ nous constatons que seul $r = 1$ convient.

Cas où $p \neq 5$ et $p \equiv \pm 1 \bmod 5$:

Ecrivons $d = (p-1)n + r$ avec $n \in \mathbb{N}$ et $0 \leq r \leq p-2$. Comme $\alpha\beta = -1$ alors nous ne considérons que les r impairs $3 \leq r \leq p-2$. Il s'agit donc de montrer que :

si $p \not\equiv 1 \bmod 4$ alors $\alpha^r + \beta^r \not\equiv 1 \bmod p$ pour tout r impair $3 \leq r \leq p-2$,

si $p \equiv 1 \bmod 4$ alors $\alpha^r + \beta^r \not\equiv 1 \bmod p$ pour tout r impair $3 \leq r \leq p-2$

et $r \notin \left\{ \dfrac{p-3}{2},\ \dfrac{p+1}{2} \right\}$.

Examinons d'abord les exemples suivants
Pour $p = 19$, $r \in \{3, 5, 7, 9, 11, 13, 15, 17\}$ et $\alpha^r + \beta^r$ est congru modulo 19 à :

$$4, 11, 10, 0, -10, -11, -4, -1.$$

Pour $p = 41$, $r \in \{3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39\}$ et $\alpha^r + \beta^r$ est

congru modulo 41 à :

$$4, 11, 29, 35, 35, 29, 11, 4, 1, -1, -4, -11, -29, -35, -35, -29, -11, -4, -1.$$

Commentaires

- Pour $p = 19$ nous observons une symétrie pour les valeurs de $\alpha^r + \beta^r$ de part et d'autre de la valeur 0 (qui correspond à $r = 9$) et nous retrouvons aussi une symétrie dans le cas de $p = 41$ où les valeurs de $\alpha^r + \beta^r$ pour $21 \leq r \leq 37$ sont les opposées de celles pour lesquelles $3 \leq r \leq 19$.
- Pour $p = 41$ nous avons $\alpha^{19} + \beta^{19} = 1$ alors que cette valeur 1 n'apparait pas pour $p = 19$. En fait, il se trouve que $41 \equiv 1 \bmod 4$ et $19 = \dfrac{41-3}{2}$ et justement nous ne devons pas tenir compte de cette valeur.
  De plus dans les deux cas $\alpha^{p-2} + \beta^{p-2} = -1$.

Ce sont ces remarques qui sont notées dans la proposition 2.23 , dans un contexte générale.

Donc, tenant compte de la proposition 2.23, il suffit de montrer que si r est impair et

$3 \leq r \leq \frac{p-5}{2}$ alors $\alpha^r + \beta^r$ n'est pas congru à ± 1 modulo p ou de manière équivalente, si

$1 \leq k \leq \frac{p-7}{4}$ alors $\alpha^{2k+1} + \beta^{2k+1}$ n'est pas congru à ± 1 modulo p.

Comme dans le cas irréductible, supposons qu'il existe un k tel que

$$\alpha^{2k+1} + \beta^{2k+1} \equiv 1 \bmod p$$

alors, en remplaçant β par $-\alpha^{-1}$, nous obtenons modulo p

$$(\alpha^{2k+1})^2 - \alpha^{2k+1} - 1 = 0$$

.

Par suite α^{2k+1} est racine de f. Nous avons alors deux cas :

Si $\alpha^{2k+1} = \alpha$ alors $\alpha^{2k} = 1$. Donc l'ordre de α divise $2k$. Par suite $p - 1 \leq 2k$ d'où $k \geq \frac{p-1}{2}$ ce qui contredit l'hypothèse.

Si $\alpha^{2k+1} = \beta$ alors $\alpha^{4k+4} = 1$ donc l'ordre de α divise $4k + 4$. Le raisonnement précédent nous conduit à $k \geq \frac{p-5}{4}$. Ce qui n'est pas le cas.

Supposons maintenant que

$$\alpha^{2k+1} + \beta^{2k+1} \equiv -1 \bmod p.$$

Nous avons alors

$$(\alpha^{2k+1})^2 + \alpha^{2k+1} - 1 = 0.$$

Dans ce cas α^{2k+1} est racine du polynôme $X^2 + X - 1 = (X + \alpha)(X + \beta)$.

Si $\alpha^{2k+1} = -\alpha$ alors l'ordre de α divise $4k + 2$ et nous déduisons que $k \geq \frac{p-3}{4}$ ce qui n'est pas le cas.

Si $\alpha^{2k+1} = -\beta = \alpha^{-1}$ alors l'ordre de α divise $2k + 2$ ce qui entraine $k \geq \frac{p-3}{2}$. Ce qui est faux.

□

Remarque 2.25. *Plaçons nous dans les cas où la période $T(p)$ de la suite de Fibonacci, quand elle est réduite modulo p, est maximale i.e. on s'intéresse aux p congrus à 2 ou 3 modulo 5 tels que $T(p) = 2(p + 1)$ et aux p congrus à ± 1 modulo 5 tels que $T(p) = p - 1$.*

Les résultats concernant la suite de Fibonacci se traduisent de la manière suivante :

Soient $d \in \mathbb{N}^*$, p un nombre premier tel que $T(p)$ est maximale et (F_n) la suite de Fibonacci.

1. *Si p est congru à 2 ou 3 modulo 5 alors pour tout n,*

$$F_{n+2d} \equiv F_{n+d} + F_n \bmod p \Leftrightarrow d = \begin{cases} 3m \pm 1 & \text{si } p = 2 \\ (p+1)m + (-1)^m & \text{si } p \neq 2 \end{cases}$$

   $(m \in \mathbb{N})$.

2. *Si p est égal à 5 ou congru à ± 1 modulo 5 alors*

   (a) *Si $p = 5$ ou p n'est pas congru à 1 modulo 4 alors, pour tout n,*

$$F_{n+2d} \equiv F_{n+d} + F_n \bmod p \Leftrightarrow d \equiv 1 \bmod (p-1).$$

(b) Si $p \neq 5$ et congru à 1 modulo 4 alors, pour tout n,

$$F_{n+2d} \equiv F_{n+d} + F_n \bmod p \Leftrightarrow d \equiv \begin{cases} \text{soit à } 1 \text{ ou } \dfrac{p-3}{2} \bmod (p-1) \\ \\ \text{soit à } 1 \text{ ou } \dfrac{p+1}{2} \bmod (p-1) \end{cases}$$

Remarque 2.26. *Le corollaire 2.11 qui affirme, dans le cas où $f(X) = X^2 - X - 1$ est réductible modulo p, que $f_d(X) \equiv f(X) \bmod p$ chaque fois que $d \equiv 1 \bmod (p-1)$ est une conséquence du théorème 2.24 mais ne fournit pas tous les d qui réalisent cette congruence.*

Remarque 2.27. *Le théorème 2.2, dû à H.T. Freitag énoncé au début de ce chapitre et qui à motivé ce travail, est un cas particulier de notre résultat concernant la suite $(F_n)_n$ de Fibonacci.*

En effet, d'après la remarque 2.25,

$$\begin{aligned} F_{n+2d} \equiv F_{n+d} + F_n \bmod 10 \quad &\Leftrightarrow \quad \begin{cases} F_{n+2d} \equiv F_{n+d} + F_n \bmod 2 \\ \quad et \\ F_{n+2d} \equiv F_{n+d} + F_n \bmod 5 \end{cases} \\ &\Leftrightarrow \quad d \equiv \begin{cases} 1 \text{ ou } 2 \bmod 3 \\ et \\ 1 \bmod 4 \end{cases} \\ &\Leftrightarrow \quad d \equiv 1 \text{ ou } 5 \bmod 12. \end{aligned}$$

2.3.4 Suite des nombres de Lucas

La suite $(L_n)_n$ des nombres de Lucas, appelée aussi suite compagnon de la suite $(F_n)_n$ de Fibonacci, est la suite qui vérifie la même relation de récurrence que la suite de Fibonacci

$$\forall n \in \mathbb{N}, \quad L_{n+2} = L_{n+1} + L_n,$$

mais dont les termes initiaux sont $L_0 = 2$ et $L_1 = 1$ au lieu de 0 et 1 (voir [43]). Les premiers termes de cette suite sont

$$2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, 843, 1364, ...$$

La suite $(F_n)_n$ de Fibonacci et sa suite compagnon $(L_n)_n$ sont des cas particuliers des suites de Lucas $U(a,b)$ et $V(a,b)$, où a et b sont dans $\mathbb{Z}$, définies pour tout n dans $\mathbb{N}$ par :

$$U_{n+2}(a,b) = aU_{n+1}(a,b) + bU_n(a,b), \qquad U_0(a,b) = 0,\ U_1(a,b) = 1 \tag{2.4}$$

et

$$V_{n+2}(a,b) = aV_{n+1}(a,b) + bV_n(a,b), \qquad V_0(a,b) = 2,\ V_1(a,b) = a, \tag{2.5}$$

étudiées par le mathématicien français Edouard Lucas (1842-1891) dans [51]. Elles correspondent à $a = b = 1$.

La suite des nombres de Lucas et la suite de Fibonacci sont liées par plusieures identités. Parmi celles-ci, nous avons

$$\forall n \geq 1, \quad L_n = F_{n-1} + F_{n+1} \tag{2.6}$$

et

$$\forall n \geq 1, \quad 5F_n = L_{n-1} + L_{n+1} \tag{2.7}$$

Ces 2 identités nous permettent de montrer que, pour tous entiers naturels n, d et tout nombre premier p différent de 5,

$$L_{n+2d} \equiv L_{n+d} + L_n \bmod p \ \Leftrightarrow\ F_{n+2d} \equiv F_{n+d} + F_n \bmod p.$$

Par suite, le résultat énoncé pour la suite de Fibonacci (voir remarque 2.25) s'applique pour la suite des nombre de Lucas à condition que $p \neq 5$.

En fait, il est valable aussi pour $p = 5$. Il suffit pour cela de se rappeler que

$$L_{n+2d} \equiv L_{n+d} + L_n \bmod 5 \Leftrightarrow f_d(X) \equiv f(X) \bmod 5$$

et de montrer que

$$f_d(X) \equiv f(X) \bmod 5 \Leftrightarrow d \equiv 1 \bmod 4.$$

Ce qui se démontre comme dans le cas de la suite de Fibonacci.

2.3.5 Suite de polynôme caractéristique $f(X) = X^2 + X - 1$

Soit p un nombre premier. On considère la suite $(w_n)_n$ définie, pour tout entier naturel n, par la relation de récurrente linéaire $w_{n+2} = -w_{n+1} + w_n$ et par ses deux premiers termes $w_0 = 0$ et $w_1 = 1$. Elle est de polynôme caractéristique $f(X) = X^2 + X - 1$ ayant pour racines $-\alpha$ et $-\beta$ où α et β sont les racines du polynôme caractéristique $X^2 - X - 1$ de la suite $(F_n)_n$ de Fibonacci dans une extension convenable de $\mathbb{Q}_p$. Son terme général vérifie, pour tout n dans $\mathbb{N}$,

$$w_n = (-1)^{n+1}\ F_n.$$

Soient d, n dans $\mathbb{N}$, la congruence

$$w_{n+2d} \equiv -w_{n+d} + w_n \bmod p$$

est équivalente au système

$$\begin{cases} \alpha^d + \beta^d & \equiv \quad 1 \bmod p \\ \alpha^d\ \beta^d & \equiv -1 \bmod p. \end{cases}$$

Hormis pour $p = 2$, la deuxième congruence du système impose à d d'être impair. Il s'ensuit que

$$w_{n+2d} \equiv -w_{n+d} + w_n \bmod p \ \Leftrightarrow\ F_{n+2d} \equiv (-1)^{d+1} F_{n+d} + F_n \bmod p \ \Leftrightarrow\ F_{n+2d} \equiv F_{n+d} + F_n \bmod p.$$

Comme $-1 = 1$ modulo 2, alors ses équivalences sont aussi valables pour $p = 2$.

Il en résulte que le théorème concernant la suite de Fibonacci (voir remarque 2.25) s'applique pour la suite $(w_n)_n$.

2.3.6 Suite des nombres de Pell et sa suite compagnon

La suite $(P_n)_n$ des nombres de Pell (voir [44]) est définie par ses termes initiaux $P_0 = 0,\ \ P_1 = 1$ et, pour tout n dans $\mathbb{N}$, par la relation de récurrence $P_n = 2P_{n-1} + P_{n-2}$. Ses premiers termes sont :

$$0, 1, 2, 5, 12, 29, 70, 169, 408, 985, 2378, 5741, 13860, 33461, 80782, 195025, 470832, 1136682, ...$$

C'est Euler qui l'a nommée ainsi en hommage au mathématicien (et diplomate) anglais John Pell ($1611 - 1685$). C'est une suite récurrente linéaire d'ordre 2 et est un cas particulier de la suite $(U_n(a, b))_n$ de Lucas (voir la relation (2.4)) correspondant à $a = 2$ et $b = -1$, bien qu'historiquement elle lui fut antérieure.

Puisque nous avons réservé la notation p pour désigner les nombres premiers, alors afin d'éviter toute confusion nous noterons la suite $(P_n)_n$ par $(X_n)_n$.

La suite compagnon $(Y_n)_n$ de la suite des nombres de Pell appelée aussi la suite de Pell-Lucas est définie par la même relation de récurrence que la suite $(X_n)_n$ mais dont les termes initiaux sont $Y_0 = Y_1 = 2$. Elle correspond à la suite de Lucas $V_n(2, -1)$ (voir (2.5)). Ses premiers termes sont :

$$2, 2, 6, 16, 34, 82, 198, 478, 1154, 2786, 6726, 16238, 39202, 94642, 228486, 551614, 1331714, ...$$

Les propriétés suivantes, reliant les deux suites $(X_n)_n$ et $(Y_n)_n$, se démontrent par une simple récurrence :

$$\forall n \geq 1, \quad Y_n = X_{n-1} + X_{n+1}, \tag{2.8}$$

$$\forall n \geq 1, \quad 8X_n = Y_{n-1} + Y_{n+1}. \tag{2.9}$$

Ells induisent, pour tout p premier et tous n, d dans $\mathbb{N}$, la relation

$$Y_{n+2d} \equiv 2Y_{n+d} + Y_n \bmod p \Leftrightarrow X_{n+2d} \equiv 2X_{n+d} + X_n \bmod p. \tag{2.10}$$

Donc les entiers d qui réalisent la congruence $Y_{n+2d} \equiv 2Y_{n+d} + Y_n \bmod p$ sont ceux pour lesquels $X_{n+2d} \equiv 2X_{n+d} + X_n \bmod p$.

La suite des nombres de Pell admet $f(X) = X^2 - 2X - 1$ pour polynôme caractéristique. Il est irréductible modulo le nombre premier p si et seulement si p est congru à 3 ou 5 modulo 8. Et il est réductible modulo p si et seulement si $p = 2$ ou p est congru à 1 ou 7 modulo 8.

Le résultat concernant la suite des nombres de Pell est, moyennant quelques petites modifications, le même que celui énoncé pour la suite de Fibonacci. C'est à dire, pour p premier donné, les entiers d qui vérifient la congruence $f_d(X) \equiv f(X) \bmod p$ sont, à quelques modifications près, les mêmes que ceux trouvés pour la suite de Fibonacci.

Nous allons réécrire le lemme 2.19 ainsi que les propositions 2.20 et 2.23 pour les adapter à la suite de Pell.

Lemme 2.28. *Soit p un nombre premier et soient α, β les racines de $f(X) = X^2 - 2X - 1$ dans son corps de décomposition sur $\mathbb{Q}_p$. On a :*

1. *Pour tout $n \in \mathbb{N}^*$, $\alpha^n = \alpha X_n + X_{n-1}$,*
2. *Si p congru à 3 ou 5 modulo 8, alors*

$$X_{p+1} \equiv 0 \mod p, \quad X_p \equiv -1 \mod p \text{ et } \alpha^{p+1} \equiv -1 \mod p.$$

Donc l'ordre de α est un diviseur de $2(p+1)$.

Proposition 2.29. *Sot p un nombre premier congru à 3 ou 5 modulo 8 et soient α, β les racines de $f(X) = X^2 - 2X - 1$ dans son corps de décomposition sur $\mathbb{Q}_p$. On a :*

1. $\forall\ 0 \leq k \leq p-1, \quad \alpha^{2p-(2k+1)} + \beta^{2p-(2k+1)} = -\alpha^{2k+3} - \beta^{2k+3}$,
2. $\alpha^{2p+1} + \beta^{2p+1} \equiv -2 \bmod p$,
3. $\alpha^{p+2} + \beta^{p+2} \equiv -2 \bmod p$,
4. $\forall\ 0 \leq k \leq p-1, \quad \alpha^{(p+1)-(2k+1)} + \beta^{(p+1)-(2k+1)} = \alpha^{2k+1} + \beta^{2k+1}$.

Proposition 2.30. *Soit p un nombre premier congru à ± 1 modulo 8 et soient α, β les racines de $f(X) = X^2 - 2X - 1$ dans son corps de décomposition sur $\mathbb{Q}_p$. Nous avons, pour tout entier k tel que $3 \leq k \leq \frac{p-3}{2}$,*

1. $\alpha^{p-2} + \beta^{p-2} \equiv -2 \bmod p$.
2. $\alpha^{(p-1)-(2k+1)} + \beta^{(p-1)-(2k+1)} = -(\alpha^{2k+1} + \beta^{2k+1})$.
3. *Si p est congru à -1 modulo 8 alors $\alpha^{\frac{p-1}{2}} + \beta^{\frac{p-1}{2}} \equiv 0 \bmod p$.*

4. *Si p est congru à 1 modulo 8 alors* $\alpha^{\frac{p-3}{2}} + \beta^{\frac{p-3}{2}} \equiv \pm 2 \bmod p$.

   De plus

   si $\alpha^{\frac{p-3}{2}} + \beta^{\frac{p-3}{2}} \equiv 2 \bmod p$ *alors* $\alpha^{\frac{p+1}{2}} + \beta^{\frac{p+1}{2}} \equiv -2 \bmod p$

   si $\alpha^{\frac{p-3}{2}} + \beta^{\frac{p-3}{2}} \equiv -2 \bmod p$ *alors* $\alpha^{\frac{p+1}{2}} + \beta^{\frac{p+1}{2}} \equiv 2 \bmod p$.

Nous déduisons du corollaire 2.11 et du lemme 2.28 que lorsque f est réductible modulo $p \neq 2$ alors l'ordre de α est un diviseur de $p-1$ et que lorsque f est irréductible modulo p alors l'ordre de α est un diviseur de $2(p+1)$. Ce qui équivaut à dire que si $p \equiv \pm 1 \bmod 8$ alors la péridode $T'(p)$ de la suite des nombres de Pell réduite modulo p est un diviseur de $p-1$ et que si $p \equiv 3$ ou $5 \bmod 8$ alors $T'(p)$ est un diviseur de $2(p+1)$. Nous dirons que la période $T'(p)$ est maximale si les bornes sont atteintes.

Le résultat concernant la suite $(X_n)_n$ est le suivant :

Théorème 2.31. *Soient $d \in \mathbb{N}^*$, (X_n) la suite des nombres de Pell et p un nombre premier tel que $T'(p)$ est maximale.*

1. *Si p est congru à 3 ou 5 modulo 8 alors, pour tout n,*

$$X_{n+2d} \equiv 2X_{n+d} + X_n \bmod p \Leftrightarrow d \equiv 1 \text{ ou } p \bmod 2(p+1).$$

2. *Si $p = 2$ alors, pour tout n,* $X_{n+2d} \equiv 2X_{n+d} + X_n \bmod p$.
3. *Si p est congru à -1 modulo 8 alors, pour tout n,*

$$X_{n+2d} \equiv 2X_{n+d} + X_n \bmod p \Leftrightarrow d \equiv 1 \bmod (p-1).$$

4. *Si p est congru à 1 modulo 8 alors, pour tout n,*

$$X_{n+2d} \equiv 2X_{n+d} + X_n \bmod p \Leftrightarrow d \equiv \begin{cases} \text{soit à } 1 \text{ ou } \dfrac{p-3}{2} \bmod (p-1) \\ \\ \text{soit à } 1 \text{ ou } \dfrac{p+1}{2} \bmod (p-1) \end{cases}$$

Les preuves de ces résultats se font de la même manière que pour la suite de Fibonacci.

Grâce à l'équivalence (2.10), le théorème précèdent s'applique aussi à la suite de Pell-Lucas $(Y_n)_n$.

2.3.7 Cas cyclotomique

Soit q un nombre premier ≥ 3 et soit

$$f(X) = \frac{X^q - 1}{X - 1} = X^{q-1} + X^{q-2} + \cdots + X + 1$$

le q-ème polynôme cyclotomique dont les racines ξ_i sont les racines q-ièmes de l'unité.

Soit p un nombre premier.

Observons d'abord que si $p = q$ alors, modulo p,

$$\begin{aligned} f(X) &= \frac{X^p - 1}{X - 1} \\ &= \frac{(X-1)^p}{X-1} \\ &= (X-1)^{p-1}. \end{aligned}$$

Par suite $\xi = 1$ est l'unique racine de f. Par conséquent, pour tout d dans $\mathbb{N}^*$, nous avons, modulo p,

$$\begin{aligned} f_d(X) &= (X - 1^d)^{p-1} \\ &= f(X). \end{aligned}$$

Donc si $p = q$ alors, pour d dans $\mathbb{N}^*$,

$$f_d(X) \equiv f(X) \bmod p.$$

Dans la suite, nous supposons le nombre premier p différent de q.

Pour tout $1 \leq i \leq q-1$, les racines ξ_i sont des racines q-ièmes de l'unité distinctes de 1.

Soit d dans $\mathbb{N}^*$. Dans le corps de décomposition L de f sur $\mathbb{Q}_p$, nous avons

$$f(X) = \prod_{i=1}^{q-1} (X - \xi_i) \tag{2.11}$$

et

$$f_d(X) = \prod_{i=1}^{q-1} (X - \xi_i^d). \tag{2.12}$$

Désignons par $\sigma_1, ..., \sigma_{q-1}$ les polynômes symétriques élémentaires à $(q-1)$ indéterminées définis par :

$$\begin{aligned} \sigma_1(X_1, X_2, ..., X_{q-1}) &= X_1 + X_2 + \cdots + X_{q-1}, \\ \sigma_2(X_1, X_2, ..., X_{q-1}) &= \sum_{1 \leq i < j \leq q-1} X_i X_j, \\ &\vdots \\ \sigma_k(X_1, X_2, ..., X_{q-1}) &= \sum_{1 \leq i_1 < ... < i_k \leq q-1} X_{i_1} X_{i_2} \cdots X_{i_k}, \\ &\vdots \\ \sigma_{q-1}(X_1, X_2, ..., X_{q-1}) &= X_1 X_2 \cdots X_{q-1}. \end{aligned}$$

Le développement du produit (2.11) s'écrit

$$\begin{aligned} f(X) &= X^{q-1} - \sigma_1(\xi_1,\xi_2,...,\xi_{q-1})\, X^{q-2} + \cdots + (-1)^k\, \sigma_k(\xi_1,\xi_2,...,\xi_{q-1})\, X^{q-(k+1)} \\ &\quad + \cdots + \sigma_{q-1}(\xi_1,\xi_2,...,\xi_{q-1}). \end{aligned}$$

Notons alors que, pour chaque $1 \leq k \leq q-1$, $\sigma_k(\xi_1,\xi_2,...,\xi_{q-1}) = (-1)^k$.

Nous avons besoin du résultat suivant pour démontrer le théorème relatif au polynôme cyclotomique.

Lemme 2.32. *Pour k et r dans $\mathbb{N}$ tels que $1 \leq k \leq q-1$ et $1 \leq r \leq q-1$,*

$$\sigma_k(\xi_1^r,\xi_2^r,...,\xi_{q-1}^r) = \sigma_k(\xi_1,\xi_2,...,\xi_{q-1}). \tag{2.13}$$

Preuve.

Considérons l'ensemble $\mathcal{C}$ des entiers de L qui sont racines q-ièmes de l'unité. C'est un groupe cyclique d'ordre q. Soit ξ un générateur de $\mathcal{C}$.

Nous avons

$$\mathcal{C} = \{1,\xi_1,...,\xi_{q-1}\} = \langle\xi\rangle.$$

Pour $1 \leq r \leq q-1$, on définit l'endomorphisme ψ_r de $\mathcal{C}$ par $\psi_r(z) = z^r$.
le morphisme ψ_r est un isomorphisme de groupe car son noyau est réduit à l'élément neutre. En effet, un élément du noyau est un $z = \xi^n \quad (0 \leq n \leq q-1)$ tel que $\xi^{nr} = 1$. Il s'ensuit que $n = 0$ car sinon le nombre premier q serait un diviseur de nr ce qui est impossible.

Notre objectif est de montrer que

$$\sum_{1\leq i_1<...<i_k\leq q-1} \xi_{i_1}^r \xi_{i_2}^r ... \xi_{i_k}^r = \sum_{1\leq i_1<...<i_k\leq q-1} \xi_{i_1}\xi_{i_2}...\xi_{i_k}.$$

Chaque $\xi_{i_j} \quad (1 \leq j \leq k)$ s'écrit $\xi_{i_j} = \xi^{n_j} \quad (1 \leq n_j \leq q-1)$. Donc $\xi_{i_j}^r = \xi^{rn_j} = \xi_{m_j}$ $(1 \leq m_j \leq q-1)$. Les ξ_{m_j} sont distincts deux à deux du fait de la bijectivité de ψ_r. Il s'ensuit que

$$\sigma_k(\xi_1^r,\xi_2^r,...,\xi_{q-1}^r) = \sigma_k(\xi_{m_1},\xi_{m_2},...,\xi_{m_{q-1}}) = \sigma_k(\xi_1,\xi_2,...,\xi_{q-1}).$$

□

Suite à ce qui vient d'être fait, nous avons le théorème suivant :

Théorème 2.33. *Soient d un entier, p, q deux nombre premier avec $q \geq 3$ et $f(X) = X^{q-1} + X^{q-2} + ... + X + 1$ le polynôme cyclotomique de degré $(q-1)$. On a*

1. *Si $p = q$ alors $\forall d \in \mathbb{N}^*, \quad f_d(X) \equiv f(X) \mod p$*
2. *Si $p \neq q$ alors $f_d(X) \equiv f(X) \mod p$ si et seulement si d n'est pas un multiple de q.*

Preuve.

Le cas $q = 3$ a déjà été étudié (cf théorème 2.17).

Supposons donc que $q \geq 5$ et $q \neq p$.

Écrivons $d = qq' + r$ avec $0 \leq r \leq q-1$.

Intéressons nous d'abord au cas $r \neq 0$.

Sachant que pour tout $1 \leq i \leq q-1$, $\xi_i^q = 1$, la congruence $f_d(X) \equiv f(X) \mod p$ est alors équivalente, modulo p, à

$$\sigma_k(\xi_1^r, ..., \xi_{q-1}^r) = \sigma_k(\xi_1, ..., \xi_{q-1})$$

pour tout $1 \leq k \leq q-1$.

Ce qui est vrai d'après le lemme 2.32.

Nous venons ainsi de montrer que si $1 \leq r \leq q-1$, c'est-à-dire si d n'est pas un multiple de q alors

$$f_d(X) \equiv f(X) \bmod p.$$

Examinons, enfin, le cas $r = 0$ (i.e. d multiple de q).

Nous avons

$$\sigma_1(\xi_1^d, ..., \xi_{q-1}^d) = \sum_{i=1}^{q-1} \xi_i^d = q - 1$$

Puisque $p \neq q$, cette somme n'est pas congrue à -1 modulo p donc $f_d(X) \not\equiv f(X) \bmod p$. Ce qui démontre le théorème 2.33.

□

Remarque 2.34. *Ce théorème se traduit de la manière suivante :*

Soient d dans $\mathbb{N}^*$, p, q deux nombres premiers avec q impair et $(u_n)_n$ la suite récurrente linéaire de longueur $q-1$ définie, pour tout n dans $\mathbb{N}$, par

$$u_{n+(q-1)} = -u_{n+(q-2)} - u_{n+(q-3)} - \cdots - u_{n+1} - u_n.$$

On a

1. *Si $p = q$ alors, pour tout d dans $\mathbb{N}^*$ et tout n dans $\mathbb{N}$,*

$$u_{n+(q-1)d} \equiv -u_{n+(q-2)d} - u_{n+(q-3)d} - \cdots - u_{n+d} - u_n \mod p.$$

2. *Si $p \neq q$ alors, $\forall n \in \mathbb{N}$, $u_{n+(q-1)d} \equiv -u_{n+(q-2)d} - u_{n+(q-3)d} - \cdots - u_{n+d} - u_n \mod p$ si et seulement si d n'est pas un multiple de q.*

2.3.8 Suites de polynôme caractéristique $f(X) = X^{q-1} - X^{q-2} + X^{q-3} - X^{q-4} + \cdots - X + 1$

Soit q un nombre premier impair. Considérons le polynôme de degré $(q-1)$

$$f(X) = \frac{X^q + 1}{X + 1} = X^{q-1} - X^{q-2} + X^{q-3} - X^{q-4} + \cdots - X + 1$$

dont les racines sont les racines q-ièmes de -1. Nous allons donner, dans cette partie, un résultat qui généralise le théorème 2.14 obtenu pour f dans le cas où $q = 3$.

Soient p un nombre premier et d dans $\mathbb{N}^*$.

Éxaminons d'abord le cas $q = p$.

Comme dans le cas cyclotomique, nous avons modulo p,

$$\begin{aligned} f(X) &= \frac{X^p + 1}{X + 1} \\ &= \frac{(X+1)^p}{X+1} \\ &= (X - (-1))^{p-1} \end{aligned}$$

et

$$f_d(X) = (X - (-1)^d)^{p-1}.$$

Par suite, pour avoir $f_d(X) \equiv f(X) \bmod p$ il faut et il suffit que d soit impair.

Supposons, dans la suite que $q \neq p$, et désignons par ξ_i les racines de f dans son corps de décomposition L sur $\mathbb{Q}_p$. Dans L, nous avons

$$f(X) = \prod_{i=1}^{q-1} (X - \xi_i) \tag{2.14}$$

et

$$f_d(X) = \prod_{i=1}^{q-1} (X - \xi_i^d). \tag{2.15}$$

Pour $1 \leq i \leq (q-1)$, les racines ξ_i sont des racines q-ièmes de -1 distinctes de -1. Désignons par σ_k $(1 \leq k \leq q-1)$ les polynômes symétriques élémentaires à $(q-1)$ indéterminées définis par :

$$\sigma_k(X_1, X_2, ..., X_{q-1}) = \sum_{1 \leq i_1 < ... < i_k \leq q-1} X_{i_1} X_{i_2} \cdots X_{i_k}.$$

Le développement de (2.14) s'écrit

$$\begin{aligned} f(X) &= X^{q-1} - \sigma_1(\xi_1, \xi_2, ..., \xi_{q-1})\, X^{q-2} + \cdots + (-1)^k\, \sigma_k(\xi_1, \xi_2, ..., \xi_{q-1})\, X^{q-(k+1)} \\ &\quad + \cdots + \sigma_{q-1}(\xi_1, \xi_2, ..., \xi_{q-1}). \end{aligned}$$

Nous avons alors, pour chaque $1 \leq k \leq q-1$, $\sigma_k(\xi_1, \xi_2, ..., \xi_{q-1}) = 1$.

Avant d'énoncer le résultat relatif au polynôme f, nous avons besoin des lemmes suivants :

Lemme 2.35. *Pour tout entier naturel k tel que $1 \leq k \leq q-1$ et pour tout entier naturel r impair $r \neq q$ et $1 \leq r \leq 2q-1$, on a*

$$\sigma_k(\xi_1^r, \xi_2^r, ..., \xi_{q-1}^r) = \sigma_k(\xi_1, \xi_2, ..., \xi_{q-1}). \tag{2.16}$$

Preuve.

Considérons le groupe cyclique $\mathcal{C}$ des entiers de L racines $(2q)$-ièmes de l'unité et soit ξ un générateur de $\mathcal{C}$. Les racines de f sont les ξ^r avec r impair, $r \neq q$ et $1 \leq r \leq 2q-1$.

Pour chacun de ces r, considérons l'endomorphisme

$$\begin{array}{rccc} \psi_r : & \mathcal{C} & \to & \mathcal{C} \\ & z & \mapsto & z^r \end{array}$$

L'endomorphisme ψ_r est un isomorphisme de groupe. En effet, si $z = \xi^n \quad (0 \leq n \leq 2q-1)$ est dans le noyau de ψ_r alors $z^{nr} = 1$. Par suite $2q$ divise nr. En supposant $n \neq 0$ alors $n = 2m$ avec $1 \leq m \leq q-1$. D'où q divise mr et donc q divise r. Ce qui ne se réalise que si $q = r$. Ce qui n'est pas le cas. D'où $n = 0$ est ψ_r est injective.

Pour $1 \leq i \leq q-1$, posons $\xi_i = \xi^{k_i}$ avec k_i impair, $1 \leq k_i \leq 2q-1$ et $k_i \neq q$. Nous avons $\xi_i^r = \xi^{rk_i}$. Comme rk_i est impair et différent de q alors chaque ξ_i^r est un certain ξ_j avec $1 \leq j \leq q-1$. Les ξ_i^r étant au nombre de $(q-1)$ distints deux à deux, nous déduisons grâce à l'isomorphisme ψ_r, que les ξ_j sont aussi au nombre de $(q-1)$ distincts deux à deux. Ce qui entraîne

$$\forall 1 \leq k \leq q-1, \quad \sigma_k(\xi_1^r, \xi_2^r, ..., \xi_{q-1}^r) = \sigma_k(\xi_1, \xi_2, ..., \xi_{q-1}).$$

□

Lemme 2.36. *Soit p un nombre premier différent de 2 et de q. Alors si $r = q$ ou si r est pair non nul , il existe k $(1 \leq k \leq q-1)$ tel que*

$$\sigma_k(\xi_1^r, \xi_2^r, ..., \xi_{q-1}^r) \not\equiv \sigma_k(\xi_1, \xi_2, ..., \xi_{q-1}) \bmod p. \tag{2.17}$$

Preuve. Pour $r = q$

$$\sigma_1(\xi_1^q, \xi_2^q, ..., \xi_{q-1}^q) = (q-1)(-1) \not\equiv \sigma_1(\xi_1, \xi_2, ..., \xi_{q-1}) \bmod p, \quad \forall p \neq q. \tag{2.18}$$

Pour r pair, $2 \leq r \leq 2q-2$:

Nous distinguons deux cas :

Premier cas : $q+1 \leq r \leq 2q-2$

Posons $r = q + m$ avec m impair $1 \leq m \leq q-3$.
Nous avons, pour $1 \leq i \leq q-1$, $\xi_i^r = -\xi_i^m$.
Donc pour k impair $1 \leq k \leq q-1$ et pour p premier différent de 2

$$\begin{aligned}\sigma_k(\xi_1^r, \xi_2^r, ..., \xi_{q-1}^r) &= -\sigma_k(\xi_1^m, \xi_2^m, ..., \xi_{q-1}^m) \\ &= -\sigma_k(\xi_1, \xi_2, ..., \xi_{q-1}) \qquad \text{(lemme 2.35)} \\ &\not\equiv \sigma_k(\xi_1, \xi_2, ..., \xi_{q-1}) \bmod p\end{aligned}$$

Second cas : $2 \leq r \leq q-1$ et $r \neq q$
Posons $q = r + m$ avec m impair $1 \leq m \leq q-2$.
Pour chaque $1 \leq i \leq q-1$

$$\xi_i^r = \xi^{q-m} = -\xi^{-m} = -\xi^{2q-m}$$

avec $2q-m$ impair et $q+2 \leq 2q-m \leq 2q-1$.
Par suite, pour k impair $1 \leq k \leq q-1$ et pour p premier différent de 2

$$\begin{aligned}\sigma_k(\xi_1^r, \xi_2^r, ..., \xi_{q-1}^r) &= -\sigma_k(\xi_1^{2q-m}, \xi_2^{2q-m}, ..., \xi_{q-1}^{2q-m}) \\ &= -\sigma_k(\xi_1, \xi_2, ..., \xi_{q-1}) \qquad \text{(lemme 2.35)} \\ &\not\equiv \sigma_k(\xi_1, \xi_2, ..., \xi_{q-1}) \bmod p.\end{aligned}$$

□

Nous allons énoncer, maintenant, le théorème relatif au polynôme
$f(X) = X^{q-1} - X^{q-2} + \cdots - X + 1$.

Théorème 2.37. *Soient $d \in \mathbb{N}^*$, p, q deux nombres premiers avec q impair et $f(X) = X^{q-1} - X^{q-2} + \cdots - X + 1$. On a*

$$f_d(X) \equiv f(X) \bmod p \Leftrightarrow \begin{cases} d \not\equiv 0 \bmod q & \text{si } p = 2 \\ d \equiv 1 \bmod 2 & \text{si } p = q \\ d \equiv r \bmod 2q & \text{si } p \neq 2 \text{ et } p \neq q \\ \text{avec } 1 \leq r \leq 2q-1 & \\ r \text{ impair et } r \neq q & \end{cases}$$

Preuve.
Nous avons $f_d(X) \equiv f(X) \bmod p$ si et seulement si pour tout $1 \leq k \leq q-1$

$$\sigma_k(\xi_1^d, \xi_2^d, ..., \xi_{q-1}^d) \equiv \sigma_k(\xi_1, \xi_2, ..., \xi_{q-1}) \bmod p. \tag{2.19}$$

Soit r le reste de la division de d par $2q$. Pour tout $1 \leq i \leq q-1$, nous avons $\xi_i^d = \xi_i^r$.

Commençons par l'étude du cas $r = 0$.

Nous allons montrer que, pour tout p premier,

$$f_d(X) \not\equiv f(X) \bmod p.$$

C'est-à-dire qu'il existe $1 \leq k \leq q-1$ tel que

$$\sigma_k(\xi_1^0, ..., \xi_{q-1}^0) \not\equiv \sigma_k(\xi_1, \xi_2, ..., \xi_{q-1}) \bmod p.$$

Notons que

$$\sigma_k(\xi_1^0, ..., \xi_{q-1}^0) = \binom{q-1}{k}$$

où $\binom{\cdot}{\cdot}$ est le coefficient binomial.
Si $p \geq q$, alors $\sigma_1(\xi_1^0, ..., \xi_{q-1}^0) = q-1 \not\equiv \sigma_1(\xi_1, \xi_2, ..., \xi_{q-1}) \bmod p$
Si $p < q$ alors nous avons deux cas :

- $\sigma_1(\xi_1^0, ..., \xi_{q-1}^0) \not\equiv 1 \bmod p$. Dans ce cas c'est terminé.
- $\sigma_1(\xi_1^0, ..., \xi_{q-1}^0) \equiv 1 \bmod p$. Dans ce cas p divise $(q-2)$. Par suite

$$\sigma_2(\xi_1^0, ..., \xi_{q-1}^0) = \frac{(q-1)(q-2)}{2} \equiv 0 \bmod p$$

Donc $\sigma_2(\xi_1^0, ..., \xi_{q-1}^0) \not\equiv \sigma_2(\xi_1, ..., \xi_{q-1}) \bmod p$.

Supposons, dans la suite que $r \neq 0$.
Pour $p \neq 2,\ p \neq q$ et $1 \leq r \leq 2q-1$, nous avons, d'après le lemme 2.35 et le lemme 2.36

$$f_d(X) \equiv f(X) \bmod p \Leftrightarrow r \text{ impair et } r \neq q. \tag{2.20}$$

Reste à étudier le cas $p = 2$ et le cas $p = q$.
Supposon $p = 2$; nous avons du lemme 2.35, pour tout $1 \leq k \leq q-1$ et pour tout r impair avec $r \neq q$

$$\sigma_k(\xi_1^r, \xi_2^r, ..., \xi_{q-1}^r) = \sigma_k(\xi_1, \xi_2, ..., \xi_{q-1}) \bmod 2 \tag{2.21}$$

et en reprenant la preuve du lemme 2.36, nous avons pour r pair

$$\begin{aligned}
\sigma_k(\xi_1^r, \xi_2^r, ..., \xi_{q-1}^r) &= -\sigma_k(\xi_1^m, \xi_2^m, ..., \xi_{q-1}^m) \\
&= \begin{cases} -\sigma_k(\xi_1, \xi_2, ..., \xi_{q-1}) & \text{si} \quad k \text{ impair} \\ \sigma_k(\xi_1, \xi_2, ..., \xi_{q-1}) & \text{si} \quad k \text{ pair} \end{cases} \\
&\equiv \sigma_k(\xi_1, \xi_2, ..., \xi_{q-1}) \bmod 2.
\end{aligned}$$

Donc

$$f_d(X) \equiv f(X) \bmod 2 \Leftrightarrow r \neq 0 \text{ et } r \neq q.$$

□

Remarque 2.38. *Ce théorème se traduit de la manière suivante :*

Soient $d \in \mathbb{N}^*$, p et q deux nombres premiers avec q impair et $(u_n)_n$ la suite récurrente linéaire de longueur $(q-1)$ définie par $u_{n+(q-1)} = u_{n+(q-2)} - u_{n+(q-3)} + \cdots + u_{n+1} - u_n$. Alors, pour tout n,

$$u_{n+(q-1)d} \equiv u_{n+(q-2)d} - u_{n+(q-3)d} + \cdots + u_{n+d} - u_n \mod p \Leftrightarrow \begin{cases} d \not\equiv 0 \mod q & \text{si } p = 2, \\ d \equiv 1 \mod 2 & \text{si } p = q, \\ d \equiv r \mod 2q & \text{si } p \neq 2 \text{ et } p \neq q, \\ \text{avec } r \text{ impair,} & \\ 1 \leq r \leq 2q-1 & \\ \text{et } r \neq q. & \end{cases}$$

Chapitre 3

Polynômes bivariés généralisés de Fibonacci et de Lucas

Ce chapitre est consacré à l'étude de la suite des polynômes bivariés de Fibonacci et de la suite des polynômes bivariés de Lucas, qui sont une généralisation des suites de Lucas, dont nous avons déjà parlé au chapitre 2, définies par les relations (2.4) et (2.5) de la section 2.3.4. Les suites de Fibonacci, de Pell, de Pell Lucas,... en sont, donc, des cas particuliers. Nous allons donner leurs formes explicites, leurs séries génératrices et certaines de leurs propriétés.

3.1 Introduction

Pour n dans $\mathbb{N}$, soient $U_n(x,y)$ et $V_n(x,y)$ les polynômes à deux variables x et y à coefficients réels définis, pour tout n dans $\mathbb{N}$, par les relations de récurrence du second ordre suivantes :

$$\begin{cases} U_0 = 0,\ U_1 = 1, \\ U_n(x,y) = h(x)U_{n-1}(x,y) + k(y)U_{n-2}(x,y) \end{cases} \tag{3.1}$$

et

$$\begin{cases} V_0 = 2,\ V_1 = h(x), \\ V_n(x,y) = h(x)V_{n-1}(x,y) + k(y)V_{n-2}(x,y), \end{cases} \tag{3.2}$$

où $h(x)$ (resp. $k(y)$) est un polynôme en l'indéterminée x (resp. y) à coefficients réels.

Le cas où $h(x)$ ou $k(y)$ est nul étant trivial, nous supposerons dans la suite que $h(x)$ et $k(y)$ ne sont pas identiquement nuls.

Les polynômes $U_n(x,y)$ et $V_n(x,y)$ sont appelés, respectivement, polynômes bivariés généralisés de Fibonacci et de Lucas.

Nombres de suites classiques connues dans la littérature découlent des suites $(U_n(x,y))_n$ et $(V_n(x,y))_n$. Par exemple :

- Pour $h(x) = k(y) = 1$, nous obtenons les suites de Fibonacci et de Lucas (voir [43] et [66]) : $U_n(x,y) = F_n$ et $V_n(x,y) = L_n$ définies, pour tout n dans $\mathbb{N}$, par

$$\begin{cases} F_n = F_{n-1} + F_{n-2}, \\ F_0 = 0,\ F_1 = 1 \end{cases} \quad \text{et} \quad \begin{cases} L_n = L_{n-1} + L_{n-2}, \\ L_0 = 2,\ L_1 = 1. \end{cases} \tag{3.3}$$

- Pour $h(x) = 2$ et $k(y) = 1$, nous obtenons les nombres de Pell et de Pell-Lucas (voir [44]) : $U_n(x, y) = P_n$ et $V_n(x, y) = Q_n$ définis, pour tout n dans $\mathbb{N}$, par

$$\begin{cases} P_n = 2P_{n-1} + P_{n-2}, \\ P_0 = 0,\ P_1 = 1 \end{cases} \text{ et } \begin{cases} Q_n = 2Q_{n-1} + Q_{n-2}, \\ Q_0 = 2,\ Q_1 = 2. \end{cases} \tag{3.4}$$

- Pour $h(x) = a \in \mathbb{R}$ et $k(y) = b \in \mathbb{R}$, nous obtenons les suites de Lucas (voir [51]) définies, pour tout n dans $\mathbb{N}$, par

$$\begin{cases} U_n(a, b) = aU_{n-1}(a, b) + bU_{n-2}(a, b), \\ U_0 = 0,\ U_1 = 1 \end{cases} \text{ et } \begin{cases} V_n(a, b) = aV_{n-1(a,b)} + bV_{n-2}(a, b). \\ V_0 = 2,\ V_1 = a. \end{cases} \tag{3.5}$$

- Pour $h(x) = x$ et $k(y) = 1$, nous obtenons les polynômes de Fibonacci (appelés aussi polynômes de Catalan) et les polynômes de Lucas (voir [44]) : $U_n(x, y) = F_n(x)$ et $V_n(x, y) = L_n(x)$ définis, pour tout n dans $\mathbb{N}$, par

$$\begin{cases} F_n(x) = xF_{n-1}(x) + F_{n-2}(x), \\ F_0(x) = 0,\ F_1(x) = 1 \end{cases} \text{ et } \begin{cases} L_n(x) = xL_{n-1}(x) + L_{n-2}(x), \\ L_0(x) = 2,\ L_1(x) = x. \end{cases} \tag{3.6}$$

- Pour $h(x) = 1$ et $k(y) = y$, nous obtenons les polynômes de Jacobsthal [43] : $U_n(x, y) = J_n(y)$ définis, pour tout n dans $\mathbb{N}$, par

$$\begin{cases} J_n(y) = J_{n-1}(y) + yJ_{n-2}(y), \\ J_0(y) = 0,\ J_1(y) = 1. \end{cases} \tag{3.7}$$

- Pour $h(x) = 2x$ et $k(y) = 1$, nous obtenons les polynômes étudiés par Byrd [17] $U_n(x, y) = \varphi_n(x)$ définis, pour tout n dans $\mathbb{N}$, par

$$\begin{cases} \varphi_n(x) = 2x\varphi_{n-1}(x) + \varphi_{n-2}(x), \\ \varphi_0(x) = 0,\ \varphi_1(x) = 1. \end{cases} \tag{3.8}$$

- Le cas $k(y) = 1$ et h quelconque a été étudié par A. Nalli et P. Haukkanen [62].

3.2 Connexion entre les polynômes bivariés

Le résultat qui suit permet d'exprimer $U_n(x, y)$ en fonction des $V_n(x, y)$ et inversement. Il généralise les relations (2.6), (2.7), (2.8) et (2.9).

Théorème 3.1. *Pour tout $n \geq 1$, on a :*

$$V_n(x, y) = U_{n+1}(x, y) + k(y)U_{n-1}(x, y), \tag{3.9}$$

$$(h^2(x) + 4k(y))U_n(x, y) = V_{n+1}(x, y) + k(y)V_{n-1}(x, y). \tag{3.10}$$

Preuve. Les deux relations se démontrent par récurrence sur n. □

Comme conséquences, nous avons le corollaire suivant :

Corollaire 3.2.

$$\forall n \geq 1, \quad V_n(x,y) = h(x)U_n(x,y) + 2k(y)U_{n-1}(x,y). \tag{3.11}$$

$$\forall n \geq 0, \quad V_n(x,y) = 2U_{n+1}(x,y) - h(x)U_n(x,y). \tag{3.12}$$

$$\forall n \geq 1, \quad (h^2(x) + 4k(y))U_n(x,y) = h(x)V_n(x,y) + 2k(y)V_{n-1}(x,y). \tag{3.13}$$

$$\forall n \geq 0, \quad (h^2(x) + 4k(y))U_n(x,y) = 2V_{n+1}(x,y) - h(x)V_n(x,y). \tag{3.14}$$

Preuve. Les formules (3.11) et (3.12) sont des conséquences immédiates de (3.2) et (3.9).
Les formules (3.13) et (3.14) sont des conséquences immédiates de (3.1) et (3.10).

□

3.3 Séries génératrices

Soient $G_U(t) = \sum_{n=0}^{+\infty} U_n(x,y)t^n$ et $G_V(t) = \sum_{n=0}^{+\infty} V_n(x,y)t^n$ les fonctions génératrices des suites $U = (U_n(x,y))_n$ et $V = (V_n(x,y))_n$ respectivement. En utilisant les techniques standards de calculs, nous obtenons :

Théorème 3.3. *Les fonctions génératrices des suites $U = (U_n(x,y))_n$ et $V = (V_n(x,y))_n$ sont :*

$$G_U(t) = \frac{t}{1 - h(x)t - k(y)t^2} \tag{3.15}$$

et

$$G_V(t) = \frac{2 - h(x)t}{1 - h(x)t - k(y)t^2}. \tag{3.16}$$

A l'aide de ces fonctions génératrices nous déduisons le résultat suivant :

Théorème 3.4. *Si h est un polynôme impair alors pour tout $n \geq 0$,*

$$U_n(-x,y) = (-1)^{n+1}U_n(x,y), \tag{3.17}$$

$$V_n(-x,y) = (-1)^n V_n(x,y). \tag{3.18}$$

Preuve. A partir de (3.15), nous avons

$$\sum_{n=0}^{+\infty} U_n(-x,y)(-t)^n = \frac{-t}{1 - h(x)t - k(y)t^2}.$$

Par suite

$$\sum_{n=0}^{+\infty} (-1)^{n+1}U_n(-x,y)t^n = \sum_{n=0}^{+\infty} U_n(x,y)t^n.$$

Nous déduisons alors l'équation (3.17).

L'équation (3.18) se démontre de la même manière. □

3.4 Formules de Binet

Les suites définies par (3.1) et (3.2) ont pour polynôme caractéristique :

$$f(t) = t^2 - h(x)t - k(y)$$

de discriminant $\Delta = h^2(x) + 4k(y)$.

Soit $\overline{K}$ une clôture algébrique du corps des fractions $K = \mathbb{R}(x, y)$ de l'anneau des polynômes $\mathbb{R}[x, y]$.

Désignons par $\sqrt{\Delta}$ une racine du polynôme $t^2 - \Delta$ de $K[t]$ dans $\overline{K}$.

Le polynôme f admet pour racines

$$\alpha(x, y) = \frac{h(x) + \sqrt{\Delta}}{2}$$

et

$$\beta(x, y) = \frac{h(x) - \sqrt{\Delta}}{2}.$$

Théorème 3.5. *Pour $n \geq 0$, on a*

1. *Si $\Delta = 0$ alors*

$$U_n(x, y) = n \left(\frac{h(x)}{2}\right)^{n-1}, \tag{3.19}$$

$$V_n(x, y) = 2 \left(\frac{h(x)}{2}\right)^{n}. \tag{3.20}$$

2. *Si $\Delta \neq 0$ alors*

$$U_n(x, y) = \frac{\alpha^n(x, y) - \beta^n(x, y)}{\alpha(x, y) - \beta(x, y)}, \tag{3.21}$$

$$V_n(x, y) = \alpha^n(x, y) + \beta^n(x, y). \tag{3.22}$$

Preuve. Pour établir la preuve de ce théorème, nous allons suivre la méthode de détermination du terme général d'une suite récurrente linéaire décrite dans le chapitre 1 et que nous avons prise de l'article de Mignotte [19].

1. Si $\Delta = 0$ alors $\alpha(x) = \dfrac{h(x)}{2}$ est racine double de f.

   La série génératrice de $U = (U_n(x, y))_n$ est

$$G_U(t) = \frac{t}{1 - h(x)t + \dfrac{h^2(x)}{4}t^2} = \frac{A(t)}{B(t)},$$

avec $B(t) = 1 - h(x)t + \dfrac{h^2(x)}{4}\ t^2 = \ t^2\ f\left(\dfrac{1}{t}\right) = \dfrac{h^2(x)}{4}\ (t-\omega)^2$ où $\omega = \dfrac{1}{\alpha(x)}$.

La décomposition de la fraction rationnelle $\dfrac{A(t)}{B(t)}$ en éléments simples donne

$$\frac{A(t)}{B(t)} = \frac{\lambda}{t-\omega} + \frac{\mu}{(t-\omega)^2},$$

avec $\lambda = \dfrac{1}{\alpha^2(x)} \in \mathbb{R}(x)$ et $\mu = \dfrac{1}{\alpha^3(x)} \in \mathbb{R}(x)$.

L'identité formelle

$$\frac{1}{(X-\omega)^j} = (-1)^j \omega^{-j} \sum_{n\geq 0} \binom{n+j-1}{j-1} (X\omega^{-1})^n, \tag{3.23}$$

où j est dans $\mathbb{N}^*$, entraîne

$$\sum_{n\geq 0} U_n(x,y)t^n = \sum_{n\geq 0} (-\lambda\alpha^{n+1}(x) + (n+1)\mu\alpha^{n+2}(x))t^n.$$

D'où l'on déduit que, pour tout $n \geq 0$,

$$U_n(x,y) = ((n+1)\mu\alpha(x) - \lambda)\alpha^{n+1}(x) = n\left(\frac{h(x)}{2}\right)^{n-1}.$$

2. Si $\Delta \neq 0$ alors $\alpha(x,y)$ et $\beta(x,y)$ sont les racines distinctes de f. La série génératrice de $(U_n(x,y))_n$ est une fraction rationnelle $\dfrac{A(t)}{B(t)}$ avec

$$B(t) = 1 - h(x)t - k(y)t^2 = t^2 f(\frac{1}{t}) = -b(t-\omega_1)(t-\omega_2),$$

où $\omega_1 = \dfrac{1}{\alpha(x,y)} \in K$ et $\omega_2 = \dfrac{1}{\beta(x,y)} \in K$.

La décomposition en éléments simples de $\dfrac{A(t)}{B(t)}$ donne

$$\frac{A(t)}{B(t)} = \frac{\lambda}{t-w_1} + \frac{\mu}{t-w_2},$$

avec $\lambda = \dfrac{1}{\alpha(x,y)(\beta(x,y)-\alpha(x,y))} \in \overline{K}$ et $\mu = \dfrac{1}{\beta(x,y)(\alpha(x,y)-\beta(x,y))} \in \overline{K}$.

En utilisant l'identité (3.23), on obtient

$$\sum_{n\geq 0} U_n(x,y)t^n = -\sum_{n\geq 0} (-\lambda\alpha^{n+1}(x,y) + \mu\beta^{n+1}(x,y))t^n.$$

D'où l'on déduit que, pour tout $n \geq 0$,

$$U_n(x,y) = -(\lambda\alpha^{n+1}(x,y) + \mu\beta^{n+1}(x,y)) = \frac{\alpha^n(x,y) - \beta^n(x,y)}{\alpha(x,y) - \beta(x,y)}.$$

Les formules (3.20) et (3.22) s'obtiennent de manière analogue.

□

Le corollaire suivant, découle immédiatement du théorème 3.5.

Corollaire 3.6. *Pour tout entier $n \geq 0$,*

$$\alpha^n(x,y) = \frac{V_n(x,y) + \sqrt{h^2(x)+4k(y)}U_n(x,y)}{2}, \tag{3.24}$$

$$\beta^n(x,y) = \frac{V_n(x,y) - \sqrt{h^2(x)+4k(y)}U_n(x,y)}{2}. \tag{3.25}$$

Une autre conséquence du théorème 3.5 est :

Corollaire 3.7. *Pour tout entier $n \geq 0$,*

$$V_n^2(x,y) - \left[h^2(x)+4k(y)\right] U_n^2(x,y) = 4(-1)^n k^n(y), \tag{3.26}$$

$$U_{2n}(x,y) = V_n(x,y)U_n(x,y). \tag{3.27}$$

Preuve. Les formules sont vraies pour $\Delta = 0$.

Pour $\Delta \neq 0$, posons $\theta(x,y) = \dfrac{1}{\alpha(x,y)-\beta(x,y)}$.

Des équations

$$\alpha^n(x,y)\beta^n(x,y) = \frac{V_n^2(x,y) - [h^2(x)+4k(y)]\,U_n^2(x,y)}{4}$$

et

$$\alpha(x,y)\beta(x,y) = -k(y),$$

nous obtenons l'identité (3.26).

Preuve de (3.27).

Grâce au théorème 3.5, nous avons

$$\begin{aligned} U_n(x,y)V_n(x,y) &= \theta(x,y)\left[\alpha^n(x,y) - \beta^n(x,y)\right]\left[\alpha^n(x,y) + \beta^n(x,y)\right]. \\ &= \theta(x,y)\left[\alpha^{2n}(x,y) - \beta^{2n}(x,y)\right]. \\ &= U_{2n}(x,y). \end{aligned}$$

□

Lorsque $\Delta \neq 0$, nous avons l'identité suivante qui généralise l'identité (3.27) :

Corollaire 3.8. *Si $\Delta \neq 0$ alors, pour tous entiers n, m tels que $m \geq n$, on a :*

$$U_{n+m}(x,y) = V_n(x,y)\ U_m(x,y) + (-1)^{n+1}k^n(y)U_{m-n}(x,y).$$

Preuve. Nous avons $\alpha(x,y)\ \beta(x,y) = -k(y)$. D'après les formules de Binet

$$\begin{aligned} V_n\ U_m + (-1)^{n+1}k^n U_{m-n} &= \theta\ [(\alpha^n+\beta^n)(\alpha^m-\beta^m) + (-1)^{n+1}k^n(\alpha^{m-n}-\beta^{m-n})] \\ &= \theta\ (\alpha^{n+m} - \alpha^n\beta^m + \alpha^m\beta^n - \beta^{n+m} + (-1)^{n+1}k^n\alpha^{m-n} - (-1)^{n+1}k^n\beta^{m-n}) \\ &= \theta\ (\alpha^{n+m} - (-1)^n k^n\beta^{m-n} + (-1)^n k^n\alpha^{m-n} - \beta^{n+m} - (-1)^n k^n\alpha^{m-n} + \\ &\qquad (-1)^n k^n\beta^{m-n}). \\ &= \theta\ (\alpha^{n+m} - \beta^{n+m}). \\ &= U_{n+m}. \end{aligned}$$

□

3.5 Formules explicites

Il s'agit dans ce paragraphe, d'exprimer le terme général des suites $(U_n(x,y))_n$ et $(V_n(x,y))_n$ en fonction de n.

Théorème 3.9. *Pour tout entier $n \geq 0$,*

$$U_{n+1}(x,y) = \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n-j}{j} h^{n-2j}(x)k^j(y), \tag{3.28}$$

$$V_n(x,y) = \sum_{j=0}^{\lfloor n/2 \rfloor} \frac{n}{n-j}\binom{n-j}{j} h^{n-2j}(x)k^j(y). \tag{3.29}$$

Preuve. Les formules sont vraies pour $n = 1$ et $n = 2$, supposons, par récurrence, qu'elles soient vraies pour n, $(n \geq 2)$. Nous avons

$$\begin{aligned} U_{n+1}(x,y) &= h(x)\sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n-i-1}{i} h^{n-2i-1}(x)k^i(y) + k(y)\sum_{i=0}^{\lfloor \frac{n-2}{2} \rfloor} \binom{n-i-2}{i} h^{n-2i-2}(x)k^i(y), \\ &= \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n-i-1}{i} h^{n-2i}(x)k^i(y) + \sum_{i=0}^{\lfloor \frac{n-2}{2} \rfloor} \binom{n-i-2}{i} h^{n-2i-2}(x)k^{i+1}(y). \end{aligned}$$

Posons $j = i+1$, nous obtenons

$$U_{n+1}(x,y) = \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n-i-1}{i} h^{n-2i}(x)k^i(y) + \sum_{j=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n-j-1}{j-1} h^{n-2j}(x)k^j(y).$$

Si n est impair alors

$$\begin{aligned}U_{n+1}(x,y) &= \binom{n-1}{0}h^n(x)k^0(y) + \sum_{i=1}^{\lfloor\frac{n-1}{2}\rfloor}\left[\binom{n-i-1}{i}+\binom{n-i-1}{i-1}\right]h^{n-2i}(x)k^i(y).\\ &= \binom{n}{0}h^n(x)k^0(y) + \sum_{i=1}^{\lfloor\frac{n-1}{2}\rfloor}\binom{n-i}{i}h^{n-2i}(x)k^i(y).\\ &= \sum_{i=0}^{\lfloor\frac{n}{2}\rfloor}\binom{n-i}{i}h^{n-2i}(x)k^i(y).\end{aligned}$$

Si n est pair alors

$$\begin{aligned}U_{n+1}(x,y) &= \binom{n-1}{0}h^n(x)k^0(y) + \binom{n-1-\frac{n}{2}}{\frac{n}{2}-1}h^0(x)k^{n-\frac{n}{2}}(y)+\\ &\qquad \sum_{i=1}^{\lfloor\frac{n-2}{2}\rfloor}\left[\binom{n-i-1}{i}+\binom{n-i-1}{i-1}\right]h^{n-2i}(x)k^i(y).\\ &= \binom{n}{0}h^n(x)k^0(y) + \binom{\frac{n}{2}}{\frac{n}{2}}h^0(x)k^{n-\frac{n}{2}}(y) + \sum_{i=1}^{\lfloor\frac{n-2}{2}\rfloor}\binom{n-i}{i}h^{n-2i}(x)k^i(y).\\ &= \sum_{i=0}^{\lfloor\frac{n}{2}\rfloor}\binom{n-i}{i}h^{n-2i}(x)k^i(y).\end{aligned}$$

La preuve de (3.29) se fait de la même manière. □

Théorème 3.10. *Pour $n \geq 0$ et $h^2(x)+4k(y) \neq 0$, on a*

$$U_{n+1}(x,y) = \frac{1}{2^n}\sum_{j=0}^{\lfloor\frac{n}{2}\rfloor}\binom{n+1}{2j+1}h^{n-2j}(x)\left[h^2(x)+4k(y)\right]^j, \tag{3.30}$$

$$V_n(x,y) = \frac{1}{2^{n-1}}\sum_{j=0}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{2j}h^{n-2j}(x)\left[h^2(x)+4k(y)\right]^j. \tag{3.31}$$

Preuve. Nous avons

$$\alpha^{n+1}(x,y)-\beta^{n+1}(x,y) = 2^{-n-1}\left[\left(h(x)+\sqrt{h^2(x)+4k(y)}\right)^{n+1} - \left(h(x)-\sqrt{h^2(x)+4k(y)}\right)^{n+1}\right].$$

En utilisant la formule du binôme

$$\alpha^{n+1}(x,y)-\beta^{n+1}(x,y) = 2^{-n}\sum_{i=0,\ i\text{ impair}}^{n+1}\binom{n+1}{i}h^{n+1-i}(x)\sqrt{h^2(x)+4k(y)}\left(h^2(x)+4k(y)\right)^{\frac{i}{2}}.$$

Posons $i = 2j+1$. Grâce au théorème (3.5), nous obtenons (3.30).

Nous procédons de même pour (3.31). □

3.6 Lien avec les polynômes de Chebyshev

Soient T_n et W_n les polynômes de degré n, définis par

$$T_n(t) = \frac{n}{2} \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \frac{(-1)^j}{n-j} \binom{n-j}{j} (2t)^{n-2j},$$

$$W_n(t) = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^j \binom{n-j}{j} (2t)^{n-2j}.$$

Ils sont appelés, respectivement, les polynômes de Chebyshev de première et seconde espèce, auxquels nous avons consacré le chapitre 4.

Théorème 3.11. *Pour $n \geq 1$,*

$$U_{n+1}(x,y) = i^n \left(\sqrt{k(y)}\right)^n \; W_n\left(\frac{h(x)}{2i\sqrt{k(y)}}\right), \tag{3.32}$$

$$V_n(x,y) = 2i^n \left(\sqrt{k(y)}\right)^n \; T_n\left(\frac{h(x)}{2i\sqrt{k(y)}}\right), \tag{3.33}$$

avec $i^2 = -1$.

Preuve. Comme nous le verrons au chapitre 4, les séries génératrices des polynômes de Chebyshev sont

$$\sum_{n\geq 0} W_n(t) z^n = \frac{1}{1-2tz+z^2}$$

et

$$\sum_{n\geq 0} T_n(t) z^n = \frac{1-tz}{1-2tz+z^2}.$$

Dans $\overline{K}$, posons $z = i\sqrt{k(y)}\; s$ et $t = \dfrac{h(x)}{2i\sqrt{k(y)}}$, nous avons

$$\sum_{n\geq 0} i^n (\sqrt{k(y)})^n \; W_n\left(\frac{h(x)}{2i\sqrt{k(y)}}\right) s^n = \frac{1}{1-h(x)s-k(y)s^2},$$

ou encore

$$\sum_{n\geq 0} i^n (\sqrt{k(y)})^n \; W_n\left(\frac{h(x)}{2i\sqrt{k(y)}}\right) s^n = \sum_{n\geq 0} U_n(x,y) s^n.$$

D'où (3.32). De la même manière

$$\begin{aligned}\sum_{n=0}^{+\infty} i^n (\sqrt{k(y)})^n T_n\left(\frac{h(x)}{2i\sqrt{k(y)}}\right) s^n &= \frac{1-\frac{1}{2}h(x)s}{1-h(x)s-k(y)s^2},\\ &= \frac{1}{2}\,\frac{2-h(x)s}{1-h(x)s-k(y)s^2},\\ &= \frac{1}{2}\sum_{n=0}^{+\infty} V_n(x,y)s^n.\end{aligned}$$

□

3.7 Représentation par les déterminants

Pour $n \geq 1$, considérons les deux déterminants d'ordre n suivants

$$D_n(x,y) := \begin{vmatrix} 1 & ik(y) & 0 & \cdots & & 0 \\ 0 & h(x) & ik(y) & \cdots & & 0 \\ 0 & i & h(x) & \cdots & & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ & & & & & ik(y) \\ 0 & 0 & 0 & & i & h(x) \end{vmatrix},$$

et

$$E_n(x,y) := \begin{vmatrix} 2 & ik(y) & 0 & \cdots & & 0 \\ 0 & \frac{h(x)}{2} & ik(y) & \cdots & & 0 \\ 0 & i & h(x) & \cdots & & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ & & & & & ik(y) \\ 0 & 0 & 0 & & i & h(x) \end{vmatrix},$$

où $i^2 = -1$.

Théorème 3.12. *Pour $n \geq 1$,*

$$D_n(x,y) = U_n(x,y), \tag{3.34}$$

et

$$E_n(x,y) = V_{n-1}(x,y). \tag{3.35}$$

Preuve. Il est clair que (3.34) est vraie pour $n = 1$. Supposons, par récurrence, que c'est le cas jusqu'à $n-1$. Nous avons alors

$$\begin{aligned}D_n(x,y) &= h(x)D_{n-1}(x,y) - i^2k(y)D_{n-2}(x,y),\\ &= h(x)U_{n-1}(x,y) + k(y)U_{n-2}(x,y),\\ &= U_n(x,y).\end{aligned}$$

La relation (3.35) s'obtient par le même raisonnement en utilisant la relation

$$E_n(x,y) = h(x)D_{n-1}(x,y) + 2k(y)D_{n-2}.$$

□

3.8 Formules de Simpson

Soit $Q_{h,k}(x,y)$ la matrice 2×2 suivante :

$$\begin{pmatrix} h(x) & 1 \\ k(y) & 0 \end{pmatrix}$$

Théorème 3.13. *Pour $n \geq 1$,*

$$Q^n_{h,k}(x,y) = \begin{pmatrix} U_{n+1}(x,y) & U_n(x,y) \\ k(y)U_n(x,y) & k(y)U_{n-1}(x,y) \end{pmatrix}.$$

Preuve. Le résultat est vérifié pour $n = 1$. Suppose qu'il est vrai pour n, nous avons

$$\begin{aligned} Q^n_{h,k}(x,y)Q_{h,k}(x,y) &= \begin{pmatrix} h(x)U_{n+1}(x,y) + k(y)U_n(x,y) & U_{n+1}(x,y) \\ k(y)(h(x)U_n(x,y) + k(y)U_{n-1}(x,y)) & k(y)U_n(x,y) \end{pmatrix}, \\ &= \begin{pmatrix} U_{n+2}(x,y) & U_{n+1}(x,y) \\ k(y)U_{n+1}(x,y) & k(y)U_n(x,y) \end{pmatrix}, \\ &= Q^{n+1}_{h,k}(x,y). \end{aligned}$$

□

Comme conséquence directe du théorème 3.13 , nous avons les formules de Simpson :

Corollaire 3.14. *Pour $n \geq 1$,*

$$U_{n+1}(x,y)U_{n-1}(x,y) - U^2_n(x,y) = (-1)^n k^{n-1}(y), \tag{3.36}$$

et pour $n, m \geq 0$,

$$U_{m+n+1}(x,y) = U_{m+1}(x,y)U_{n+1}(x,y) + k(y)U_m(x,y)U_n(x,y). \tag{3.37}$$

En particulier

$$U_{2n+1}(x,y) = U^2_{n+1}(x,y) + k(y)U^2_n(x,y). \tag{3.38}$$

Preuve. D'un côté

$$\det Q_{h,k}(x,y) = -k(y),$$

donc

$$\det Q^n_{h,k}(x,y) = (-1)^n k^n(y).$$

D'un autre côté

$$\det Q_{h,k}^n(x,y) = k(y)U_{n+1}(x,y)U_{n-1}(x,y) - k(y)U_n^2(x,y).$$

D'où la formule (3.36).
La formule (3.37) découle de

$$Q_{h,k}^{m+n}(x,y) = Q_{h,k}^m(x,y)Q_{h,k}^n(x,y).$$

L'expression (3.38) s'obtient en posant $n = m$ dans (3.37). □

Le théorème suivant nous donne les valeurs propres de la matrice $Q_{h,k}^n(x,y)$.

Théorème 3.15. *Les racines du polynôme caractéristique de $Q_{h,k}^n(x,y)$ sont $\alpha^n(x,y)$ et $\beta^n(x,y)$.*

Preuve. Le polynôme caractéristique de la matrice $Q_{h,k}^n(x,y)$ est

$$\det(Q_{h,k}^n(x,y)-\lambda I_2) = \lambda^2-\lambda\left(U_{n+1}(x,y) + k(y)U_{n-1}(x,y)\right)+k(y)U_{n+1}(x,y)U_{n-1}(x,y)-k(y)U_n^2(x,y),$$

Par le théorème 3.1 et le corollaire 3.14, nous obtenons

$$\det(Q_{h,k}^n(x,y) - \lambda I_2) = \lambda^2 - \lambda V_n(x,y) + (-1)^n k^n(y)$$

dont les racines dans $\overline{K}$ sont

$$\lambda = \frac{1}{2}\left(V_n(x,y) \pm \sqrt{V_n^2(x,y) - 4(-1)^n k^n(y)}\right),$$

Il s'ensuit du corollaire 3.7 que,

$$\lambda = \frac{1}{2}\left(V_n(x,y) \pm \sqrt{h^2(x) + 4k(y)}\; U_n(x,y)\right).$$

Autrement dit, les racines du polynôme caractéristique de la matrice $Q_{h,k}^n(x,y)$ sont $\alpha^n(x,y)$ et $\beta^n(x,y)$ (voir corollaire 3.6). □

La démarche suivie dans cette section nous a permis d'avoir de nouvelles propriétés pour la suite $(U_n(x,y))_n$. Nous allons faire de même pour la suite $(V_n(x,y))_n$. Pour cela, considérons, pour tout $n \geq 1$, la matrice

$$M_n(x,y) = Q_{h,k}^{n-1}(x,y)\begin{pmatrix} h^2(x)+2k(y) & h(x) \\ h(x)k(y) & 2k(y) \end{pmatrix}.$$

Théorème 3.16. *Pour tout $n \geq 1$, on a*

$$M_n(x,y) = \begin{pmatrix} V_{n+1}(x,y) & V_n(x,y) \\ k(y)V_n(x,y) & k(y)V_{n-1}(x,y) \end{pmatrix}.$$

Preuve. Pour $n = 1$, nous avons

$$M_n(x,y) = Q_{h,k}^{n-1}(x,y) \begin{pmatrix} h^2(x)+2k(y) & h(x) \\ h(x)k(y) & 2k(y) \end{pmatrix} = \begin{pmatrix} V_2(x,y) & V_1(x,y) \\ kV_1(x,y) & kV_0(x,y) \end{pmatrix}.$$

Supposons, par récurrence, que la propriété est vraie jusqu'à n. Nous avons

$$\begin{aligned} M_{n+1}(x,y) &= Q_{h,k}^{1}(x,y)\, Q_{h,k}^{n-1}(x,y) \begin{pmatrix} h^2(x)+2k(y) & h(x) \\ h(x)k(y) & 2k(y) \end{pmatrix} \\ &= \begin{pmatrix} h(x) & 1 \\ k(y) & 0 \end{pmatrix} M_n \\ &= \begin{pmatrix} h(x) & 1 \\ k(y) & 0 \end{pmatrix} \begin{pmatrix} V_{n+1}(x,y) & V_n(x,y) \\ k(y)V_n(x,y) & k(y)V_{n-1}(x,y) \end{pmatrix} \\ &= \begin{pmatrix} h(x)V_{n+1}(x,y)+k(y)V_n(x,y) & h(x)V_n(x,y)+k(y)V_{n-1}(x,y) \\ k(y)V_{n+1}(x,y) & k(y)V_n(x,y) \end{pmatrix} \\ &= \begin{pmatrix} V_{n+2}(x,y) & V_{n+1}(x,y) \\ k(y)V_{n+1}(x,y) & k(y)V_n(x,y) \end{pmatrix}. \end{aligned}$$

□

Corollaire 3.17. *1. $\forall n \geq 1$, on a*

$$V_{n+1}(x,y)V_{n-1}(x,y) - V_n^2(x,y) = (-1)^{n-1}k(y)^{n-1}(h^2(x)+4k(y)). \tag{3.39}$$

2. $\forall n \geq 0,\ \forall m \geq 0$, on a

$$V_{n+m+1}(x,y) = U_{n+1}(x,y)V_{m+1}(x,y) + k(y)U_n(x,y)V_m(x,y). \tag{3.40}$$

En particulier

$$V_{2n+1}(x,y) = U_{n+1}(x,y)V_{n+1}(x,y) + k(y)U_n(x,y)V_n(x,y) \tag{3.41}$$

et

$$(h^2(x)+4k(y))V_{2n+1}(x,y) = h(x)V_{n+1}^2(x,y) - h(x)k(y)V_n^2(x,y) + 4k(y)V_{n+1}(x,y)V_n(x,y). \tag{3.42}$$

Preuve.

1. Pour $n \geq 1$, nous avons d'un côté

$$M_n(x,y) = Q_{h,k}^{n-1}(x,y) \begin{pmatrix} h^2(x)+2k(y) & h(x) \\ h(x)k(y) & 2k(y) \end{pmatrix}.$$

D'où

$$\det M_n(x,y) = (-1)^{n-1}k^n(h^2(x)+4k(y)).$$

D'un autre côté

$$M_n(x,y) = \begin{pmatrix} V_{n+1}(x,y) & V_n(x,y) \\ kV_n(x,y) & kV_{n-1}(x,y) \end{pmatrix}.$$

Par suite

$$\det M_n(x,y) = k(y)V_{n+1}(x,y)V_{n-1}(x,y) - k(y)V_n^2(x,y).$$

D'où la formule (3.39).

2. Nous avons

$$M_{n+(m-1)}(x,y) = Q_{h,k}^n(x,y)\ M_{m-1}(x,y).$$

La formule (3.40) s'obtient alors en utilisant les théorèmes (3.13) et (3.16).
L'expression (3.41) s'obtient en posant $m = n$ dans (3.40).
En lui associant la formule (3.10), nous obtenons (3.42).

□

Nous allons clore cette section par la détermination des valeurs propres de la matrice $M_n(x,y)$.

Théorème 3.18. *Les valeurs propres de la matrice $M_n(x,y)$ sont $\sqrt{h^2(x)+4k(y)}\ \alpha^n$ et $-\sqrt{h^2(x)+4k(y)}\ \beta^n$.*

Preuve. Le polynôme caractéristique de la matrice $M_n(x,y)$ est

$$P_{M_n(x,y)}(\lambda) = \lambda^2 - \lambda(k(y)V_{n-1}(x,y) + V_{n+1}(x,y)) + k(y)V_{n+1}(x,y)V_{n-1}(x,y) - k(y)V_n^2(x,y).$$

Grâce aux expressions (3.10) et (3.39), nous avons

$$P_{M_n(x,y)}(\lambda) = \lambda^2 - \lambda(h^2(x)+4k(y))U_n(x,y) + (-1)^{n-1}k^n(y)(h^2(x)+4k(y)).$$

Par le corollaire 3.7, le discriminant de ce polynôme est $(h^2(x)+4k(y))V_n^2(x,y)$.
Il s'ensuit du corollaire 3.6, que ses racines dans $\overline{K}$ sont $\sqrt{h^2(x)+4k(y)}\,\alpha^n$ et $-\sqrt{h^2(x)+4k(y)}\,\beta^n$.

□

3.9 Illustration

Nous allons, à présent, adapter les énoncés des propriétés obtenues dans cette étude aux suites classiques citées au début de ce chapitre.

1. **Propriétés de la suite de Fibonacci et de sa suite compagnon**
   Soient $F = (F_n)_n$ la suite de Fibonacci et $L = (L_n)_n$ sa suite compagnon définies par les relations (3.3).
   Pour tous entiers n et m nous avons :
   $5F_n = L_{n+1} + L_{n-1}$,
   $5F_n = L_n + 2L_{n-1}$,
   $5F_n = 2L_{n+1} - L_n$,
   $F_{2n} = F_n\ L_n$,
   $F_{n+m} = L_n F_m + (-1)^{n+1} F_{m-n}$,
   $L_n = F_{n+1} + F_{n-1}$,
   $L_n = F_n + 2F_{n-1}$,
   $L_n = 2F_{n+1} - F_n$,
   $L_n^2 - 5F_n^2 = 4(-1)^n$,
   $G_F(t) = \dfrac{t}{1-t-t^2}$ (série génératrice de la suite F),
   $G_L(t) = \dfrac{2-t}{1-t-t^2}$ (série génératrice de la suite L),
   $\sqrt{5}F_n = \left(\dfrac{1+\sqrt{5}}{2}\right)^n - \left(\dfrac{1-\sqrt{5}}{2}\right)^n$ (formule de Binet),
   $L_n = \left(\dfrac{1+\sqrt{5}}{2}\right)^n + \left(\dfrac{1-\sqrt{5}}{2}\right)^n$ (formule de Binet),
   $L_n + \sqrt{5}F_n = 2\ \left(\dfrac{1+\sqrt{5}}{2}\right)^n$,
   $L_n - \sqrt{5}F_n = 2\ \left(\dfrac{1-\sqrt{5}}{2}\right)^n$,
   $F_{n+1} = \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n-j}{j}$,
   $L_n = \sum_{j=0}^{\lfloor n/2 \rfloor} \dfrac{n}{n-j}\binom{n-j}{j}$,
   $F_{n+1} = \dfrac{1}{2^n} \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n+1}{2j+1} 5^j$,
   $L_n = \dfrac{1}{2^{n-1}} \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n}{2j} 5^j$,

$F_{n+1} = i^n W_n\left(\frac{1}{2i}\right)$ où $i^2 = -1$ et W_n est le n-ième polynôme de Chebyshev de seconde espèce,

$L_n = 2i^n T_n\left(\frac{1}{2i}\right)$ où $i^2 = -1$ et T_n est le n-ième polynôme de Chebyshev de première espèce,

$\begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} = Q^n$ où $Q = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$,

$F_{n+1}\ F_{n-1} - F_n^2 = (-1)^n$,

$F_{n+m+1} = F_{n+1}F_{m+1} + F_nF_m$,

$F_{2n+1} = F_{n+1}^2 + F_n^2$,

les racines du polynôme caractéristique de Q^n sont $\left(\frac{1 \pm \sqrt{5}}{2}\right)^n$,

$\begin{pmatrix} L_{n+1} & L_n \\ L_n & L_{n-1} \end{pmatrix} = M_n$ où $M_n = Q^{n-1}\begin{pmatrix} 5 & 1 \\ 1 & 2 \end{pmatrix}$,

$L_{n+1}\ L_{n-1} - L_n^2 = 5\ (-1)^{n-1}$,

$L_{n+m+1} = F_{n+1}L_{m+1} + F_nL_m$,

$L_{2n+1} = F_{n+1}L_{n+1} + F_nL_n$,

$5L_{2n+1} = L_{n+1}^2 - L_n^2 + 4L_{n+1}L_n$,

les racines du polynôme caractéristique de M_n sont $\sqrt{5}\left(\frac{1+\sqrt{5}}{2}\right)^n$ et $(-\sqrt{5})\left(\frac{1-\sqrt{5}}{2}\right)^n$.

2. **Propriétés de la suite des nombres de Pell et de sa suite compagnon**

Soient $P = (P_n)_n$ la suite des nombres de Pell et $Q = (Q_n)_n$ sa suite compagnon définies par les relations (3.4).

Pour tous entiers n et m nous avons :

$8P_n = Q_{n+1} + Q_{n-1}$,

$8P_n = 2Q_n + 2Q_{n-1}$,

$8P_n = 2Q_{n+1} - 2Q_n$,

$P_{2n} = P_n\ Q_n$,

$P_{n+m} = Q_nP_m + (-1)^{n+1}P_{m-n}$,

$Q_n = P_{n+1} + P_{n-1}$,

$Q_n = 2P_n + 2P_{n-1}$,

$Q_n = 2P_{n+1} - 2P_n$,

$Q_n^2 - 8P_n^2 = 4(-1)^n$,

$G_P(t) = \dfrac{t}{1-2t-t^2}$ (série génératrice de la suite P),

$G_Q(t) = \dfrac{2-2t}{1-2t-t^2}$ (série génératrice de la suite Q),

$\sqrt{8}P_n = (1+\sqrt{2})^n - (1-\sqrt{2})^n$ (formule de Binet),

$Q_n = (1+\sqrt{2})^n + (1-\sqrt{2})^n$ (formule de Binet),

$Q_n + \sqrt{8}P_n = 2\ (1+\sqrt{2})^n$,

$Q_n - \sqrt{8}P_n = 2\ (1-\sqrt{2})^n$,

$P_{n+1} = \displaystyle\sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n-j}{j}\ 2^{n-2j}$,

$Q_n = \displaystyle\sum_{j=0}^{\lfloor n/2 \rfloor} \frac{n}{n-j}\binom{n-j}{j}\ 2^{n-2j}$,

$P_{n+1} = \dfrac{1}{2^n}\ \displaystyle\sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n+1}{2j+1}\ 2^{n+j}$,

$Q_n = \dfrac{1}{2^{n-1}}\ \displaystyle\sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n}{2j}\ 2^{n+j}$,

$P_{n+1} = i^n W_n(-i)$ où $i^2 = -1$ et W_n est le n-ième polynôme de Chebyshev de seconde espèce,

$Q_n = 2i^n T_n(-i)$ où $i^2 = -1$ et T_n est le n-ième polynôme de Chebyshev de première espèce,

$\begin{pmatrix} P_{n+1} & P_n \\ P_n & P_{n-1} \end{pmatrix} = N^n$ où $N = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$,

$P_{n+1}\ P_{n-1} - P_n^2 = (-1)^n$,

$P_{n+m+1} = P_{n+1}P_{m+1} + P_nP_m$,

$P_{2n+1} = P_{n+1}^2 + P_n^2$,

les racines du polynôme caractéristique de N^n sont $(1 \pm \sqrt{2})^n$,

$\begin{pmatrix} Q_{n+1} & Q_n \\ Q_n & Q_{n-1} \end{pmatrix} = M_n$ où $M_n = N^{n-1}\ \begin{pmatrix} 6 & 2 \\ 2 & 2 \end{pmatrix}$,

$Q_{n+1}\ Q_{n-1} - Q_n^2 = 8\ (-1)^{n-1}$,

$Q_{n+m+1} = P_{n+1}Q_{m+1} + P_nQ_m$,

$Q_{2n+1} = P_{n+1}Q_{n+1} + P_nQ_n$,

$4Q_{2n+1} = Q_{n+1}^2 - Q_n^2 + 2Q_{n+1}Q_n$,

les racines du polynôme caractéristique de M_n sont $\sqrt{8}\ (1+\sqrt{2})^n$ et $(-\sqrt{8})\ (1-\sqrt{2})^n$.

3. **Propriétés des suites de Lucas**

Soient $U = (U_n(a,b))_n$ et $V = (V_n(a,b))_n$ les suites de Lucas définies par les relations (3.5) où a et b sont des réels non nuls. Pour alléger les écritures, nous noterons $U_n(a,b)$ par U_n et $V_n(a,b)$ par V_n.

Pour tous entiers n et m nous avons :

$(a^2+4b)U_n = V_{n+1} + V_{n-1}$,

$(a^2+4b)U_n = aV_n + 2bV_{n-1}$,

$(a^2+4b)U_n = 2V_{n+1} - aV_n$,

$U_{2n} = U_n\ V_n$,

$U_{n+m} = V_nU_m + (-1)^{n+1}b^nU_{m-n}$, à condition que $a^2+4b \neq 0$,

$V_n = U_{n+1} + bU_{n-1}$,

$V_n = aU_n + 2bU_{n-1}$,

$V_n = 2U_{n+1} - aU_n$,

$V_n^2 - (a^2+4b)U_n^2 = 4(-1)^nb^n$,

$U_n(-a,b) = (-1)^{n+1}U_n(a,b)$,

$V_n(-a,b) = (-1)^nV_n(a,b)$,

$G_U(t) = \dfrac{t}{1-at-bt^2}$ (série génératrice de la suite U),

$G_L(t) = \dfrac{2-at}{1-at-bt^2}$ (série génératrice de la suite V),

$U_n = n\left(\dfrac{a}{2}\right)^{n-1}$, lorsque $a^2+4b=0$,

$V_n = 2\left(\dfrac{a}{2}\right)^{n}$, lorsque $a^2+4b=0$,

$\sqrt{a^2+4b}U_n = \left(\dfrac{a+\sqrt{a^2+4b}}{2}\right)^n - \left(\dfrac{a-\sqrt{a^2+4b}}{2}\right)^n$, lorsque $a^2+4b \neq 0$,

$V_n = \left(\dfrac{a+\sqrt{a^2+4b}}{2}\right)^n + \left(\dfrac{a-\sqrt{a^2+4b}}{2}\right)^n$, lorsque $a^2+4b \neq 0$,

$V_n + \sqrt{a^2+4b}U_n = 2\ \left(\dfrac{a+\sqrt{a^2+4b}}{2}\right)^n$,

$V_n - \sqrt{a^2+4b}U_n = 2\ \left(\dfrac{a-\sqrt{a^2+4b}}{2}\right)^n$,

$U_{n+1} = \displaystyle\sum_{j=0}^{\lfloor n/2\rfloor} \binom{n-j}{j}\ a^{n-2j}\ b^j$,

$$V_n = \sum_{j=0}^{\lfloor n/2 \rfloor} \frac{n}{n-j} \binom{n-j}{j} \; a^{n-2j} \; b^j,$$

$$U_{n+1} = \frac{1}{2^n} \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n+1}{2j+1} \; a^{n-2j} \; (a^2+4b)^j, \quad \text{lorsque} \quad a^2+4b \neq 0,$$

$$V_n = \frac{1}{2^{n-1}} \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n}{2j} \; a^{n-2j} \; (a^2+4b)^j, \quad \text{lorsque} \quad a^2+4b \neq 0,$$

$U_{n+1} = i^n \; (\sqrt{b})^n \; W_n \left(\dfrac{a}{2i\sqrt{b}} \right)$ où $i^2 = -1$ et W_n est le n-ième polynôme de Chebyshev de seconde espèce,

$V_n = 2 \; i^n \; (\sqrt{b})^n \; T_n \left(\dfrac{a}{2i\sqrt{b}} \right)$ où $i^2 = -1$ et T_n est le n-ième polynôme de Chebyshev de première espèce,

$$\begin{pmatrix} U_{n+1} & U_n \\ bU_n & bU_{n-1} \end{pmatrix} = Q^n \quad \text{où } Q = \begin{pmatrix} a & 1 \\ b & 0 \end{pmatrix},$$

$U_{n+1} \; U_{n-1} - U_n^2 = (-1)^n \; b^{n-1},$

$U_{n+m+1} = U_{n+1}U_{m+1} + bU_nU_m,$

$U_{2n+1} = U_{n+1}^2 + bU_n^2,$

les racines du polynôme caractéristique de Q^n sont $\left(\dfrac{a \pm \sqrt{a^2+4b}}{2} \right)^n$,

$$\begin{pmatrix} V_{n+1} & V_n \\ bV_n & bV_{n-1} \end{pmatrix} = M_n \quad \text{où } M_n = Q^{n-1} \begin{pmatrix} a^2+2b & a \\ ab & 2b \end{pmatrix},$$

$V_{n+1} \; V_{n-1} - V_n^2 = (-1)^{n-1} \; b^{n-1} \; (a^2+4b),$

$V_{n+m+1} = U_{n+1}V_{m+1} + bU_nV_m,$

$V_{2n+1} = U_{n+1}V_{n+1} + bU_nV_n,$

$(a^2+4b)V_{2n+1} = aV_{n+1}^2 - abV_n^2 + 4bV_{n+1}V_n,$

les racines du polynôme caractéristique de M_n sont $\sqrt{a^2+4b} \left(\dfrac{a+\sqrt{a^2+4b}}{2} \right)^n$ et $(-\sqrt{a^2+4b}) \left(\dfrac{a-\sqrt{a^2+4b}}{2} \right)^n$.

4. **Propriétés de la suite des polynômes de Catalan et des polynômes de Lucas**
   Soient $F = (F_n(x))_n$ la suite des polynômes de Fibonacci (ou de Catalan) et $L = (L_n(x))_n$ la suite des polynômes de Lucas définies par les relations (3.6).
   Pour tous entiers n et m nous avons :
   $(x^2+4)F_n(x) = L_{n+1}(x) + L_{n-1}(x),$

$(x^2+4)F_n(x) = xL_n(x) + 2L_{n-1}(x)$,

$(x^2+4)F_n(x) = 2L_{n+1}(x) - xL_n(x)$,

$F_{2n}(x) = F_n(x)\ L_n(x)$,

$F_{n+m}(x) = L_n(x)F_m(x) + (-1)^{n+1}F_{m-n}(x)$,

$L_n(x) = F_{n+1}(x) + F_{n-1}(x)$,

$L_n(x) = xF_n(x) + 2F_{n-1}(x)$,

$L_n(x) = 2F_{n+1}(x) - xF_n(x)$,

$L_n^2(x) - (x^2+4)F_n^2(x) = 4(-1)^n$,

$F_n(-x) = (-1)^{n+1}F_n(x)$,

$L_n(-x) = (-1)^n L_n(x)$,

$G_F(t) = \dfrac{t}{1-xt-t^2}$ (série génératrice de la suite F),

$G_L(t) = \dfrac{2-xt}{1-xt-t^2}$ (série génératrice de la suite L),

$\sqrt{x^2+4}F_n(x) = \left(\dfrac{x+\sqrt{x^2+4}}{2}\right)^n - \left(\dfrac{x-\sqrt{x^2+4}}{2}\right)^n$ (formule de Binet),

$L_n(x) = \left(\dfrac{x+\sqrt{x^2+4}}{2}\right)^n + \left(\dfrac{x-\sqrt{x^2+4}}{2}\right)^n$ (formule de Binet),

$L_n(x) + \sqrt{x^2+4}F_n(x) = 2\ \left(\dfrac{x+\sqrt{x^2+4}}{2}\right)^n$,

$L_n(x) - \sqrt{x^2+4}F_n(x) = 2\ \left(\dfrac{x-\sqrt{x^2+4}}{2}\right)^n$,

$F_{n+1}(x) = \sum_{j=0}^{\lfloor n/2\rfloor} \binom{n-j}{j} x^{n-2j}$,

$L_n(x) = \sum_{j=0}^{\lfloor n/2\rfloor} \dfrac{n}{n-k}\binom{n-j}{j} x^{n-2j}$,

$F_{n+1}(x) = \dfrac{1}{2^n} \sum_{j=0}^{\lfloor n/2\rfloor} \binom{n+1}{2j+1} x^{n-2j}(x^2+4)^j$,

$L_n(x) = \dfrac{1}{2^{n-1}} \sum_{j=0}^{\lfloor n/2\rfloor} \binom{n}{2j} x^{n-2j}(x^2+4)^j$,

$F_{n+1}(x) = i^n W_n\left(\dfrac{x}{2i}\right)$ où $i^2 = -1$ et W_n est le n-ième polynôme de Chebyshev de seconde espèce,

$L_n(x) = 2i^n T_n\left(\frac{x}{2i}\right)$ où $i^2 = -1$ et T_n est le n-ième polynôme de Chebyshev de première espèce,

$\begin{pmatrix} F_{n+1}(x) & F_n(x) \\ F_n(x) & F_{n-1}(x) \end{pmatrix} = Q^n$ où $Q = \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}$,

$F_{n+1}(x)\ F_{n-1}(x) - F_n^2(x) = (-1)^n$,

$F_{n+m+1}(x) = F_{n+1}(x)F_{m+1}(x) + F_n(x)F_m(x)$,

$F_{2n+1}(x) = F_{n+1}^2(x) + F_n^2(x)$,

les racines du polynôme caractéristique de Q^n sont $\left(\frac{x \pm \sqrt{x^2+4}}{2}\right)^n$,

$\begin{pmatrix} L_{n+1}(x) & L_n(x) \\ L_n(x) & L_{n-1}(x) \end{pmatrix} = M_n$ où $M_n = Q^{n-1} \begin{pmatrix} x^2+2 & x \\ x & 2 \end{pmatrix}$,

$L_{n+1}(x)\ L_{n-1}(x) - L_n^2(x) = (-1)^{n-1}(x^2+4)$,

$L_{n+m+1}(x) = F_{n+1}(x)L_{m+1}(x) + F_n(x)L_m(x)$,

$L_{2n+1}(x) = F_{n+1}(x)L_{n+1}(x) + F_n(x)L_n(x)$,

$(x^2+4)L_{2n+1}(x) = xL_{n+1}^2(x) - xL_n^2(x) + 4L_{n+1}(x)L_n(x)$,

les racines du polynôme caractéristique de M_n sont $\sqrt{x^2+4}\ \left(\frac{x+\sqrt{x^2+4}}{2}\right)^n$ et

$(-\sqrt{x^2+4})\ \left(\frac{x-\sqrt{x^2+4}}{2}\right)^n$.

5. **Propriétés de la suite des polynômes de Jacobsthal**

Soit $J = (J_n(y))_n$ la suite des polynômes de Jacobsthal définies par la relation (3.7) et soit $I = (I_n(y))_n$ sa suite compagnon. La suite I vérifie la même relation de récurrence que la suite J avec pour premiers termes $I_0(y) = 2$ et $I_1(y) = 1$. Pour alléger les écritures, nous noterons $J_n(y)$ par J_n et $I_n(y)$ par I_n.

Pour tous entiers n et m nous avons :

$(1+4y)J_n = I_{n+1} + I_{n-1}$,

$(1+4y)J_n = I_n + 2yI_{n-1}$,

$(1+4y)J_n = 2I_{n+1} - I_n$,

$J_{2n} = J_n\ I_n$,

$I_n = J_{n+1} + yJ_{n-1}$,

$I_n = J_n + 2yJ_{n-1}$,

$I_n = 2J_{n+1} - J_n$,

$I_n^2 - (1+4y)J_n^2 = 4(-1)^n y^n$,

$G_J(t) = \dfrac{t}{1-t-yt^2}$ (série génératrice de la suite U),

$G_I(t) = \dfrac{2-t}{1-t-yt^2}$ (série génératrice de la suite V),

$J_n = n\left(\dfrac{1}{2}\right)^{n-1}$, lorsque $1+4y=0$,

$I_n = 2\left(\dfrac{1}{2}\right)^{n}$, lorsque $1+4y=0$,

$\sqrt{1+4y}J_n = \left(\dfrac{1+\sqrt{1+4y}}{2}\right)^n - \left(\dfrac{1-\sqrt{1+4y}}{2}\right)^n$, lorsque $1+4y\neq 0$,

$I_n = \left(\dfrac{1+\sqrt{1+4y}}{2}\right)^n + \left(\dfrac{1-\sqrt{1+4y}}{2}\right)^n$, lorsque $1+4y\neq 0$,

$I_n + \sqrt{1+4y}J_n = 2\left(\dfrac{1+\sqrt{1+4y}}{2}\right)^n$,

$I_n - \sqrt{1+4y}J_n = 2\left(\dfrac{1-\sqrt{1+4y}}{2}\right)^n$,

$J_{n+1} = \displaystyle\sum_{j=0}^{\lfloor n/2\rfloor}\binom{n-j}{j}y^j$,

$I_n = \displaystyle\sum_{j=0}^{\lfloor n/2\rfloor}\frac{n}{n-j}\binom{n-j}{j}y^j$,

$J_{n+1} = \dfrac{1}{2^n}\displaystyle\sum_{j=0}^{\lfloor n/2\rfloor}\binom{n+1}{2j+1}(1+4y)^j$, lorsque $1+4y\neq 0$,

$I_n = \dfrac{1}{2^{n-1}}\displaystyle\sum_{j=0}^{\lfloor n/2\rfloor}\binom{n}{2j}(1+4y)^j$, lorsque $1+4y\neq 0$,

$J_{n+1} = i^n\,(\sqrt{y})^n\,W_n\left(\dfrac{1}{2i\sqrt{y}}\right)$ où $i^2=-1$ et W_n est le n-ième polynôme de Chebyshev de seconde espèce,

$I_n = 2\,i^n\,(\sqrt{y})^n\,T_n\left(\dfrac{1}{2i\sqrt{y}}\right)$ où $i^2=-1$ et T_n est le n-ième polynôme de Chebyshev de première espèce,

$\begin{pmatrix} J_{n+1} & J_n \\ yJ_n & yJ_{n-1}\end{pmatrix} = Q^n$ où $Q = \begin{pmatrix} 1 & 1 \\ y & 0\end{pmatrix}$,

$J_{n+1}\,J_{n-1} - J_n^2 = (-1)^n\,y^{n-1}$,

$J_{n+m+1} = J_{n+1}J_{m+1} + yJ_nJ_m$,

$J_{2n+1} = J_{n+1}^2 + yJ_n^2$,

les racines du polynôme caractéristique de Q^n sont $\left(\frac{1 \pm \sqrt{1+4y}}{2}\right)^n$,

$\begin{pmatrix} I_{n+1} & I_n \\ yI_n & yI_{n-1} \end{pmatrix} = M_n$ où $M_n = Q^{n-1} \begin{pmatrix} 1+2y & 1 \\ y & 2y \end{pmatrix}$,

$I_{n+1}\ I_{n-1} - I_n^2 = (-1)^{n-1}\ y^{n-1}\ (1+4y)$,

$I_{n+m+1} = I_{n+1}J_{m+1} + yJ_nI_m$,

$I_{2n+1} = J_{n+1}I_{n+1} + yJ_nI_n$,

$(1+4y)I_{2n+1} = I_{n+1}^2 - yI_n^2 + 4yI_{n+1}I_n$,

les racines du polynôme caractéristique de M_n sont $\sqrt{1+4y}\left(\frac{1+\sqrt{1+4y}}{2}\right)^n$ et $(-\sqrt{1+4y})\left(\frac{1-\sqrt{1+4y}}{2}\right)^n$.

Chapitre 4

Polynômes de Chebyshev généralisés

4.1 Introduction

Les n-ème polynômes de Chebyshev de première et seconde espèce sont respectivement définis, pour tout n dans $\mathbb{N}$, par les relations de récurrence de second ordre suivantes :

$$T_n = 2XT_{n-1} - T_{n-2} \quad \text{avec } T_0 = 1 \text{ et } T_1 = X, \tag{4.1}$$

$$U_n = 2XU_{n-1} - U_{n-2} \quad \text{avec } U_0 = 1 \text{ et } U_1 = 2X. \tag{4.2}$$

Ce sont, voir [11], les uniques polynômes à coefficients entiers satisfaisant, pour $n \in \mathbb{N}$ et $X \in \mathbb{R}$, aux identités

$$cosnX = T_n(cosX) \text{ et } sin((n+1)X) = sinX\ U_n(cosX). \tag{4.3}$$

Les relations (4.1) et (4.2) découlent de ces dernières équations et des formules de Simpson

$$\begin{array}{rcl} cos\ nX & = & 2cos\ X\ cos\ (n-1)X - cos\ (n-2)X \\ sin\ (n+1)X & = & 2cos\ X\ sin\ nX - sin\ (n-1)X \end{array}$$

Remarque 4.1. *Dans [20], Cesarano définit les polynômes de Chebyshev de première espèce par la relation*

$$T_n(X) = cos\ (n\ arccos\ (X))$$

et ceux de seconde espèce par

$$U_n(X) = \frac{sin\ [(n+1)arccos\ (X)]}{\sqrt{1-X^2}}.$$

Pour l'étude des propriétes de ces polynômes, il introduit la fonction complexe à variable réelle X définie par

$$f_n(X) = exp(i\ n\ arcos(X))$$

dont la partie réelle est justement $T_n(X)$ et la partie imaginaire est $\sqrt{1-X^2}\ U_{n-1}(X)$.

Cette définition des polynômes de Chebyshev est bien évidemment équivalente à la première.

Les polynômes de Chebyshev sont appelés ainsi en l'honneur au mathématicien russe Pafnouti Lvovitch Chebyshev $(1821-1894)$. Ils sont particulièrement utiles en analyse numériques pour l'interpolation polynomiale des fonctions. Chebyshev a découvert cette famille de polynômes en travaillant, justement, sur le problème de convergence des interpolations de Lagrange. Il y montre que les racines de ces polynômes, appelées les abscisses de Chebyshev, sont les meilleurs points d'interpolation pour obtenir les meilleures convergences possibles.

Les polynômes de Chebyshev ont servi également à démontrer le théorème d'approximation de Weierstrass selon lequel toute fonction continue sur un intervalle est limite uniforme d'une suite de fonctions polynomiales.

On les retrouve aussi en électricité dans le cadre des filtres (en bande passante et en bande atténuée).

Pour des détails concernant leurs définitions, propriétés et utilisations (surtout en analyse numérique), les lecteurs sont invités à consulter, entre autres, le livre de T. J. Rivlin [67] et celui de J. C. Mason et D. C. Handscomb [56].

4.2 Séries génératrices

Les séries formelles $G_{T_n}(t) = \sum_{n\geq 0} T_n t^n$ et $G_{U_n}(t) = \sum_{n\geq 0} U_n t^n$ sont les séries génératrices ordinaires des suites $(T_n)_n$ et $(U_n)_n$ repectivement. Elles valent

$$G_{T_n}(t) = \frac{1-Xt}{1-2Xt+t^2} \quad \text{et} \quad G_{U_n}(t) = \frac{1}{1-2Xt+t^2}.$$

En effet, en effectuant le produit de la série $\sum_{n\geq 0} t^n T_n$ par le polynôme $1-2Xt+t^2$ en la variable t, nous avons :

$$\begin{aligned}(1-2Xt+t^2)\, G_{T_n}(t) &= \sum_{n\geq 0} t^n T_n \; - 2X \sum_{n\geq 0} t^{n+1} T_n \; + \sum_{n\geq 0} t^{n+2} T_n \\ &= T_0 + tT_1 - 2XtT_0 \; + \sum_{n\geq 0} t^{n+2} T_n \; - 2X \sum_{n\geq 0} t^{n+2} T_n \; + \sum_{n\geq 0} t^{n+2} T_n\end{aligned}$$

Nous déduisons alors, de la relation (4.1), que $(1-2Xt+t^2)\, G_{T_n}(t) = 1-Xt$.
Idem pour $G_{U_n}(t)$.

4.3 Formules explicites

Les série génératrices sont un outil efficace pour la détermination des formes explicites de suites récurrentes linéaires.

Proposition 4.2. *Pour tout entier $n \geq 1$,*

$$T_n = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \; 2^{n-2k-1} \frac{n}{n-k} \binom{n-k}{k} \; X^{n-2k} \tag{4.4}$$

$$U_n = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \; 2^{n-2k} \binom{n-k}{k} \; X^{n-2k} \tag{4.5}$$

Ces expressions montrent que, pour $n \geq 0$, T_n et U_n sont dans le $\mathbb{Q}$-espace vectoriel $\mathbb{E}_n[X]$ des polynômes de degré $\leq n$ et ayant la même parité que n. Et les formules (4.4) et (4.5) représentent l'écriture de T_n et U_n dans la base canonique $\mathscr{B}_n = (X^{n-2k})_{0 \leq k \leq \lfloor n/2 \rfloor}$ de $\mathbb{E}_n[X]$.

Les cinq premiers polynômes étant :

$$\begin{array}{lcllcl} T_0 &=& 1, & U_0 &=& 1, \\ T_1 &=& X, & U_1 &=& 2X, \\ T_2 &=& 2X^2 - 1, & U_2 &=& 4X^2 - 1, \\ T_3 &=& 4X^3 - 3X, & U_3 &=& 8X^3 - 4X, \\ T_4 &=& 8X^4 - 8X^2 + 1, & U_4 &=& 16X^4 - 12X^2 + 1. \end{array}$$

4.4 Nouvelles expressions des polynômes de Chebyshev

Dans [11], les auteurs ont construit deux autres bases de $\mathbb{E}_n[X]$ dans le but de donner d'autres formes d'écriture des polynômes de Chebyshev. Ces bases sont

$\mathscr{T}_n = (X^k \; T_{n-k})_k$ et $\mathscr{U}_n = (X^k \; U_{n-k})_k$ pour $n - 2\lfloor \frac{n}{2} \rfloor \leq k \leq n - \lfloor \frac{n}{2} \rfloor$.

Avant de donner les coordonnées de T_n et de U_n dans ces nouvelles bases, considérons, pour tous entiers n et k, les suites $(\alpha_{n,k})_{n,k}$, $(\beta_{n,k})_{n,k}$ et $(\gamma_{n,k})_{n,k}$ définies par

$$\begin{array}{lcl} \alpha_{n,k} &=& (-1)^{k+1} \; 2^k \; \binom{n}{k}, \\ \beta_{n,k} &=& \alpha_{n,k} - \alpha_{n,k-1}, \\ \gamma_{n,k} &=& (-1)^{n+1} \alpha_{n,k} + 2 \sum_{j=0}^{n-1} (-1)^{j+1} \; \alpha_{j,k}. \end{array}$$

Les coordonnés de T_n et de U_n dans les bases $\mathscr{T}_n$ et $\mathscr{U}_n$ sont donnés par les théorèmes suivants :

Théorème 4.3. *Pour $n \geq 0$,*

$$T_{2n+1} = \sum_{k=1}^{n+1} \beta_{n,k} \; X^k \; T_{2n+1-k}, \tag{4.6}$$

$$U_{2n+1} = \sum_{k=1}^{n+1} \alpha_{n+1,k} \; X^k \; U_{2n+1-k}. \tag{4.7}$$

Le théorème 4.3 donne la décomposition de T_{2n+1} dans la base $\mathscr{T}_{2n+1}$ et de U_{2n+1} dans la base $\mathscr{U}_{2n+1}$.

Théorème 4.4. *Pour* $n \geq 0$,

$$T_{2n} = U_{2n} - XU_{2n-1}, \quad n \geq 1, \tag{4.8}$$

$$U_{2n} = \sum_{k=0}^{n} \gamma_{n,k}\ X^k\ T_{2n-k}. \tag{4.9}$$

Le théorème 4.4 donne la décomposition de T_{2n} dans la base $\mathscr{U}_{2n}$ et de U_{2n} dans la base $\mathscr{T}_{2n}$.

Théorème 4.5. *Pour* $n \geq 0$,

$$T_{2n+1} = \sum_{k=1}^{n+1} (\alpha_{n+1,k} - \delta_{k,1})\ X^k\ U_{2n+1-k}, \tag{4.10}$$

$$U_{2n+1} = \sum_{k=1}^{n+1} (\gamma_{n,k-1} + \beta_{n,k})\ X^k\ T_{2n+1-k}. \tag{4.11}$$

où $\delta_{i,j}$ est le symbole de Kronecker.

Le théorème 4.5 donne la décomposition de T_{2n+1} dans la base $\mathscr{U}_{2n+1}$ et de U_{2n+1} dans la base $\mathscr{T}_{2n+1}$.

Les premiers polynômes de Chebyshev écrits dans ces nouvelles bases sont donc :

A partir du théorème 4.3

$$\begin{array}{rcl} T_1 &=& XT_0, \\ T_3 &=& 3XT_2 - 2X^2T_1, \\ T_5 &=& 5XT_4 - 8X^2T_3 + 4X^3T_2, \\ T_7 &=& 7XT_6 - 18X^2T_5 + 20X^3T_4 - 8X^4T_3, \end{array} \qquad \begin{array}{rcl} U_1 &=& 2XU_0, \\ U_3 &=& 4XU_2 - 4X^2U_1, \\ U_5 &=& 6XU_4 - 12X^2U_3 + 8X^3U_2, \\ U_7 &=& 8XU_6 - 24X^2U_5 + 32X^3U_4 - 16X^4U_3. \end{array}$$

A partir du théorème 4.4

$$\begin{array}{rcl} T_0 &=& U_0, \\ T_2 &=& U_2 - XU_1, \\ T_4 &=& U_4 - XU_3, \\ T_6 &=& U_6 - XU_5, \\ T_8 &=& U_8 - XU_7, \end{array} \qquad \begin{array}{rcl} U_0 &=& T_0, \\ U_2 &=& T_2 + 2XT_1, \\ U_4 &=& T_4 + 4X^2T_2, \\ U_6 &=& T_6 + 2XT_5 - 4X^2T_4 + 8X^3T_3, \\ U_8 &=& T_8 + 8X^2T_6 - 16X^3T_5 + 16X^4T_4. \end{array}$$

A partir du théorème 4.5

$$\begin{array}{lcllcl} T_1 &=& XU_0, & & U_1 &=& 2XT_0, \\ T_3 &=& 3XU_2 - 4X^2U_1, & & U_3 &=& 4XT_2, \\ T_5 &=& 5XU_4 - 12X^2U_3 + 8X^3U_2, & & U_5 &=& 6XT_4 - 8X^2T_3 + 8X^3T_2, \\ T_7 &=& 7XU_6 - 24X^2U_5 + 32X^3U_4 - 16X^4U_3, & & U_7 &=& 8XT_6 - 16X^2T_5 + 16X^3T_4. \end{array}$$

4.5 Polynômes généralisés de Chebyshev

Nous nous proposons, dans ce paragraphe, d'étendre l'étude faite plus haut, aux polynômes généralisés de Chebyshev obtenus en remplaçant dans (4.1) et (4.2) le monôme $2X$ par un polynôme h quelconque non constant à coefficients réels. Comme nous le verrons plus loin, Il nous est apparu dès le début, qu'il fallait distinguer le cas où h est un monôme du premier degré à coefficient rationnel des autres cas. Tous les résultats obtenus ont lieu quelque soit le polynôme h à l'exception du cas $h(X) = aX$ $(a \in \mathbb{Q}^*)$. Ce qui nous permet de dire que cette étude n'est pas une généralisation du travail fait dans [11] mais une étude qui complète ce travail aux cas des polynômes $h(X) \neq aX, \quad a \in \mathbb{Q}^*$.

Soit donc h un polynôme de degré ≥ 1 distinct du monôme aX, avec $a \in \mathbb{Q}^*$, à coefficients réels. Considérons alors, pour tout entier naturel n, les suites de polynômes en l'indéterminée X définis par :

$$T_n = h(X)T_{n-1} - T_{n-2} \quad \text{avec } T_0 = 1 \text{ et } T_1 = X, \tag{4.12}$$

$$U_n = h(X)U_{n-1} - U_{n-2} \quad \text{avec } U_0 = 1 \text{ et } U_1 = 2X, \tag{4.13}$$

que nous appelons respectivement polynômes h-Chebyshev de première et seconde espèce. Ce sont les polynômes de Chebyshev généralisés à h.

4.6 Séries génératrices des polynômes h-Chebyshev et formules explicites

Les séries génératrices des suites $(T_n)_n$ et $(U_n)_n$ sont données par :

$$G_{T_n}(t) = \frac{1 - t(h(X) - X)}{1 - h(X)t + t^2} \quad \text{et} \quad G_{U_n}(t) = \frac{1 - t(h(X) - 2X)}{1 - h(X)t + t^2}.$$

elles nous permettent d'établir les formules explicites des suites $(T_n)_n$ et $(U_n)_n$ via le théorème suivant :

Théorème 4.6. *Pour tout $n \geq 1$,*

$$T_n = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \ \frac{k}{n-k} \binom{n-k}{k} \ h(X)^{n-2k} \ + \ \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} (-1)^k \ \frac{n-2k}{n-k} \binom{n-k}{k} \ X \ h(X)^{n-2k-1}, \tag{4.14}$$

$$U_n = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \ \frac{k}{n-k} \binom{n-k}{k} \ h(X)^{n-2k} \ + \ 2 \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} (-1)^k \ \frac{n-2k}{n-k} \binom{n-k}{k} \ X \ h(X)^{n-2k-1}. \tag{4.15}$$

Preuve. Nous avons

$$\frac{1}{1-ht+t^2} = \sum_{m \geq 0} t^m \ (h-t)^m = \sum_{m \geq 0} \sum_{k=0}^{m} \binom{m}{k} (-1)^k \ h^{m-k} \ t^{m+k}.$$

En posant $m+k=n$, nous obtenons

$$\frac{1}{1-ht+t^2} = \sum_{n \geq 0} \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n-k}{k} (-1)^k \ h^{n-2k} \ t^n.$$

Il s'ensuit que

$$1 + \sum_{n \geq 1} T_n \ t^n = 1 + \sum_{n \geq 1} S \ t^n,$$

où S est la somme

$$S = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \ \tbinom{n-k}{k} \ h^{n-2k} \ - \ \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} (-1)^k \ \tbinom{n-k-1}{k} \ h^{n-2k} \ + \ \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} (-1)^k \ \tbinom{n-k-1}{k} \ X \ h^{n-2k-1}.$$

En utilisant l'égalité

$$\binom{n-k-1}{k} = \frac{n-2k}{n-k} \binom{n-k}{k},$$

nous obtenons

$$S = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \ \frac{k}{n-k} \binom{n-k}{k} \ h(X)^{n-2k} \ + \ \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} (-1)^k \ \frac{n-2k}{n-k} \binom{n-k}{k} \ X \ h(X)^{n-2k-1}.$$

La formule (4.15) s'obtient de manière analogue. □

Remarque 4.7. *La preuve du théorème 4.6 est faite sans aucune restriction sur le polynôme h. Dans le cas particulier où $h(X) = aX$ avec $a \neq 0$ les formules* (4.14) *et* (4.16) *deviennent pour $n \geq 1$*

$$T_n = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \frac{1}{n-k} \binom{n-k}{k} a^{n-2k-1} X^{n-2k} [n + (a-2)k],$$

$$U_n = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \frac{1}{n-k} \binom{n-k}{k} a^{n-2k-1} X^{n-2k} [2n + (a-4)k].$$

Par conséquent, en posant $h(X) = 2X$ ie. $a = 2$ nous retrouvons les formules (4.4) *et* (4.5).

4.7 L'espace vectoriel des polynômes h-Chebyshev

Soient $\mathfrak{B}_1 = \{X\}$ et $\mathfrak{B}_n = (h^{n-2k}, Xh^{n-2l-1})_{n\geq 2}$ avec $1 \leq k \leq \lfloor \frac{n}{2} \rfloor$ et $0 \leq l \leq \lfloor \frac{n-1}{2} \rfloor$.

Considérons l'espace des polynôme $\mathbb{R}[X]$ comme $\mathbb{Q}$-espace vectoriel. Pour $n \geq 1$, soit $\mathbb{E}_n[X]$ le sous-espace vectoriel de $\mathbb{R}[X]$ engendré par la famille $\mathfrak{B}_n$.

Pour tout $n \geq 2$, les polynômes T_n et U_n sont dans $\mathbb{E}_n[X]$. Nous allons montrer que la famille $\mathfrak{B}_n$ est libre pourvu que le polynôme h ne soit pas un monôme de degré 1 à coefficient rationnel i.e. $h(X) \neq aX \ \ (a \in \mathbb{Q}^*)$. Pour ce cas précis, il faut plutôt prendre pour $\mathfrak{B}_n$ la famille $(X^k)_n \ \ (1 \leq k \leq \lfloor \frac{n}{2} \rfloor)$ qui engendre le $\mathbb{Q}$-espace vectoriel $\mathbb{E}_n[X]$ des polynômes ayant la même parité que n. On se retrouve donc dans le cas classique des polynômes de Chebyshev.

Considérons donc h un polynôme non constant de $\mathbb{R}[X]$ et différent de $aX \ \ (a \in \mathbb{Q}^*)$.

Théorème 4.8. *Pour $n \geq 1$, $\mathfrak{B}_n$ est une base de $\mathbb{E}_n[X]$.*

Preuve. Il s'agit de vérifier que la famille $\mathfrak{B}_n$ est libre. Supposons d'abord que n est pair. Le cas $n = 2$ est trivial. Pour $n = 2m \ \ (m \geq 2)$,

$$\mathfrak{B}_n = \{1, Xh, h^2, Xh^3, \cdots, h^{2m-2}, Xh^{2m-1}\}.$$

Compte tenu du fait que le degré de Xh^{2m-1} est strictement plus grand que celui de h^{2m-1} et de celui de Xh^{2m-k} pour tout $k \geq 2$, le polynôme Xh^{2m-1} ne peut pas s'écrire comme combinaison linéaire de $1, Xh, \cdots, h^{2m-2}$.

Supposons maintenant qu'il existe $a_i \in \mathbb{Q} \ \ (0 \leq i \leq 2m-3)$ tels que

$$h^{2m-2} = a_{2m-3}Xh^{2m-3} + a_{2m-4}h^{2m-4} + \cdots + a_1Xh + a_0. \tag{4.16}$$

Le degré de h^{2m-2} est strictement plus grand que celui de Xh^{2m-3} sauf lorsque $d^\circ h = 1$ auquel cas les deux degrés sont égaux. Donc, si $d^\circ h > 1$ alors l'écriture (4.16) n'est pas possible.

Si $d^\circ h = 1$ alors $h(x) = ax + b$ avec (a et b dans $\mathbb{R}^*$) ou ($b = 0$ et $a \in \mathbb{R} \setminus \mathbb{Q}$). Par identification au niveau de l'identité (4.16), on obtient les deux premières équations :

$$\begin{cases} a^{2m-2} &= a_{2m-3}a^{2m-3} \\ (2m-2)a^{2m-3}b &= (2m-3)a^{2m-4}ba_{2m-3} \end{cases}$$

d'où l'on tire

$$a = a_{2m-3} \text{ et } a = \frac{2m-3}{2m-2} a_{2m-3}.$$

Ce qui est manifestement pas possible.
Par suite $\mathfrak{B}_{2m}$ est une base de $\mathbb{E}_n[X]$.

Le cas n impair se traite de la même manière. □

A partir du théorème 4.6, les premières valeurs de T_n et U_n dans la base $\mathfrak{B}_n$ sont :

$$\begin{aligned}
T_1 &= X, \\
T_2 &= Xh - 1, \\
T_3 &= Xh^2 - h - X, \\
T_4 &= Xh^3 - h^2 - 2Xh + 1, \\
T_5 &= Xh^4 - h^3 - 3Xh^2 + 2h + X, \\
T_6 &= Xh^5 - h^4 - 4Xh^3 + 3h^2 + 3Xh - 1.
\end{aligned}$$

$$\begin{aligned}
U_1 &= 2X, \\
U_2 &= 2Xh - 1, \\
U_3 &= 2Xh^2 - h - 2X, \\
U_4 &= 2Xh^3 - h^2 - 4Xh + 1, \\
U_5 &= 2Xh^4 - h^3 - 6Xh^2 + 2h + 2X, \\
U_6 &= 2Xh^5 - h^4 - 8Xh^3 + 3h^2 + 6Xh - 1.
\end{aligned}$$

4.8 Deux autres bases de l'espace vectoriel des polynômes h-Chebyshev

Nous allons montrer maintenant que pour tout $n \geq 1$, $\mathfrak{T}_n = (h^k\, T_{n-k})_k$ et $\mathfrak{U}_n = (h^k\, U_{n-k})_k$ $(0 \leq k \leq n-1)$ sont deux autres bases de $\mathbb{E}_n[X]$ et nous allons donner les coordonnées de T_n et U_n dans ces nouvelles bases.

Théorème 4.9. *Pour $n \geq 1$, $\mathfrak{T}_n$ et $\mathfrak{U}_n$ sont des bases de $\mathbb{E}_n[X]$.*

Ce théorème provient du lemme suivant

Lemme 4.10. *Pour $n \geq 1$,*

$$det_{\mathfrak{B}_n}(\mathfrak{T}_n) = \begin{cases} 1 & \text{si } n \text{ pair} \\ (-1)^{\lfloor n/2 \rfloor} & \text{si } n \text{ impair} \end{cases}$$

$$det_{\mathfrak{B}_n}(\mathfrak{U}_n) = \begin{cases} 2^{\lfloor n/2 \rfloor} & \text{si } n \text{ pair} \\ (-1)^{\lfloor n/2 \rfloor}\ 2^{\lfloor n/2 \rfloor + 1} & \text{si } n \text{ impair} \end{cases}$$

Preuve.

Considérons d'abord le cas pair $n = 2m$.

Pour $m \geq 1$ et $1 \leq k \leq 2m+1$, posons $V_k^{(m)} := h^{k-1}T_{2m+1-k}$ et $W_k^{(m)} := h^{k-1}U_{2m+1-k}$.

Il est clair que

$$V_{k+1}^{(m)} - V_k^{(m)} = V_k^{(m-1)} \text{ et } W_{k+1}^{(m)} - W_k^{(m)} = W_k^{(m-1)}.$$

Soit $\Delta_m := \det_{\mathfrak{B}_{2m}}(V_1^{(m)}, V_2^{(m)}, ..., V_{2m}^{(m)})$ et $D_m := \det_{\mathfrak{B}_{2m}}(W_1^{(m)}, W_2^{(m)}, ..., W_{2m}^{(m)})$. Nous avons

$$\begin{aligned}\Delta_m &= det_{\mathfrak{B}_{2m}}(V_1^{(m)}, V_2^{(m)} - V_1^{(m)}, ..., V_{2m}^{(m)} - V_{2m-1}^{(m)}) \\ &= det_{\mathfrak{B}_{2m}}(V_1^{(m)}, V_1^{(m-1)}, V_2^{(m-1)}, ..., V_{2m-1}^{(m-1)}).\end{aligned}$$

Désignons par $d_h^\circ T_n$ la plus grande puissance de h dans l'écriture de T_n dans la base $\mathfrak{B}_n$. Nous avons $d_h^\circ T_0 = 0$ et $d_h^\circ T_n = n-1 \quad (n \geq 1)$. Il s'ensuit que $d_h^\circ V_k^{(m)} = 2m-1 \quad (1 \leq k \leq 2m)$, $d_h^\circ V_k^{(m-1)} = 2m-3 \quad (1 \leq k \leq 2m-2)$ et $d_h^\circ V_{2m-1}^{(m-1)} = 2m-2$. Les coefficients dominants de $V_1^{(m)}$, $V_{2m-1}^{(m-1)}$ et $V_k^{(m-1)} \quad (1 \leq k \leq 2m-2)$ sont égaux à 1. Par conséquent

$$\Delta_m = (-1)^{1+2m-1} \det_{\mathfrak{B}_{2(m-1)}}(V_1^{(m-1)}, V_2^{(m-1)}, ..., V_{2(m-1)}^{(m-1)}) = \Delta_{m-1} = \cdots = \Delta_1 = 1.$$

De façon Similaire

$$\begin{aligned}D_m &= det_{\mathfrak{B}_{2m}}(W_1^{(m)}, W_2^{(m)}, ..., W_{2m}^{(m)}) \\ &= det_{\mathfrak{B}_{2m}}(W_1^{(m)}, W_1^{(m-1)}, W_2^{(m-1)}, ..., W_{2m-1}^{(m-1)}).\end{aligned}$$

Comme $d_h^\circ W_k^{(m)} = 2m-1 \quad (1 \leq k \leq 2m)$, $d_h^\circ W_k^{(m-1)} = 2m-3 \quad (1 \leq k \leq 2m-2)$ et $d_h^\circ W_{2m-1}^{(m-1)} = 2m-2$ avec coefficient dominant de $W_1^{(m)}$ et $W_k^{(m-1)} \quad (1 \leq k \leq 2m-2)$ égaux à 2 et coefficient dominant de $W_{2m-1}^{(m-1)}$ égal 1 alors

$$D_m = 2(-1)^{2m} D_{m-1} = 2D_{m-1} = \cdots = 2^m.$$

Pour le cas impair $n = 2m+1$, nous avons

$$\begin{aligned}det_{\mathfrak{B}_{2m+1}}(T_{2m+1}, hT_{2m}, ..., h^{2m}T_1) &= (-1)^{2m}\ (-1)^m\ det_{\mathfrak{B}_{2m}}(T_{2m}, hT_{2m-1}, ..., h^{2m-1}T_1) \\ &= (-1)^m\ det_{\mathfrak{B}_{2m}}(T_{2m}, hT_{2m-1}, ..., h^{2m-1}T_1) \\ &= (-1)^m\ det_{\mathfrak{B}_{2m}}(V_1^{(m)}, V_2^{(m)}, ..., V_{2m}^{(m)}) \\ &= (-1)^m \Delta_m \\ &= (-1)^m\end{aligned}$$

et

$$\begin{aligned} det_{\mathfrak{B}_{2m+1}}(U_{2m+1}, hU_{2m}, ..., h^{2m}U_1) &= 2(-1)^{2m+2}\ (-1)^m\ det_{\mathfrak{B}_{2m}}(U_{2m}, hU_{2m-1}, ..., h^{2m-1}U_1) \\ &= 2(-1)^m\ det_{\mathfrak{B}_{2m}}(U_{2m}, hU_{2m-1}, ..., h^{2m-1}U_1) \\ &= 2(-1)^m D_m \\ &= (-1)^m 2^{m+1}. \end{aligned}$$

□

4.9 Coordonnées des polynômes h-Chebyshev dans les nouvelles bases

Il s'agit, dans ce paragraphe, de donner les coordonnées des polynômes h-Chebyshev T_n et U_n dans chacune des nouvelles bases $\mathfrak{T}_n$ et $\mathfrak{U}_n$. Il y'a 8 cas à considérer :

Coordonnées de T_{2n} dans la base $\mathfrak{T}_{2n}$;
Coordonnées de U_{2n} dans la base $\mathfrak{U}_{2n}$;
Coordonnées de T_{2n+1} dans la base $\mathfrak{T}_{2n+1}$;
Coordonnées de U_{2n+1} dans la base $\mathfrak{U}_{2n+1}$;
Coordonnées de T_{2n} dans la base $\mathfrak{U}_{2n}$;
Coordonnées de U_{2n} dans la base $\mathfrak{T}_{2n}$;
Coordonnées de T_{2n+1} dans la base $\mathfrak{U}_{2n+1}$;
Coordonnées de U_{2n+1} dans la base $\mathfrak{T}_{2n+1}$.

Les 4 premiers cas sont triviaux. Les 4 suivants s'obtiennent par les résultats ci-après :

Théorème 4.11. *Pour tout entier $n \geq 1$, on a*

$$2T_{2n} = 2U_{2n} + \sum_{j=1}^{2n-1}(-1)^{j+1}\alpha_{2n-1,j}h^j U_{2n-j}, \tag{4.17}$$

$$2T_{2n+1} = U_{2n+1} + \sum_{j=1}^{2n}(-1)^{j+1}\alpha_{2n,j}h^j U_{2n+1-j}. \tag{4.18}$$

Théorème 4.12. *Pour tout entier $n \geq 1$, on a*

$$U_{2n} = T_{2n} + \frac{1}{2}\sum_{j=1}^{2n-1}(-1)^{j-1}\left[\binom{2n-1}{j} + \alpha_{2n-2,j-1}\right]h^j T_{2n-j}, \tag{4.19}$$

$$U_{2n+1} = 2T_{2n+1} + \sum_{j=1}^{2n}(-1)^{j}\alpha_{2n,j}h^j T_{2n+1-j}. \tag{4.20}$$

La suite $(\alpha_{n,j})_n$ est définie pour tout $n \geq 0$ et tout $0 \leq j \leq n$ par $\alpha_{n,j} = \sum_{k=j}^{n}(-1)^k\binom{k}{j}$ dont les premières valeurs sont

n/j	0	1	2	3	4	5	6
0	0						
1	0	−1					
2	1	1	1				
3	0	−2	−2	−1			
4	1	2	4	3	1		
5	0	−3	−6	−7	4	−1	
6	1	3	9	10	11	5	1

$\alpha_{n,j}$, pour $1 \leq n \leq 6$ et $0 \leq j \leq 6$.

Pour l'établissement des preuves des théorèmes 4.11 et 4.12 nous avons besoin de la proposition suivante :

Proposition 4.13. *Pour tous entiers n et j avec $n \geq 1$,*

1. $\alpha_{n+1,j} + \alpha_{n,j-1} = \alpha_{n-1,j} + \alpha_{n-1,j-1}$,
2. $\alpha_{2n,j-1} + \alpha_{2n-2,j-2} + \alpha_{2n-2,j-1} = \binom{2n}{j-1}$,
3. $-\alpha_{2n+2,j} + \alpha_{2n,j-1} + \alpha_{2n,j} + \frac{1}{2}\alpha_{2n,j-2} = -\frac{1}{2}\binom{2n+1}{j-1}$.

Preuve. Nous avons

1. $\alpha_{n+1,j} + \alpha_{n,j-1} - \alpha_{n-1,j} - \alpha_{n-1,j-1} = (-1)^n\binom{n}{j} + (-1)^n\binom{n}{j-1} + (-1)^{n+1}\binom{n+1}{j} = 0.$

$$\begin{aligned}
2.\ \alpha_{2n,j-1} + \alpha_{2n-2,j-2} + \alpha_{2n,j-1} &= 2\sum_{k=j-1}^{2n-2}(-1)^k\binom{k}{j-1} - \binom{2n-1}{j-1} + \binom{2n}{j-1} + \sum_{k=j-2}^{2n-2}(-1)^k\binom{k}{j-2} \\
&= \sum_{k=j-1}^{2n-2}(-1)^k\binom{k}{j-1} + \sum_{k=j-1}^{2n-2}(-1)^k\binom{k+1}{j-1} - \binom{2n-1}{j-1} + \binom{2n}{j-1} \\
&\qquad +(-1)^j\binom{j-2}{j-2} \\
&= (-1)^{j-1}\binom{j-1}{j-1} + \binom{2n-1}{j-1} - \binom{2n-1}{j-1} + \binom{2n}{j-1} + (-1)^j\binom{j-2}{j-2} \\
&= \binom{2n}{j-1}.
\end{aligned}$$

$$
\begin{aligned}
3.\ -\alpha_{2n+2,j}+\alpha_{2n,j-1}+\alpha_{2n,j}+\tfrac{1}{2}\alpha_{2n,j-2} &= \tbinom{2n+1}{j}-\tbinom{2n+2}{j}+\tfrac{1}{2}(-1)^j\tbinom{j-2}{j-2}+\tfrac{1}{2}\sum_{k=j-1}^{2n}(-1)^k\tbinom{k}{j-1}\\
&\quad +\tfrac{1}{2}\sum_{k=j-1}^{2n}(-1)^k\tbinom{k+1}{j-1}\\
&= \tbinom{2n+1}{j}-\tbinom{2n+2}{j}+\tfrac{1}{2}(-1)^j\tbinom{j-2}{j-2}+\tfrac{1}{2}(-1)^{j-1}\tbinom{j-1}{j-1}\\
&\quad +\tfrac{1}{2}\tbinom{2n+1}{j-1}\\
&= -\tfrac{1}{2}\tbinom{2n+1}{j-1}
\end{aligned}
$$

□

Nous obtenons grâce au théorème 4.11

$$
\begin{aligned}
2T_1 &= U_1,\\
2T_2 &= 2U_2-hU_1,\\
2T_3 &= U_3+hU_2-h^2U_1,\\
2T_4 &= 2U_4-2hU_3+2h^2U_2-h^3U_1,\\
2T_5 &= U_5+2hU_4-4h^2U_3+3h^3U_2-h^4U_1,\\
2T_6 &= 2U_6-3hU_5+6h^2U_4-7h^3U_3+4h^4U_2-h^5U_1,\\
2T_7 &= U_7+3hU_6-9h^2U_5+13h^3U_4-11h^4U_3+5h^5U_2-h^6U_1,
\end{aligned}
$$

T_n dans la base $\mathfrak{U}_n$

et grâce au théorème 4.12

$$
\begin{aligned}
U_1 &= 2T_2,\\
U_2 &= T_2+hT_1,\\
U_3 &= 2T_3-hT_2+h^2T_1,\\
U_4 &= T_4+2hT_3-2h^2T_2+h^3T_1,\\
U_5 &= 2T_5-2hT_4+4h^2T_3-3h^3T_2+h^4T_1,\\
U_6 &= T_6+3hT_5-6h^2T_4+7h^3T_3-4h^4T_2+h^5T_1,\\
U_7 &= 2T_7-3hT_6+9h^2T_5-13h^3T_4+11h^4T_3-5h^5T_2+h^6T_1.
\end{aligned}
$$

U_n dans la base $\mathfrak{T}_n$

4.10 Preuves des théorèmes

Les preuves des théorèmes 4.11 et 4.12 utilisent un raisonnement par récurrence et la proposition 4.13.

Preuve.

- **Preuve du théorème 4.11** Les tables précédentes montrent que les formules (4.17) et (4.18) sont vraies pour les premiers termes. Supposons qu'elles le soient à l'ordre n. Grâce alors aux relations (4.12) et (4.13), nous avons

$$2T_{2n+2} = hU_{2n+1} + \sum_{j=1}^{2n}(-1)^{j+1}\alpha_{2n,j}h^{j+1}U_{2n+1-j} - 2U_{2n} - \sum_{j=1}^{2n-1}(-1)^{j+1}\alpha_{2n-1,j}h^jU_{2n-j}.$$

En posant $j+1=j'$ dans la première somme nous obtenons

$$\begin{aligned} 2T_{2n+2} &= 2U_{2n+2} - hU_{2n+1} - \alpha_{2n,2n}h^{2n+1}U_1 + \alpha_{2n,2n-1}h^{2n}U_2 + \alpha_{2n-1,1}hU_{2n+1} + \\ &\quad -\alpha_{2n-1,2n-1}h^{2n}U_2 + \sum_{j=2}^{2n-1}(-1)^j h^j U_{2n+2-j}\left[\alpha_{2n,j-1} - \alpha_{2n-1,j} - \alpha_{2n-1,j-1}\right]. \end{aligned}$$

Or $\alpha_{n,1} = \frac{1}{4}(-1)^n(2n+1) - \frac{1}{4}$, $\alpha_{n,n} = (-1)^n$, $\alpha_{n,n-1} = (-1)^n n + (-1)^{n-1}$ et de la proposition 4.13, $\alpha_{2n,j-1} - \alpha_{2n-1,j} - \alpha_{2n-1,j-1} = -\alpha_{2n+1,j}$.
Nous déduisons que

$$2T_{2n+2} = 2U_{2n+2} + \sum_{j=1}^{2n+1}(-1)^{j+1}\alpha_{2n+1,j}h^jU_{2n+2-j}.$$

La formule (4.17) est prouvée.

Nous procédons de la même manière pour établir la formule (4.18). Nous avons donc

$$\begin{aligned} 2T_{2n+3} &= 2hU_{2n+2} + \sum_{j=1}^{2n+1}(-1)^{j+1}\alpha_{2n+1,j}h^{j+1}U_{2n+2-j} - U_{2n+1} - \sum_{j=1}^{2n}(-1)^{j+1}\alpha_{2n,j}h^jU_{2n+1-j}. \\ &= U_{2n+3} + hU_{2n+2} - \alpha_{2n+1,2n}h^{2n+1}U_2 + \alpha_{2n+1,2n+1}h^{2n+2}U_1 + \alpha_{2n,1}hU_{2n+2} + \\ &\quad +\alpha_{2n,2n}h^{2n+1}U_2 + \sum_{j=2}^{2n}(-1)^{j+1}\left[-\alpha_{2n+1,j-1} + \alpha_{2n,j} + \alpha_{2n,j-1}\right]h^jU_{2n+3-j}. \\ &= U_{2n+3} + \sum_{j=1}^{2n+2}(-1)^{j+1}\alpha_{2n+2,j}h^jU_{2n+3-j}. \end{aligned}$$

- **Preuve du théorème 4.12** Supposons par récurrence que les relations (4.19) et (4.20)

soient vraies pour n. Alors

$$\begin{aligned}
U_{2n+2} &= 2hT_{2n+1} + \sum_{j=1}^{2n}(-1)^j \alpha_{2n,j} h^{j+1} T_{2n+1-j} - T_{2n} \\
&\quad -\frac{1}{2}\sum_{j=1}^{2n-1}(-1)^{j-1}\left[\tbinom{2n-1}{j} + \alpha_{2n-2,j-1}\right] h^j T_{2n-j}. \\
&= T_{2n+2} + hT_{2n+1} + \alpha_{2n,2n} h^{2n+1} T_1 - \alpha_{2n,2n-1} h^{2n} T_2 - \frac{1}{2}\left[\tbinom{2n-1}{2n-1} + \alpha_{2n-2,2n-2}\right] h^{2n} T_2 \\
&\quad +\frac{1}{2}\left[\tbinom{2n-1}{1} + \alpha_{2n-2,0}\right] hT_{2n+1} \\
&\quad + \sum_{j=2}^{2n-1}(-1)^{j-1}\left[\alpha_{2n,j-1} + \frac{1}{2}\left(\tbinom{2n-1}{j-1} + \alpha_{2n-2,j-2} + \tbinom{2n-1}{j} + \alpha_{2n-2,j-1}\right)\right] h^j T_{2n+2-j}. \\
&= T_{2n+2} + \frac{1}{2}\sum_{j=1}^{2n+1}(-1)^{j-1}\left[\tbinom{2n+1}{j} + \alpha_{2n,j-1}\right] h^j T_{2n+2-j}.
\end{aligned}$$

Au niveau de la deuxième étape nous avons utilisé la relation

$$T_{2n-j} = hT_{2n+1-j} - T_{2n+2-j}.$$

De manière analogue, nous avons

$$\begin{aligned}
U_{2n+3} &= hT_{2n+2} + \frac{1}{2}\sum_{j=1}^{2n+1}(-1)^{j-1}\left[\tbinom{2n+1}{j} + \alpha_{2n,j-1}\right] h^{j+1} T_{2n+2-j} - 2T_{2n+1} \\
&\quad -\sum_{j=1}^{2n}(-1)^j \alpha_{2n,j} h^j T_{2n+1-j}. \\
&= 2T_{2n+3} - hT_{2n+2} + \frac{1}{2}\left[\tbinom{2n+1}{2n+1} + \alpha_{2n,2n}\right] h^{2n+2} T_1 - \frac{1}{2}\left[\tbinom{2n+1}{2n} + \alpha_{2n,2n-1}\right] h^{2n+1} T_2 \\
&\quad -\alpha_{2n,2n} h^{2n+1} T_2 - \alpha_{2n,1} hT_{2n+2} \\
&\quad + \sum_{j=2}^{2n}(-1)^j h^j T_{2n+3-j}\left[\frac{1}{2}\left(\tbinom{2n+1}{j-1} - \alpha_{2n,j-2}\right) + \alpha_{2n,j-1} + \alpha_{2n,j}\right]. \\
&= 2T_{2n+3} + \sum_{j=1}^{2n+2}(-1)^j \alpha_{2n+2,j} h^j T_{2n+3-j}.
\end{aligned}$$

□

Chapitre 5

Théorème de Lucas généralisé

5.1 Introduction

La branche de l'arithmétique qui traite des problèmes de congruences faisant intervenir les coefficients binomiaux, modulo des nombres premiers, a, dès ses origines, sucité l'intérêt des mathématiciens et c'est encore le cas de nos jours. Les nombreux travaux publiés chaque année sur ce sujet attestent de cet intérêt. Elle a su attirer de grands noms parmi lesquels : Lucas, Legendre, Kummer, Hermite, Hensel, Gauss, Cayley, Cauchy et d'autres. De nombreux théorèmes, importants et remarquables, ont été établis. Pour un aperçu non exhaustif de cette grande variété de résultats et des différents développements et extensions qu'ils ont connus jusqu'à récemment, le lecteur est invité à consulter le livre de Leonard Eugene Dickson [26] "History of the theory of numbers" et le très intéressant article d'Andrew Granville [37] "Arithmetic properties of binomial coefficients". Nous proposons dans ce mémoire, un petit échantillon de ces nombreux résultats. Nous avons choisi de les présenter non pas suivant l'ordre chronologique de leur apparition, mais suivant la nature et la parenté des énoncés.

Babbage (1819)
Voulant étendre la congruence

$$\binom{np-1}{p-1} \equiv 1 \bmod p,$$

où n est un entier > 0 et p premier, qui est une conséquence du théorème de Wilson, $(p-1)! \equiv 1 \bmod p$, à une congruence modulo p^2, Babbage [7] à montré que

$$\binom{2p-1}{p-1} \equiv 1 \bmod p^2,$$

pour tout nombre premier $p \geq 3$. Formule qui s'exprime aussi par

$$\binom{2p}{p} \equiv \binom{2}{1} \bmod p^2.$$

Wolstenholme, en 1862, à prouvé que le résultat précédent reste valable modulo p^3 à condition que p soit ≥ 5.

Près d'un siècle plus tard, soit en 1952, cette congruence a été généralisée par Ljunggren [16] à :

$$\binom{np}{mp} \equiv \binom{n}{m} \bmod p^3,$$

et par Jacobsthal à :

$$\binom{np}{mp} / \binom{n}{m} \equiv 1 \bmod p^q,$$

pour tous entiers $n > m > 0$ et tout premier $p \geq 5$ où q est toute puissance de p telle que p^q divise $p^3nm(n-m)$.

Notons que c'est à Babbage [7] qu'on doit la caractérisation des nombre premiers suivante : un entier $n \geq 2$ est premier si et seulement si $\binom{n+m}{n} \equiv 1 \bmod n$ pour tout $0 \leq m \leq n-1$.

Une autre caractérisation des nombres premiers utilisant le coefficient binomial est donnée par Mann et Shanks [55] en 1972. Ils ont montré qu'un entier $n \geq 3$ est premier si et seulement si m divise $\binom{m}{n-2m}$ pour tout m tel que $n - \sqrt{n} \leq 2m \leq n$.

Gauss (1828) (voir [37])

Si p est un nombre premier congru à 1 modulo 4 tel que $p = a^2 + b^2$, en choisissant le signe de a de sorte que $a \equiv 1 \bmod 4$ alors

$$\begin{pmatrix} (p-1)/2 \\ (p-1)/4 \end{pmatrix} \equiv 2a \bmod p.$$

Chowla, Dwork et Evans (1986)

Ils ont démontré dans [18] que sous les mêmes hypothèses que la formule précédente

$$\binom{(p-1)/2}{(p-1)/4} \equiv \left(1 + \frac{2^{p-1}-1}{2}\right)\left(2a - \frac{p}{2a}\right) \bmod p^2.$$

Jacobi (1846)

Si p est un nombre premier congru à 1 modulo 3, en écrivant $4p = A^2 + 27B^2$ où le signe de A est choisi de sorte que $A \equiv 1 \bmod 3$, alors (voir [37])

$$\binom{2(p-1)/3}{(p-1)/3} \equiv -A \bmod p.$$

Morley (1895)

Pour tout nombre premier $p \geq 5$ (voir [61])

$$(-1)^{\frac{p-1}{2}} \begin{pmatrix} p-1 \\ (p-1)/2 \end{pmatrix} \equiv 4^{p-1} \bmod p^3.$$

Granville (1995)

S'inspirant de la preuve proposée par Morley pour la démonstration du résultat précédent, que Granville [37] a qualifiée d'ingénieuse, ce dernier a montré que pour tout nombre premier $p \geq 5$ et tout entier $m \geq 2$ (voir [37])

$$(-1)^{\frac{(p-1)(m-1)}{2}} \binom{p-1}{\lfloor p/m \rfloor} \binom{p-1}{\lfloor 2p/m \rfloor} \cdots \binom{p-1}{\lfloor (m-1)p/m \rfloor} \equiv m^p - m + 1 \bmod p^2.$$

Kummer [45] (1852)

Si p^r est la plus grande puissance du nombre premier p qui divise le coefficient binomial $\binom{n}{m}$ alors r est égal au nombre de retenues dans l'addition de m et $n-m$ lorsque ces deux entiers sont écrits en base p. C'est un résultat considéré comme étant fondamental dans l'étude des propriétés de divisibilité des coefficients binomiaux.

Pour comprendre la signification de cette notion de retenue, examinons l'exemple suivant qui consiste à déterminer le plus grand entier r pour lequel 5^r divise $\binom{13136}{89}$.

$$\begin{array}{lcccccccc} & r_i & & 1 & & 1 & & 1 & & 1 \\ & 89 & = & 4+ & 2\times 5+ & 3\times 5^2 & & & & \\ + & & & & & & & & & \\ & 13047 & = & 2+ & 4\times 5+ & 1\times 5^2+ & 4\times 5^3+ & 0\times 5^4+ & 4\times 5^5 \\ = & & & & & & & & & \\ & 13136 & = & 1+ & 2\times 5+ & 0\times 5^2+ & 0\times 5^3+ & 1\times 5^4+ & 4\times 5^5 \end{array}$$

La sommation de 89 et de 13047 se fait en partant de la gauche. Les retenues sont en nombre de $r = \sum r_i = 4$ où r_i est la i-ème retenue. La plus grande puissance de 5 qui divise $\binom{13136}{89}$ est donc 5^4.

Nous pourrons alors nous poser la question de savoir quel serait le résidu de $\frac{1}{p^r}\binom{n}{m}$ modulo p. La question a été résolue (cf [6], [37]) par

Anton (1869)

Soit p^r la plus grande puissance de p qui divise le coefficient binomial $\binom{n}{m}$ et soient les entiers $n = n_0 + n_1 p + \cdots + n_d\, p^d$, $m = m_0 + m_1 p + \cdots + m_d\, p^d$ et $k = n - m = k_0 + k_1 p + \cdots + k_d\, p^d$ écrits en base p $(0 \leq n_i, m_i, k_i \leq p-1$ pour tout $i)$. Alors

$$\frac{(-1)^r}{p^r}\binom{n}{m} = \frac{n_0!}{m_0! k_0!}\ \frac{n_1!}{m_1! k_1!}\ \cdots\ \frac{n_d!}{m_d! k_d!}\ (\mathrm{mod} p).$$

Cette formule a été généralisée modulo p^q (voir [37]).

Hermite [40] (1876)

Si n est un entier impair et p un nombre premier impair alors

$$\sum_{\substack{1 \le m \le n \\ (p-1)|m}} \binom{n}{m}$$

est divisible par p.

Glaisher [36] (1899)
Il a généralisé le résultat précédent en montrant que pour tout nombre premier p, si j, k, n sont des entiers tels que $\forall 1 \le j, k \le p-1$ et $n \equiv k \bmod (p-1)$ alors

$$\sum_{\substack{1 \le m \le n \\ m \equiv j \bmod (p-1)}} \binom{n}{m} \equiv \binom{k}{j} \bmod p.$$

Carlitz (1953)
Il a donné une généralisation du théorème d'Hermite modulo p^q (voir [37]). Il a montré que si p^{q-1} divise l'entier n où q est un entier ≥ 1 et p premier impair alors

$$p + (p-1) \sum_{\substack{1 \le m \le n-1 \\ m \equiv 0 \bmod (p-1)}} \binom{n}{m} \equiv 0 \bmod p^q.$$

Fleck (1913) **(voir [37])**
Etant donné un nombre premier p et des entiers $1 \le j \le p-1 < n$, on a

$$\sum_{m \equiv j \bmod p} \binom{n}{m} (-1)^m \equiv 0 \bmod p^q,$$

où $q = \lfloor (n-1)/(p-1) \rfloor$, ($\lfloor x \rfloor$ désigne la partie entière de x).

Bhaskaran (1965)
Si p est un nombre premier impair alors $(p+1)$ divise l'entier n si et seulement si

$$\sum_{m \equiv j \bmod (p-1)} \binom{n}{m} (-1)^{(m-j)/(p-1)} \equiv 0 \bmod p,$$

pour tout $j = 1, 3, 5, \ldots, p-2$ (voir [37]).

5.2 Formule de congruence de Lucas

Soit p un nombre premier. Pour tout entier $1 \leq k \leq p-1$, le coefficient binomial $\binom{p}{k}$ est divisible par p. Par conséquent $(1+x)^p = 1+x^p$ modulo p. Soient $n = n_0 + n_1 p$ et $k = k_0 + k_1 p$ deux entiers tels que $n_0, n_1, k_0, k_1 \in \mathbb{N}$ avec $0 \leq n_0, k_0 < p$. Le polynôme $(1+x)^n$ s'écrit $(1+x)^n = (1+x^p)^{n_1}(1+x)^{n_0}$ modulo p. Par identification des coefficients de x^k dans les deux expressions, il en résulte la formule suivante

$$\left(\begin{array}{c} n \\ k \end{array} \right) = \left(\begin{array}{c} n_0 + n_1 p \\ k_0 + k_1 p \end{array} \right) \equiv \left(\begin{array}{c} n_0 \\ k_0 \end{array} \right) \left(\begin{array}{c} n_1 \\ k_1 \end{array} \right) \bmod p, \tag{5.1}$$

qui se généralise, par itération, aux entiers $n = n_0 + n_1 p + \cdots n_m p^m$ et $k = k_0 + k_1 p + \cdots k_m p^m$ avec $0 \leq n_i, k_i < p \ \ (0 \leq i \leq m-1)$ par l'expression

$$\left(\begin{array}{c} n \\ k \end{array} \right) \equiv \left(\begin{array}{c} n_0 \\ k_0 \end{array} \right) \left(\begin{array}{c} n_1 \\ k_1 \end{array} \right) \cdots \left(\begin{array}{c} n_m \\ k_m \end{array} \right) \bmod p, \tag{5.2}$$

connue sous le nom de formule de congruence de Lucas apparue dans son fascicule intitulé "Théorie des fonctions numériques simplement périodiques" dans la revue "American Journal of Mathematics" en 1878 (voir [51]). C'est pour rendre hommage au mathématicien français Edouard Lucas $(1842-1891)$ que la formule 5.2 porte son nom.

En 1869, H. Anton [6] a montré que si n, m sont des entiers et p un nombre premier alors

$$\binom{n}{m} \equiv \binom{n \ div \ p}{m \ div \ p} \binom{n \bmod p}{m \bmod p} \bmod p, \tag{5.3}$$

où $n \ div \ p$ désigne la partie entière de $\dfrac{n}{p}$ et $n \bmod p$ désigne le reste de la division de n par p.

Cette formule est une forme équivalente de la congruence (5.1). La formule de Lucas apparait donc comme une généralisation de la formule d'Anton.

Il existe plusieurs preuves de la formule de Lucas. Des preuves utilisant des techniques algébriques et de théorie des nombres (voir [31], [49] et [47]) et des preuves combinatoires (voir [39] et [4]).

La formule de Lucas est considérée comme une congruence très importante dans la théorie combinatoire des nombres. Nous allons donner quelques uns des nombreux développements et extensions qu'elle a connus ainsi que certaines de ces applications en théories des nombres et en combinatoire. Nous conclurons ce chapitre par la présentation de notre contribution, qui consiste en une généralisation de la formule (5.2) aux coefficients bi^{s}nomiaux.

5.2.1 Quelques conséquences et extensions du théorème de Lucas

Dans toute la suite, p désigne un nombre premier. Les formules suivantes sont importantes et très utiles en combinatoire. Elles ont été démontrées (pour la plus part) indépendemment de la formule de Lucas, pourtant ce ne sont que des conséquences directes de cette dernière.

En prenant $n_0 = k_0 = 0$ dans la formule (5.1), nous avons pour tous entiers n et m :

$$\binom{np}{mp} \equiv \binom{n}{m} \bmod p. \tag{5.4}$$

Cette congruence a été proposée sous forme d'un problème (le problème $A-5$) au concours universitaire William Powell Putnam Mathematical Competion en 1979 (voir [75]). La solution proposée n'utilise pas directement la formule de congruence de Lucas.

Il vient par récurrence, que pour tout entier k

$$\binom{np^k}{mp^k} \equiv \binom{n}{m} \bmod p. \tag{5.5}$$

En 2011, A. Nowicki [64] a noté que si $n = n_0 + n_1 p + \cdots + n_s p^s$ est l'écriture p-adique de l'entier n alors pour tout $0 \leq k \leq s$

$$\binom{n}{p^k} \equiv \left\lfloor \frac{n}{p^k} \right\rfloor \bmod p. \tag{5.6}$$

Et par conséquent, pour $k = 1$,

$$\binom{n}{p} \equiv \left\lfloor \frac{n}{p} \right\rfloor \bmod p. \tag{5.7}$$

Il suffit juste de remarquer que la partie entière $\lfloor \frac{n}{p^k} \rfloor$ de $\frac{n}{p^k}$ est égale à $n_k + n_{k+1}p + \cdots + n_s p^{s-k}$ et ensuite d'appliquer la formule (5.2) pour avoir (5.6).

La congruence (5.7) a été proposée par L. E. Clarke [21] en 1956 sous forme d'un problème. Il a été résolu par P. A. Piza [65] en 1957.

Nous signalerons au passage, qu'en 2010 M. P. Saika et J. Vogrinc [70] ont démontré qu'un entier $p \geq 2$ est premier si et seulement s'il vérifie la congruence (5.7) pour tout entier n.

A. Nowicki a aussi noté que si $0 \leq r < p^f$ et $0 \leq m < p^f$, où f est un entier ≥ 1, alors, pour tout a dans $\mathbb{N}$, la formule de Lucas entraine

$$\binom{ap^f + r}{m} \equiv \binom{r}{m} \bmod p. \tag{5.8}$$

Supposons maintenant que $0 \leq r < p^f$ et que $m \geq p^f$ alors, à partir de l'écriture p-adique de m et de r, la formule de Lucas donne

$$\binom{p^f + r}{m} \equiv \binom{r}{m - p^f} \bmod p \tag{5.9}$$

Certaines des preuves de la Formule de Lucas n'utilisent pas la congruence

$$\binom{p}{k} \equiv 0 \bmod p, \quad (\ 1 \leq k \leq p-1), \tag{5.10}$$

celle-ci en est donc une conséquence immédiate.

Elle a été généralisée dans [13], théorème 24, à

$$\binom{p^f}{k} \equiv 0 \bmod p, \quad (\ 1 \leq k \leq p^f - 1). \tag{5.11}$$

En fait, il suffit juste de prendre $r = 0$ et $a = 1$ dans la formule (5.8).

En 1994, J. M. Holte [41] propose la version suivante du théorème de Lucas : il définit les entiers $B(m, n)$ par

$$B(m, n) = \binom{m+n}{m} = \frac{(m+n)!}{m!n!}$$

et montre alors que

$$B(m, n) \equiv B(m \ div \ p, n \ div \ p)\ B(m \mod p, n \mod p) \bmod p, \tag{5.12}$$

où $n \ div \ p$ est la partie entière de $\dfrac{n}{p}$. De plus, si $n = n_0 + n_1 p + \cdots + n_s p^s$ et $m = m_0 + m_1 p + \cdots + m_s p^s$ sont les dévéloppements p-adiques respectifs de n et m alors

$$B(m, n) \equiv B(m_0, n_0) B(m_1, n_1) \cdots B(m_s, n_s) \bmod p. \tag{5.13}$$

Conséquence : p divise $B(m, n)$ si et seulement si p divise $B(m_i, n_i)$ pour un certain $0 \leq i \leq s$.

La congruence qui suit est une extension du théorème de Lucas. Elle a été établie en 2006 par T. J. Evans [29, Théorème 3]. Soient $n \geq 1, m, M, m_0, r, R, r_0$ des entiers tels que $m = Mn + m_0$ et $r = Rn + r_0$ avec $0 \leq m_0, r_0 \leq n$ alors

$$\sum_{d|n} \varphi\left(\frac{n}{d}\right) \sum_{j=-(d-1)}^{d-1} \sum_{\|a\|_d = R-(j/d)} \binom{M}{a_1} \cdots \binom{M}{a_d} \binom{m_0}{r_0 + (n/d)j} \equiv 0 \bmod n \tag{5.14}$$

où les d sont des diviseurs de n, φ la fonction indicatrice d'Euler et pour tout $a = (a_1, \cdots, a_d)$ dans $\mathbb{N}^d$

$$\|a\|_d = \frac{n}{d} \sum_{k=1}^{d} a_j.$$

Dans [29, Corollaire 3], T. J. Evans prouve que la formule de Lucas découle de la congruence (5.14).

5.2.2 Formule de Lucas modulo des puissances de p

Un des aspects auquel se sont intéressé les auteurs, concernant la formule de congruence de Lucas, est l'établissement de variantes de cette formule modulo des puissances du nombre premier p.

En 1990, D. F. Bailey a prouvé dans [8] que si n, m sont des entiers naturels alors

$$\binom{np}{mp} \equiv \binom{n}{m} \bmod p^2. \tag{5.15}$$

En adaptant les techniques utilisées dans la preuve de ce résultat, il a démontré que si $p \geq 5$ alors

$$\binom{np}{mp} \equiv \binom{n}{m} \bmod p^3. \tag{5.16}$$

Il faut préciser que cette dernière congruence est antérieure à 1990, elle fut établie en 1949 par Ljunggren [16]. Elle a, ensuite, été améliorée en 1952 par E. Jacobsthal [37] modulo p^t où t est la plus grande puissance de p divisant $p^3nm(n-m)$ (lorsque n est supérieur à m).

On pourrait se poser la question de savoir, pour n_0 et m_0 des entiers strictement plus petits que p, si $\binom{np+n_0}{mp+m_0}$ est congru à $\binom{n}{m}\binom{n_0}{m_0}$ modulo p^2 comme l'affirme la formule de Lucas modulo p. Il se trouve qu'il n'en est rien. Dans [9], Bailey a montré que si n, m, m_0 sont des entiers avec m_0 strictement plus petit que p alors

$$\binom{np}{mp+m_0} \equiv (m+1)\binom{n}{m+1}\binom{p}{m_0} \bmod p^2. \tag{5.17}$$

Cependant, toujours dans [8], l'auteur a prouvé que si l'on mettait p^2 au lieu de p dans le terme de gauche alors

$$\binom{np^2+n_0}{mp^2+m_0} \equiv \binom{n}{m}\binom{n_0}{m_0} \bmod p^2, \tag{5.18}$$

et que si de plus $p \geq 3$ alors

$$\binom{np^3+n_0}{mp^3+m_0} \equiv \binom{n}{m}\binom{n_0}{m_0} \bmod p^3. \tag{5.19}$$

Ces deux dernières congruences ont été généralisées en 1993 par K. Davis et W. Webb modulo p^k avec $p \geq 5$ et $k \geq 1$. Ils ont montré (voir [24]) que pour tous entiers n, m, a, b, s avec $0 \leq a, b < p^s$ et n, m, s non nuls alors

$$\binom{np^{k+s}+a}{mp^{k+s}+b} \equiv \binom{np^k}{mp^k}\binom{a}{b} \bmod p^{k+1}. \tag{5.20}$$

Une conséquence de ce résultat [24, Corollaire 1] est que sous les mêmes conditions

$$\binom{np^{k+s}+a}{mp^{k+s}+b} \equiv \binom{np^{\lfloor k/3 \rfloor}}{mp^{\lfloor k/3 \rfloor}}\binom{a}{b} \bmod p^{k+1}. \tag{5.21}$$

En 1988, R. A. Macleod [54] a démontré la généralisation suivante du théorème de Lucas : soient $r \in \mathbb{N}^*$ et $M = \sum_{i=0}^{k} M_i p^{ir}$, avec $0 \leq M_i < p^r$ pour tout $i = 0, 1, ..., k$.

Alors pour tout entier N tel que $0 \leq N \leq M$,

$$\binom{N}{M} \equiv \sum \binom{p^{r-1}M_0}{N_0}\binom{p^{r-1}M_1}{N_1}\cdots\binom{p^{r-1}M_k}{N_k} \bmod p^r, \tag{5.22}$$

la sommation se fait sur tous les $(k+1)-$uplets $(N_0, N_1, ..., N_k)$ tels que $p^{r-1}N = \sum_{i=0}^{k} N_i p^{ir}$, avec $0 \leq N_i < p^{r-1}M_i$ pour tout $i = 0, 1, ..., k$.

Notons que si l'on prend $r = 1$, on retrouve exactement la formule de congruence de Lucas.

5.2.3 Quelques applications de la formule de congruence de Lucas

Formule de Lucas et triangle de Pascal

Considérons le triangle de Pascal où chaque coefficient est un $\binom{n}{m}$

n/m	0	1	2	3	4	5	6	7	8
0	1								
1	1	1							
2	1	2	1						
3	1	3	3	1					
4	1	4	6	4	1				
5	1	5	10	10	5	1			
6	1	6	15	20	15	6	1		
7	1	7	21	35	35	21	7	1	
8	1	8	28	56	70	56	28	8	1

Triangle de Pascal.

Soit $a_k(n)$ le nombre d'entiers $m \in \{0, 1, ..., n\}$ tels que $\binom{n}{m} \not\equiv 0 \bmod k$, $(k \neq 0)$. Donc $a_k(n)$ est le nombre d'entiers non congrus à 0 modulo k parmi les coefficients qui figurent dans la ligne n du triangle de Pascal. Par exemple $a_2(5) = 4$, et $a_4(6) = 6$. Soient $n = \sum_{i=o}^{s} n_i k^i$ la représentation en base k de l'entier n et $|n|_q$ le nombre de fois où le chiffre q apparait dans la suite $n_0, n_1, ..., n_s$. Par exemple, en base 2, $|4|_0 = 2$ et $|4|_1 = 1$. J. W. L. Glaisher [36] est le premier, en 1899, à s'intéresser au "difficile" problème de la détermination des $a_k(n)$. Il a montré, à l'aide du théorème de Lucas (voir [69]) que

$$a_2(n) = 2^{|n|_1}. \tag{5.23}$$

La preuve consiste à dire que si $m = \sum_{i=o}^{s} m_i 2^i$ alors, par la formule de Lucas, pour avoir $\binom{n}{m}$ congru à 1 modulo 2 il faut que, pour tout $0 \leq i \leq s$, $\binom{n_i}{m_i}$ soit égal à 1. Par suite si $n_i = 0$ alors $m_i = 0$ et si $n_i = 1$ alors soit $m_i = 0$ soit $m_i = 1$.

En 1947, N. J. Fine [31] généralise le résultat de Glaisher à un nombre premier quelconque. Il montre en utilisant la formule de Lucas que si $n = \sum_{i=o}^{s} n_i p^i$ alors

$$a_p(n) = \prod_{i=o}^{s} (n_i + 1). \tag{5.24}$$

Il note que cette formule est équivalente à

$$a_p(n) = \prod_{r=o}^{p-1} (r+1)^{|n|_r}. \tag{5.25}$$

D'où la formule (5.23) lorsque $p = 2$.

La formule de Glaisher a été généralisée en 2011 par A. Rowland [69] de la manière suivante : si $a_{k,r}(n)$ est le nombre d'entiers $0 \leq m \leq n$ pour lesquels $\binom{n}{m} \equiv r \bmod k$ et $\alpha \in \mathbb{N}^*$ alors

$$a_{p^\alpha}(n) = \prod_{r=1}^{p^\alpha - 1} a_{p^\alpha, r}(n). \tag{5.26}$$

Autres applications de la formule de Lucas.

En utilisant le théorème de Lucas, K. Dilcher [27] a montré en 2007 que si p est un nombre premier ≥ 3 et q un entier naturel non nul alors

$$\sum_{j=0}^{\lfloor q/2 \rfloor} \binom{q(p-1)}{2j(p-1)} \equiv \begin{cases} 1 \bmod p & \text{si } q \text{ est impair,} \\ 2 \bmod p & \text{si } q \text{ est pair et } \ q \not\equiv 0 \bmod (p+1), \\ \frac{3}{2} \bmod p & \text{si } p+1 \mid q. \end{cases} \tag{5.27}$$

En 2009, R. Meštrović [57] a prouvé que si d et q sont deux entiers ≥ 2 tels que

$$\binom{nd}{md} \equiv \binom{n}{m} \bmod q,$$

pour tous entiers $n \geq m \geq 0$, alors d et q sont des puissances du même nombre premier p. Ce résultat peut être considéré partiellement, comme l'inverse de la congruence (5.5).

Dans son fascicule "Théorie des fonctions numériques simplement périodiques" E. Lucas a montré en 1878 que si p est un nombre premier alors pour tout $k \in \{0, 1, ..., p-1\}$

$$\binom{p-1}{k} \equiv (-1)^k \bmod p.$$

R. Meštrović [58] a généralisé ce résultat en 2014 à toute puissance de p en démontrant, à l'aide de la formule de congruence de Lucas, que

$$\binom{p^f - 1}{k} \equiv (-1)^k \bmod p, \tag{5.28}$$

pour tout entier non nul f.

Il a aussi prouvé dans le même papier, en utilisant toujours la formule de Lucas, que si n et q sont deux entiers > 1 tels que

$$\binom{n-1}{k} \equiv (-1)^k \bmod q,$$

pour tout $k \in \{0, 1, ..., n-1\}$ alors q est premier et n est une puissance de q. Il a ainsi résolu le problème 1494 du "Mathematics Magazine" proposé par E. Deutsch et I. M. Gessel en 1997.

5.3 Coefficients bi^{s}nomiaux

Notre contribution, dans ce cadre, voir [1], consiste en une généralisation de la formule de Lucas aux coefficients bi^{s}omiaux qui sont une extension naturelle des coefficients binomiaux. Nous allons commencer par introduire ces nombres et donner quelques unes de leurs propriétés.

Soient s, n dans $\mathbb{N}$, avec s non nul. Pour un entier $k = 0, 1, ..., sn$, le coefficient bi^{s}nomial $\binom{n}{k}_s$ est le k-ème terme de l'expression multinomiale suivante

$$(1 + x + x^2 + \cdots + x^s)^n = \sum_{k \geq 0} \left(\begin{array}{c} n \\ k \end{array} \right)_s x^k, \tag{5.29}$$

en d'autres termes, c'est le coefficient de x^k dans le développement de $(1 + x + x^2 + \cdots + x^s)^n$ avec $\binom{n}{k}_1 = \binom{n}{k}$ (le coefficient binomial) et $\binom{n}{k}_s = 0$ pour $k > sn$.

Dans [37] page 14, Granville définit des entiers, qu'il note $\binom{n}{k}_f$, dont les bi^{s}nomiaux sont un cas particulier. Etant donné un polynôme f de degré s à coefficients entiers, $\binom{n}{k}_f$ est défini comme étant le coefficient de x^k dans le développement de $f(x)^n$ en puissances de x i.e. $f(x)^n = \sum_{k=0}^{ns} \binom{n}{k}_f x^k$ avec $\binom{n}{k}_f = 0$ lorsque $k < 0$ ou $k > ns$. Dans le cas où $f(x) = 1 + x$ (respectivement $f(x) = 1 + x + \cdots + x^s$) le coefficient $\binom{n}{k}_f$ est le coefficient binomial (respectivement le coefficient bi^{s}nomial).

Les auteurs s'accordent à dire que, dans la littérature, les premières traces de ces entiers remontent à 1730 dans un article de de Moivre [25]. Il y montre que lors d'un jet de L dés, ayant chacun $(s + 1)$ faces, la probabilité que la somme des nombres obtenus sur les faces des dés soit égale à k est

$$\binom{L}{k - L}_s \Big/ (s + 1)^L.$$

C'est, semble-t-il, de la résolution de ce problème probabiliste que sont nés les bi^{s}nomiaux.

L'équation qui suit et qui se trouve dans le même papier donne une interprétation de ces nombres en fonction des coefficients binomiaux (voir aussi [23] et [12])

$$\binom{L}{k}_s = \sum_{j=0}^{\lfloor \frac{k}{(s+1)} \rfloor} (-1)^j \binom{L}{j} \binom{k - j(s+1) + L - 1}{L - 1}. \tag{5.30}$$

Cette formule est obtenue par identification des coefficients de x^k dans la formule (5.29) et dans la formule (5.31) qui suit

$$\begin{aligned}(1+x+x^2+\cdots+x^s)^L &= (1-x^{s+1})^L(1-x)^{-L} \\ &= \left(\sum_{j=0}^{L}(-1)^j\binom{L}{j}x^{j(s+1)}\right)\left(\sum_{j\geq 0}\binom{j+L-1}{L-1}x^j\right).\end{aligned} \tag{5.31}$$

Le coefficient bi^{s}nomial vérifie la propriété de symétrie

$$\left(\begin{array}{c} n \\ k \end{array}\right)_s = \left(\begin{array}{c} n \\ sn-k \end{array}\right)_s. \tag{5.32}$$

C'est Euler [28] qui a remarqué cette symétrie des coefficients bi^{s}nomiaux (voir aussi Tremblay [76], Bollanger [14], Belbachir [12]). Il suffit, pour l'établir, de remplacer x par $\frac{1}{y}$ dans la formule (5.29) puis de multiplier les deux membres de l'équation par y^{ns} pour obtenir

$$(1+y+y^2+\cdots+y^s)^n = \sum_{k\geq 0}\left(\begin{array}{c} n \\ sn-k \end{array}\right)_s y^k. \tag{5.33}$$

Euler a donné aussi une relation entre $\binom{n}{k}_s$ et $\binom{n}{k}_{s-1}$. Il lui a suffit pour cela d'écrire

$$(1+x+x^2+\cdots+x^s)^n = (1+x(1+x+x^2+\cdots+x^{s-1}))^n$$

et de récupérer le coefficient de x^k au niveau du second membre de l'égalité. D'où la formule de récurrence diagonale

$$\left(\begin{array}{c} n \\ k \end{array}\right)_s = \sum_{m=0}^{k}\left(\begin{array}{c} n \\ m \end{array}\right)\left(\begin{array}{c} m \\ k-m \end{array}\right)_{s-1}. \tag{5.34}$$

En utilisant la formule (5.34), nous déduisons par récurrence sur s, la formule suivante, qui est une autre expression des coefficients bi^{s}nomiaux comme somme de coefficients binomiaux

$$\left(\begin{array}{c} n \\ k \end{array}\right)_s = \sum_{j_1+j_2+\cdots+j_s=k}\left(\begin{array}{c} n \\ j_1 \end{array}\right)\left(\begin{array}{c} j_1 \\ j_2 \end{array}\right)\cdots\left(\begin{array}{c} j_{s-1} \\ j_s \end{array}\right). \tag{5.35}$$

Le coefficient bi^{s}nomial $\binom{n}{k}_s$ vérifie la relation de récurrence longitudinale, parfois appelée formule de Pascal généralisée, dont une preuve combinatoire est donnée par Freund (voir [35])

$$\left(\begin{array}{c} n \\ k \end{array}\right)_s = \sum_{m=0}^{s}\left(\begin{array}{c} n-1 \\ k-m \end{array}\right)_s. \tag{5.36}$$

La formule (5.36) permet la construction du triangle des coefficients bi^{s}nomiaux qui est une extension du triangle de Pascal pour les binomiaux. Par exemple, les triangles des coefficients

trinomiaux , quadrinomiaux et pentanomiaux qui correspondent respectivement à $s = 2,\ s = 3$ et $s = 4$ sont :

Table 1 : triangle des coefficients trinomiaux $\binom{n}{k}_2$.

n/k	0	1	2	3	4	5	6	7	8	9	10
0	1										
1	1	1	1								
2	1	2	3	2	1						
3	1	3	6	7	6	3	1				
4	1	4	10	16	19	16	10	4	1		
5	1	5	15	30	45	51	45	30	15	5	1

Table 2 : triangle des coefficients quadrinomiaux $\binom{n}{k}_3$.

n/k	0	1	2	3	4	5	6	7	8	9	10	11	12
0	1												
1	1	1	1	1									
2	1	2	3	4	3	2	1						
3	1	3	6	10	12	12	10	6	3	1			
4	1	4	10	20	31	40	44	40	31	20	10	4	1

Table 3 : triangle des coefficients pentanomiaux $\binom{n}{k}_4$.

n/k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	1																
1	1	1	1	1	1												
2	1	2	3	4	5	4	3	2	1								
3	1	3	6	10	15	18	19	18	15	10	6	3	1				
4	1	4	10	20	35	52	68	80	85	80	68	52	35	20	10	4	1

5.4 Généralisation du théorème de Lucas aux bi^{s}nomiaux

L'objet de ce paragraphe est d'établir deux résultats (voir [1]) qui sont des extensions des formules (5.1) et (5.2) aux coefficients bi^{s}nomiaux $\binom{n}{k}_s$. Dans le sens où lorsque l'on remplace s par 1 on retrouve les expressions (5.1) et (5.2).

Théorème 5.1. *Soient $s \in \mathbb{N}^*$, p un nombre premier, $n = n_0 + n_1 p$ et $k = k_0 + k_1 p$ deux entiers tels que $n_0, n_1, k_0, k_1 \in \mathbb{N}$ et $0 \leq n_0, k_0 < p$. Alors*

$$\binom{n}{k}_s \equiv \sum_{i=0}^{s-1} \binom{n_0}{k_0 + ip}_s \binom{n_1}{k_1 - i}_s \bmod p. \tag{5.37}$$

Preuve. A l'aide d'une récurrence sur l'entier s, $(1+x+x^2+\cdots+x^s)^p \equiv 1+x^p+\cdots+x^{sp} \bmod p$.

Par suite

$$\begin{aligned}
(1 + x + \cdots + x^s)^n &= (1 + x + \cdots + x^s)^{n_1 p}(1 + x + \cdots + x^s)^{n_0} \\
&\equiv (1 + x^p + \cdots + x^{sp})^{n_1}(1 + x + \cdots + x^s)^{n_0} \bmod p \\
&\equiv \sum_{i=0}^{sn_1} \binom{n_1}{i}_s x^{ip} \sum_{j=0}^{sn_0} \binom{n_0}{j}_s x^j \bmod p \\
&\equiv \sum_{k=0}^{sn} \sum_{ip+j=k} \binom{n_1}{i}_s \binom{n_0}{j}_s x^k \bmod p
\end{aligned}$$

Par identification avec $\sum_{k=0}^{sn} \binom{n}{k}_s x^k$, on obtient la relation

$$\binom{n}{k}_s \equiv \sum_{ip+j=k} \binom{n_1}{i}_s \binom{n_0}{j}_q \bmod p.$$

L'égalité $ip + j = k_1 p + k_0$ $(0 \leq j \leq qn_0 < sp)$ entraîne $(i = k_1$ et $j = k_0)$ ou $(i < k_1$ et $j > k_0)$. Le second cas implique $p(k_1 - i) = j - k_0$ et donc p divise $j - k_0$.

On conclut que $(i, j) \in \{(k_1, k_0), (k_1 - 1, k_0 + p), ..., (k_1 - s + 1, k_0 + (s-1)p)\}$.

Par suite

$$\binom{n}{k}_s \equiv \sum_{i=0}^{s-1} \binom{n_0}{k_0 + ip}_s \binom{n_1}{k_1 - i}_s \bmod p.$$

□

Le résultat qui suit généralise le théorème précédent et représente l'analogue du théorème de congruence de Lucas pour les bi^{s}nomiaux.

Théorème 5.2. *Soient p un nombre premier, $n = n_0 + n_1 p + \cdots + n_m p^m$, $k = k_0 + k_1 p + \cdots + k_m p^m$ tels que $0 \leq n_i,\ k_i < p$ $(0 \leq i \leq m-1)$ et n_m, k_m dans $\mathbb{N}$. Alors*

$$\binom{n}{k}_s \equiv \sum_{0 \leq i_0, i_1, \ldots, i_{m-1} \leq s-1} \prod_{j=0}^{m} \binom{n_j}{kj + i_j p - i_{j-1}}_s \bmod p, \tag{5.38}$$

avec $i_{-1} = 0$ et $i_m = 0$.

Preuve.

Pour $m = 1$, nous retrouvons la formule (5.37) du théorème 5.1.

Supposons l'identité (5.38) vraie à l'ordre m. Ecrivons $n = n_0 + n_1 p + \cdots + n_{m+1} p^{m+1}$ et $k = k_0 + k_1 p + \cdots + k_{m+1} p^{m+1}$. D'après le théorème 5.1 nous avons

$$\binom{n}{k}_s \equiv \sum_{i=0}^{s-1} \binom{n_0}{k_0 + i_0 p}_s \binom{n_1 + n_2 p + \cdots + n_{m+1} p^m}{k_1 - i_0 + k_2 p + \cdots + k_{m+1} p^m}_p \bmod p.$$

L'hypothèse de récurrence implique alors

$$\begin{aligned}
\binom{n}{k}_s &\equiv \sum_{i=0}^{s-1} \binom{n_0}{k_0 + i_0 p}_s \sum_{0 \le i_1, i_2, \ldots, i_m \le s-1} \binom{n_1}{k_1 + i_1 p - i_0}_s \prod_{j=2}^{m+1} \binom{n_j}{kj + i_j p - i_{j-1}}_s \bmod p \\
&\equiv \sum_{0 \le i_1, i_2, \ldots, i_m \le s-1} \sum_{i=0}^{s-1} \binom{n_0}{k_0 + i_0 p}_s \binom{n_1}{k_1 + i_1 p - i_0}_s \prod_{j=2}^{m+1} \binom{n_j}{kj + i_j p - i_{j-1}}_s \bmod p \\
&\equiv \sum_{0 \le i_0, i_1, \ldots, i_m \le s-1} \prod_{j=0}^{m+1} \binom{n_j}{kj + i_j p - i_{j-1}}_s \bmod p
\end{aligned}$$

avec $i_{-1} = 0$ et $i_{m+1} = 0$. □

Bibliographie

[1] M. Abchiche, H. Belbachir *Generalized Lucas'theorem.* Ars combinatoria, **(120)** (2015), 413–416.

[2] M. Abchiche, H. Belbachir *Generalized Chebyshev Polynomials.* Discussiones Mathematicae. General Algebra and Applications, **(38)** (2018), 79–89.

[3] Y. Amice, *Les nombres p-adiques.* Presses Universitaires de France, (1975).

[4] P. G. Anderson, A. T. Benjamen, J. A. Rousse, *A Combinatorial proofs of Fermat's, Lucas's and Wilson's theorems,* Amer. Math. Monthly **(112)** (2005), 266–268.

[5] G. E. Andrews, J. Baxter, *Lattice gas generalisation of the hard hexagon model III q-trinomials coefficients.* J. Stat. Phys., **(47)** (1987) 297–330.

[6] H. Anton, *Die Elferprobe und die Proben fur die Modul Neun, 9, 13 and 101.* Dreizehn und Hunderteins. Fur Volksund Mittelschulen, Archiv Math. Physik, **(49)** (1869) 241–308.

[7] C. Babbage, *Demonstration of a theorem relating to prime numbers,* Edinburgh Philosophical J. 1, (1819), 46–49.

[8] D. F. Bailey, *Two p^3 variationsof Lucas' theorem,* J. Number Theory, **(35)** (1990), 208–215.

[9] D. F. Bailey, *Some binomial coefficient congruences,* Appl. Math. Letters **(4)**, no. 4 (1991), 1–5.

[10] H. Belbachir, F. Bencherif, *Linear recurrent sequences and powers of square matrix.* Integers, **(6)** (A12) (2006), 1–17.

[11] H. Belbachir, F. Bencherif, *On some properties of Chebyshev polynomials.* Discussiones Mathematicae. General Algebra and Applications, **(28)** (2008), 121–133.

[12] H. Belbachir, S. Bouroubi, A. Khelladi, *Connection between bi^{s}nomial coefficients, Fibonacci numbers, Bell polynomials and discrete uniform distribution.* Annales Mathematicae et Informaticae, **(35)** (2008), 21–30.

[13] A. T. Benjamin, J. J. Quinn, *Proofs That Really Coubt, The Art of Combinatorial proofs,* Mathematical Asssociation of America, Providence, 2003.

[14] R. C. Bollinger, *A note on Pascal T-triangles, Muktinomial coefficients and Pascal Pyramids.* The Fibonacci Quarterly, **(24)** (1986), 140–144.

[15] Z. I. Borevitch, I. R. Chafarevitch, *Théorie des nombres.* Gauthier-Villars Paris, (1967).

[16] V. Brun, J. O. Stubban, J. E. Fjeldstad, R. Tambs Lyche, K. E. Aubert, W. Ljunggren, E. Jacobsthal, *On the divisibility of the difference between two binomial coefficients.* Den 11te Skandinaviske Matematikerkongress, Trondheim, (1949), 42–54. Johan Grundt Tanums Forlag, Oslo, 1952.

[17] P. F. Byrd, *Expansion of analytic functions in polynomials associated with Fibonacci numbers.* The Fibonacci Quarterly, **(1)** (1963), No. 1, 16–29.

[18] S. Chowla, B. Dwork, R. Evans, *On mod p^2 determination of $\binom{(p-1)/2}{(p-1)/4}$* . J. of Number Theory, **(24)** (1986), 188–196.

[19] L. Cerlienco, M. Mignotte, F. Piras, *Suites récurrentes linéaires ; propriétés algébriques et arithmétiques.* Enseign. Math., **t. (33)** (1987), 67–108.

[20] C. Cesarano, *Identities and generating functions on Chebyshev polynomials.* Georgian Math.J. **(19)** (2012), 427–440.

[21] L. E. Clarke, *Problem 4704,* Amer. Math. Monthly, **(63)** (1956), p.584 ; Solution, ibid **(64)** (1957), 597–598.

[22] P. Colmez, *Les nombres p−adiques.* Notes du cours de M2.
https ://webusers.imj-prg.fr/ pierre.colmez/nombres-p-adiques

[23] L. Comtet, *Analyse combinatoire.* Puf, Coll.Sup. Paris (1970), Vol. 1 & Vol. 2.

[24] K. S. Davis, W. A. Webb, *A binomial coefficient congruence modulo prime powers,* J. Number Theory, **(43)** (1993), 20–23.

[25] A. de Moivre, *The Doctrine of Chances : or, A Method of Calculating the Probabilities of events in Play.* 3*rd ed.* London : Millar, (1756) ; rpt. New York : Chelsea,1967.

[26] L. E. Dickson, *History of the theory of numbers.* AMS Chelsea publishing, volume 1 (2000).

[27] K. Dilcher, *Congruences for a class of alternating lacunary sums of binomial coefficients,* J. integer Sequences **(10)** (2007), Article 07.10.1.

[28] L. Euler, *Observationes analyticae,* Novi Commentarrii Academiae Scientarum Petropolitanae, **(11)** (1767), 124143, Opera Omnia, Serie 1 Vol.15, 50 -69.

[29] T. J. Evans, *On some generalizations of Fermat's, Lucas's and Wilson's theorem,* Ars Combinatoria **(79)** (2006), 189–194.

[30] L. Fibonacci *Liber abaci.* (1202).

[31] N. J. Fine, *Binomial coefficients modulo a prime,* Amer. Math. Monthly **(54)** (1947), 589–592.

[32] H. T. Freitag, *A Property of Unit Digits of Fibonacci Numbers.* Proceedings of the First International Conference on Fibonacci Numbers and Their Applications, University of Patras, Patras, Greece, August (1984), 27–31.

[33] H. T. Freitag, G. M. Phillips, *A Congruence Relation for Certain Recursive Sequences.* Fibonacci Quarterly **(24)** (1986), 332–335.

[34] H. T. Freitag, G. M. Phillips, *A Congruence Relation for a Linear Recursive Sequence of arbitrary Order.* Application of Fibonacci Numbers (1988), 39–44.

[35] J. E. Freund, *Restricted Occupancy.Theory - A Generalization of Pascal's Triangle.* Amer. Math. Monthly. **(63)** No. 1 (1956), 2–27.

[36] J. W. L. Glaisher, *On the residues of a binomial-theorem coefficients,* Q. J. Pure Appl. Math. **(30)** (1899), 150–156.

[37] A. Granville, *Arithmetic Properties of Binomial Coefficients I : Binomial coefficients modulo prime powers, in Organic Mathematics (Burnaby, BC, 1995),* CMS Conf. Proc., vol 20, American Mathematical Society, Providence, RI. (1997) 253–275.

[38] S. Gupta, P. Rockstroh and F. E. Su, *Splitting Fields and Periods Of Fibonacci sequences modulo primes,* Matematics Magazine vol. (85,) Nř (2), (2012), 130–135.

[39] M. Hausner, *Application of a simple of counting technique,* Amer. Math. Monthly **(90)** (1983), 127–129.

[40] Ch. Hermite, *Extrait d'une lettre à M. Brochardt,* J. Reine Angew. Math., **(81)** (1876), 93–95.

[41] J. M. Holte, *A Lucas-type theorem for Fibonomial-coefficient résidues,* Fibonacci Quart. **(32)**, no 1 (1994), 60–68.

[42] N. Koblitz. *p−adique numbers, p−adique analysis and zeta-functions.* volume 58 of Graduate Texts in Mathematics. Springer-Verlag, New-York, second edition, (1984).

[43] T. Koshy, *Fibonacci and Lucas Numbers with Applications.* A Wiley Interscience Publications. John Wiley and Soons, Inc., (2001).

[44] T. Koshy, *Pell and Pell-Lucas Numbers with Applications.* Springer, (2010).

[45] E. E. Kummer, *Über die Ergänzungssatze zu den allgemeinen Reciprocitätsgesetzen,* J. Reine Angew. Math., **(44)** (1852) 93–146.

[46] V. L. Kurakin, A. S. Kuzmin, A. V. Mikhalev, A. A. Nechalev, *Linear recurring sequences over rings and modules.* J. of Math.Sci., **76(6)** (1995), 2793–2915.

[47] A. Laugier, M. P. Saikia, *A new proof of Lucas' Theorem,* Notes on Number Theory and Discrete Mathematics **(18)** no. 4 (2012), 1–6.

[48] R. Lidl and H. Nierderreiter, *Finite fields.* Cambridge University Press , (1997).

[49] S. C. Liu, J. C. C. yeh, *A Catalan numbers modulo* 2^k*,* J. Integer Sequences **(13)** (2010), Article 10.5.4.

[50] E. Lucas, *Sur les congruences des nombres eulériens et les coefficients différentiels des fonctions trigonométriques, suivant un module premier.* Bull. Soc. Math. France, **(6)** (1877-1878), 49–54.

[51] E. Lucas, *Théorie des Fonctions Numériques Simplement Périodiques.* American Journal of Mathematics, **1 (2)** (1878), 184–196 (part 1).

[52] E. Lucas, *Théorie des Fonctions Numériques Simplement Périodiques.* American Journal of Mathematics, **1 (3)** (1878) 197–240 (part 2).

[53] E.Lucas, *Théorie des Fonctions Numériques Simplement Périodiques.* American Journal of Mathematics, **1 (4)** (1878) 289–321 (part 3).

[54] R. A. Macleod, *Generalization of a result of E.Lucas,* Canad. Mathb. Bull. **(31)** , no. 1, (1988), 95–98.

[55] H. B. Mann, D. S. Shanks, *A neccessary and sufficient conditionfor primality, and itd source,* J. of Comb. Theory Ser. A, **(13)** (1972), 131–134.

[56] J. C. Mason, D. C. Handscomb, *Chebyshev Polynomials.* Chapman and Hall/CRC, (2003).

[57] R. Meštrović, *A note on the congruence* $\binom{nd}{md} \equiv \binom{n}{m} \bmod p$, Amer. Math. Monthly , **(116)** (2009), 75–77.

[58] R. Meštrović, *A primality criterion based on a Lucas' congruence ;* arXiv : 1407, 7894 v1 [math,NT], 2014.

[59] R. Meštrović, *Lucas' Theorem : Its Generalisations, Extensions and Applications (1878-2014).* arXiv : 1409, 3820 vol. 1 [math,NT], 6 sep 2014.

[60] P. Montel, *Leçons sur les récurrences et leurs applications.* Paris, Gautier-Villars , (1957).

[61] F. Morley, *Note on the congruence* $2^{4n} \equiv (-)^n(2n)!/(n!)^2$, *where 2n+1 is a prime.* Annals of Math., **9** (1895), 168–170.

[62] A. Nalli and P. Haukkanen, *On generalized Fibonacci and Lucas Polynomials.* Chaos, Solitons and Fractals, **42** (2009), 3179–3186.

[63] A. Necer, *Suites récurrentes linéaires et séries formelles en plusieurs variables.* Thése de Doctorat de l'Université de Limoges (1998).

[64] A. Nowicki, *Prodròże* po Imperium Liczb. Cz
ceść 11.Silnie i symbole New-tona (Rozdziall 7), University of Torun, Poland, (2011) ; also available at http ://www.mat.univ.torun.pl/anow.

[65] P. A. Piza, *Solution of Problem 4704,* Amer. Math. Monthly, **(64)**, no.8 (1957) 597–598.

[66] M. Renault, *The Fibonacci Sequence Under Various Moduli,* A thesis submitted to Wake Forest University in partial fulfillment of the degree of Master of Arts in Mathematics, (1996).

[67] T. J. Rivlin, *Chebyshev Polynomials : From Approximation Theory to Algebra and Number Theory.* Second edition, Wiley Interscience, (1990).

[68] A. M. Robert, *A course in p−adique analysis.* volume 198 of Graduate Texts in Mathematics. Springer-Verlag, New-York, (2000).

[69] E. Rowland, *The number of nonzero binomial coefficients modulo* p^α *;* preprint
arXiv :1310.8635v2 [math.NT.], 2014.

[70] M. P. Saikia, J. Vogrinc, *A simple number theoretic result,* J. Assam Academy of Math., **(3)** (2010), 91–96.

[71] P. Samuel, *Théorie algébrique des nombres.* Deuxième edition, Hermann, Paris, (1971).

[72] J. P. Serre, *Cours d'arithmétique.* Presses Universitaires de France, Paris, (1970).

[73] C. Smith, V. E. Hogatt, *Generating functions of central values of generalized Pascal triangles.* The Fibonacci Quarterly, **(17)** (1979) 58–67.

[74] L. Somer, *Congruence Relations for $k^{th}-$Order Linear Recurrences.* Fibonacci Quarterly **(27)** (1989), 25–31.

[75] The William Lowel Putnam, *Mathematical competition, Problem A-5,* Amer. Math. Monthly, **(86)** (1979) 171–173.

[76] A. Tremblay, *Generalization of Pascal's Arithmetical Triangle,* National Mathematics Magazine, **(11)**, No. 6, (1937), 255–258.

[77] D. D. Wall, *Fibonacci Series Modulo m,* Amer. Math. Monthly, **(67)** (1960) 525–532.

Index

Annexe A

Période $T(m)$ de la suite de Fibonacci, pour $2 \leq m \leq 1000$

m	T(m)	m	T(m)	m	T(m)	m	T(m)	m	T(m)	m	T(m)
2	3	**37**	**76**	72	24	**107**	72	142	210	177	232
3	**8**	38	18	**73**	**148**	108	72	143	140	178	132
4	6	39	56	74	228	**109**	**108**	144	24	**179**	**178**
5	20	40	60	75	200	110	60	145	140	180	120
6	24	**41**	**40**	76	18	111	152	146	444	**181**	90
7	**16**	42	48	77	80	112	48	147	112	182	336
8	12	**43**	**88**	78	168	**113**	76	148	228	183	120
9	24	44	30	**79**	**78**	114	72	**149**	**148**	184	48
10	60	45	120	80	120	115	240	150	600	185	380
11	**10**	46	48	81	216	116	42	**151**	50	186	120
12	24	**47**	32	82	120	117	168	152	36	187	180
13	**28**	48	24	**83**	**168**	118	174	153	72	188	96
14	48	49	112	84	48	119	144	154	240	189	144
15	40	50	300	85	180	120	120	155	60	190	180
16	24	51	72	86	254	121	110	156	168	**191**	**190**
17	**36**	52	84	87	56	122	60	**157**	**316**	192	96
18	24	**53**	**108**	88	60	123	40	158	78	**193**	**388**
19	**18**	54	72	**89**	44	124	30	159	216	194	588
20	60	55	20	90	120	125	500	160	240	195	280
21	16	56	48	91	112	126	48	161	48	196	336
22	30	57	72	92	48	**127**	**256**	162	216	**197**	**396**
23	**48**	58	42	93	120	128	192	**163**	**328**	198	120
24	24	**59**	**58**	94	96	129	88	164	120	**199**	22
25	100	60	120	95	180	130	420	165	40	200	300
26	84	**61**	**60**	96	48	**131**	**130**	166	168	201	136
27	72	62	30	**97**	**196**	132	120	**167**	**336**	202	150
28	48	63	48	98	336	133	144	168	48	203	112
29	14	64	96	99	120	134	408	169	364	204	72
30	120	65	140	100	300	135	360	170	180	205	40
31	**30**	66	120	**101**	50	136	36	171	72	206	624
32	48	**67**	**136**	102	72	**137**	**276**	172	264	207	48
33	40	68	36	**103**	**208**	138	48	**173**	**348**	208	168
34	36	69	48	104	84	**139**	46	174	168	209	90
35	80	70	240	105	80	140	240	175	400	210	240
36	24	**71**	**70**	106	108	141	32	176	120	**211**	42

m	T(m)	m	T(m)	m	T(m)	m	T(m)	m	T(m)	m	T(m)
212	108	256	384	300	600	344	264	388	588	432	72
213	280	**257**	**516**	301	176	345	240	**389**	**388**	**433**	**868**
214	72	258	264	302	150	346	348	390	840	434	240
215	440	259	304	303	200	**347**	232	391	144	435	280
216	72	260	420	304	72	348	168	392	336	436	108
217	240	261	168	305	60	**349**	174	393	520	437	144
218	108	262	390	306	72	350	1200	394	396	438	888
219	296	**263**	176	**307**	88	351	504	395	780	**439**	**438**
220	60	264	120	308	240	352	240	396	120	440	60
221	252	265	540	309	208	**353**	236	**397**	**796**	441	336
222	456	266	144	310	60	354	696	398	66	442	252
223	**448**	267	88	**311**	**310**	355	140	399	144	**443**	**888**
224	48	268	408	312	168	356	132	400	600	444	456
225	600	**269**	**268**	**313**	**628**	357	144	**401**	200	445	220
226	228	270	360	314	948	358	534	402	408	446	1344
227	**456**	**271**	**270**	315	240	**359**	**358**	403	420	447	296
228	72	272	72	316	78	360	120	404	150	448	96
229	114	273	112	**317**	**636**	361	342	405	1080	**449**	**448**
230	240	274	276	318	216	362	90	406	336	450	600
231	80	275	100	319	70	363	440	407	380	451	40
232	84	276	48	320	480	364	336	408	72	452	228
233	52	**277**	**556**	321	72	365	740	**409**	**408**	453	200
234	168	278	138	322	48	366	120	410	120	454	456
235	160	279	120	323	36	**367**	**736**	411	552	455	560
236	174	280	240	324	216	368	48	412	624	456	72
237	312	**281**	56	325	700	369	120	413	464	**457**	**916**
238	144	282	96	326	984	370	1140	414	48	458	114
239	**238**	**283**	**568**	327	216	371	432	415	840	459	72
240	120	284	210	328	120	372	120	416	336	460	240
241	**240**	285	360	329	32	**373**	**748**	417	184	**461**	46
242	330	286	420	330	120	374	180	418	90	462	240
243	648	287	80	**331**	110	375	1000	**419**	**418**	**463**	**928**
244	60	288	48	332	168	376	96	420	240	464	168
245	560	299	612	333	456	377	28	**421**	84	465	120
246	120	290	420	334	336	378	144	422	42	466	156
247	252	291	392	335	680	**379**	**378**	423	96	**467**	**936**
248	60	292	444	336	48	380	180	424	108	468	168
249	168	**293**	**588**	**337**	**676**	381	256	425	900	469	272
250	1500	294	336	338	1092	382	570	426	840	470	480
251	**250**	295	580	339	152	**383**	**768**	427	240	471	632
252	48	296	228	340	180	384	192	428	72	472	348
253	240	297	360	341	30	385	80	429	280	473	440
254	768	298	444	342	72	386	1164	430	1320	474	312
255	360	299	336	343	784	387	264	**431**	**430**	475	900

m	T(m)	m	T(m)	m	T(m)	m	T(m)	m	T(m)	m	T(m)
476	144	520	420	564	96	608	144	652	984	696	168
477	216	**521**	26	565	380	609	112	**653**	**1308**	697	360
478	714	522	168	566	1704	610	60	654	216	698	174
479	**478**	**523**	**1048**	567	432	611	224	655	260	699	104
480	240	524	390	568	420	612	72	656	120	700	1200
481	532	525	400	**569**	**568**	**613**	**1228**	657	888	**701**	**700**
482	240	526	528	570	360	614	264	658	96	702	504
483	48	527	180	**571**	**570**	615	40	**659**	**658**	703	684
484	330	528	120	572	420	616	240	660	120	704	480
485	980	529	1104	573	760	**617**	**1236**	**661**	220	705	160
486	648	530	540	574	240	618	624	662	330	706	708
487	**976**	531	696	575	1200	**619**	206	663	504	707	400
488	60	532	144	576	96	620	60	664	168	708	696
489	328	533	280	**577**	**1156**	621	144	665	720	**709**	118
490	680	534	264	578	612	622	930	666	456	710	420
491	**490**	535	360	579	776	623	176	667	336	711	312
492	120	536	408	580	420	624	168	668	336	712	132
493	252	537	712	581	336	625	2500	669	448	713	240
494	252	538	804	582	1176	626	1884	670	2040	714	144
495	120	539	560	583	540	627	360	671	60	715	140
496	120	540	360	584	444	628	948	672	48	716	534
497	560	**541**	90	585	840	629	684	**673**	**1348**	717	952
498	168	542	270	586	588	630	240	674	2028	718	1074
499	**498**	543	360	**587**	**1176**	**631**	**630**	675	1800	**719**	**718**
500	1500	544	144	588	336	632	156	676	1092	720	120
501	336	545	540	589	90	633	168	**677**	452	721	208
502	750	546	336	590	1740	634	636	678	456	722	342
503	**1008**	**547**	**1096**	591	792	635	1280	679	784	723	240
504	48	548	276	592	456	636	216	680	180	724	90
505	100	549	120	**593**	**1188**	637	112	681	456	725	700
506	240	550	300	594	360	638	210	682	30	726	1320
507	728	551	126	595	720	639	840	**683**	**1368**	**727**	**1456**
508	768	552	48	596	444	640	960	684	72	728	336
509	254	553	624	597	88	**641**	**640**	685	1380	729	1944
510	360	554	1668	598	336	642	72	686	2352	730	2220
511	292	555	760	**599**	**598**	**643**	**1288**	687	456	731	792
512	768	556	138	600	600	644	48	688	264	732	120
513	72	**557**	124	**601**	**600**	645	440	689	756	**733**	**1468**
514	516	558	120	602	528	646	36	690	240	734	2208
515	1040	559	616	603	408	**647**	**1296**	**691**	138	735	560
516	264	560	240	604	150	648	216	692	348	736	48
517	160	561	360	605	220	649	290	693	240	737	680
518	912	562	168	606	600	650	2100	694	696	738	120
519	696	**563**	376	**607**	**1216**	651	240	695	460	**739**	**738**

m	T(m)	m	T(m)	m	T(m)	m	T(m)	m	T(m)	m	T(m)
740	1140	784	336	828	48	872	108	916	114	960	480
741	504	785	1580	**829**	276	873	1176	917	1040	961	930
742	432	786	1560	830	840	874	144	918	72	962	1596
743	496	**787**	**1576**	831	1112	875	2000	**919**	102	963	72
744	120	788	396	832	672	876	888	920	240	964	240
745	740	789	176	833	1008	**877**	**1756**	921	88	965	1940
746	2244	790	780	834	552	878	438	922	138	966	48
747	168	791	304	835	1680	879	1176	923	140	**967**	176
748	180	792	120	836	90	880	120	924	240	968	660
749	144	793	420	837	360	**881**	176	925	1900	969	72
750	3000	794	2388	838	1254	882	336	926	2784	970	2940
751	**750**	795	1080	**839**	**838**	**883**	**1768**	927	624	**971**	**970**
752	96	796	66	840	240	884	252	928	336	972	648
753	1000	**797**	228	841	406	885	1160	**929**	**928**	973	368
754	84	798	144	842	84	886	888	930	120	974	2928
755	100	799	288	843	56	**887**	**1776**	931	1008	975	1400
756	144	800	1200	844	42	888	456	932	156	976	120
757	**1516**	801	264	845	1820	889	256	933	1240	**977**	652
758	378	802	600	846	96	890	660	934	936	978	984
759	240	803	740	847	880	891	1080	935	180	979	220
760	180	804	408	848	216	892	1344	936	168	980	1680
761	380	805	240	849	568	893	288	**937**	**1876**	981	216
762	768	806	420	850	900	894	888	938	816	982	1470
763	432	807	536	851	912	895	1780	939	1256	**983**	**1968**
764	570	808	300	852	840	896	192	940	480	984	120
765	360	**809**	202	**853**	**1708**	897	336	**941**	470	985	1980
766	768	810	1080	854	240	898	1344	942	1896	986	252
767	812	**811**	270	855	360	899	210	943	240	987	32
768	384	812	336	856	72	900	600	944	696	988	252
769	192	813	1080	**857**	**1716**	901	108	945	720	989	528
770	240	814	1140	858	840	902	120	946	1320	990	120
771	1032	815	1640	**859**	78	903	176	**947**	**1896**	**991**	198
772	1164	816	72	860	1320	904	228	948	312	992	240
773	**1548**	817	792	861	80	905	180	949	1036	993	440
774	264	818	408	862	1290	906	600	950	900	994	1680
775	300	819	336	**863**	**1728**	**907**	**1816**	951	1272	995	220
776	588	820	120	864	144	908	456	952	144	996	168
777	304	**821**	**820**	865	1740	909	600	**953**	212	**997**	**1996**
778	164	822	552	866	2604	910	1680	954	216	998	498
779	360	**823**	**1648**	867	1224	**911**	70	955	380	999	1368
780	840	824	624	868	240	912	72	956	714	1000	1500
781	70	825	200	869	390	913	840	957	280		
782	144	826	1392	870	840	914	2748	958	1434		
783	504	**827**	**1656**	871	952	915	120	959	1104		

Les m en gras sont des nombres premiers.
Les $T(m)$ en gras représentent les cas où m est premier et $T(m)$ maximale.

Aspects p-adiques et combinatoires liés aux suites récurrentes linéaires

Résumé :

Ce travail comporte cinq chapitres. Le premier est un rappel de quelques notions utiles pour le chapitre 2.

Le chapitre 2 est consacré à l'établissement de congruences dans les suites récurrentes linéaires. Etant donnée une suite récurrente linéaire u de polynôme caractéristique f, nous nous intéressons à la détermination des entiers d et des nombres premiers p pour lesquels $f_d(X) \equiv f(X) \bmod p$ où f_d est le polynôme caratéristique des suites d-extraites ou d-décimées de la suite u. Nous commençons par établir, à l'aide des outils de l'analyse p-adique, quelques résultats généraux qui nous fournissent des conditions nécessaires sur d pour que de telles congruences se réalisent. Nous passons ensuite à l'études de quelques cas pratiques, comme le cas cyclotomique et le cas de la suite de Fibonacci. Pour ces exemples précis, et pour d'autres aussi, nous avons réussi à donner des conditions nécessaires et suffisantes sur d pour que $f_d \equiv f \bmod p$. Concernant la suite de Fibonacci, H.T. Freitag [32] a traité le cas $p = 2$ et $p = 5$, le résultat que nous avons obtenu le fait pour une multitude de nombres premiers p.

Nous nous intéressons, dans le chapitre 3 à l'étude des propriétés des suites des polynômes bivariés généralisés de Fibonacci et de Lucas dont nombre de suites classiques en sont des cas particuliers, telles que la suite de Fibonacci, de Lucas, de Pell, de Pell-Lucas, la suite des polynômes de Catalan, de Jacobsthal...

Le quatrième chapitre consiste à étendre une certaine étude faite sur les polynômes de Chebychev de première et seconde espèce définis respectivement par $T_n = 2XT_{n-1} - T_{n-2}$ avec $T_0 = 1$ et $T_1 = X$ et $U_n = 2XU_{n-1} - U_{n-2}$ avec $U_0 = 1$ et $U_1 = 2X$ aux polynômes généralisés de Chebyschev obtenus en remplaçant dans les expressions précédentes $2X$ par un polynôme $h(X)$ quelconque de degré ≥ 1 à coefficients réels distinct du monôme aX avec a rationnel.

Dans le cinquième chapitre, après un rappel non exhaustif des nombreuses généralisations du résultat connu sous le nom de formule de congruence de Lucas, nous donnerons sa version dans le cas des coefficients bi^{s}nomiaux qui sont les coefficients des puissances de x issus du développement de $(1 + x + x^2 + \cdots + x^s)^n$ et qui généralisent les coefficients binomiaux, dans le sens où si on prend $s = 1$ on retrouve les coefficients binomiaux.

Mots-clés : Nombres p-adiques, suites récurrentes linéaires, suites d-extraites, congruences, polynômes bivariés, polynômes de Chebyshev, coefficients bi^{s}nomiaux.