N° d'ordre : 01/2018–D/MT

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOUMEDIENE

FACULTÉ DE MATHÉMATIQUES

THÉSE

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

En : MATHÉMATIQUES

Spécialité : Algèbre et Théorie des Nombres

Par : **Tarek GARICI**

Sujet :

ÉTUDE COMBINATOIRE DE SUITES NUMÉRIQUES ET ÉQUATIONS DIOPHANTIENNES

Soutenue publiquement, le **22/02/2018** devant le jury composé de :

M.	BENSEBA B.	Maître de conférences /A à l'USTHB	Président
M.	BENCHERIF F.	Professeur à l'USTHB	Directeur de thèse
M.	BELGHABA K.	Professeur à l'U.A.B.O. Es sania	Examinateur
M.	KIHEL O.	Professeur à Brock University - Canada	Examinateur
Mme	BENFERHAT L.	Maître de conférences /A à l'USTHB	Examinatrice
M.	BENOUMHANI M.	Maître de conférences /A à U.M.B. M'sila	Examinateur
M.	BOUROUBI S.	Professeur à l'USTHB	Invité
M.	AYAD M.	Maître de conférences /HDR à ULCO -France	Invité

« *Nous ne devrions pas... avoir honte de reconnaître la vérité et de l'adopter, quelle que soit son origine, même si nous la tenions des générations précédentes ou de peuples étrangers. La vérité n'est jamais indigne ; elle ne diminue jamais qui la dit, ni qui la reçoit. Au contraire, la vérité ennoblit.* »

Abû Yûsuf ibn Ishaq Al-Kindi,
(v. 801 – v. 873)

Remerciements

Je tiens à remercier, en tout premier lieu, mon directeur de thèse, le Professeur Farid BENCHERIF *pour avoir bien voulu accepter de diriger cette thèse ainsi que pour l'attention et le suivi qu'il n'a cessé de me prodiguer. Je le remercie infiniment pour tout le temps qu'il m'a patiemment consacré. J'ai beaucoup appris grâce à ses remarquables qualités pédagogiques et scientifiques. En effet, grâce à lui, j'ai découvert l'univers des nombres de Bernoulli et des nombres de Stirling, les suites de Cesàro, les suites de Minkowski et sans oublier la magie du calcul ombral. Mais avant d'être mon directeur de thèse, il a d'abord été mon professeur d'Algèbre* (SEM 330) *en deuxième année D.E.S Mathématiques : je me rappelle très bien d'un cours bien structuré, complet et d'une clarté absolue. C'est ainsi qu'il m'a permis de découvrir et d'aimer l'Algèbre et même, plus tard, la choisir comme spécialité. Pour tout cela, je lui témoigne ma profonde gratitude et mon immense respect.*

Je voudrais également exprimer ma totale reconnaissance au Professeur Omar KIHEL *qui a dirigé, à distance, avec beaucoup de patience et grâce à de longues et passionnantes conversations téléphoniques, une partie de cette thèse. Avec son aide, j'ai été initié au monde fabuleux des fractions continues, des équations diophantiennes et à la prolifique notion de résultant. Je le remercie également pour tous ces encouragements et pour le grand honneur qu'il me fait en participant à ce jury.*

Je tiens également à remercier respectueusement le Professeur Boualem BENSEBA *pour m'avoir fait l'honneur de présider le jury de cette thèse.*

Je souhaiterais témoigner mon plus profond respect et mon infinie gratitude aux Professeurs Leila BENFERHAT, Mohamed AYAD, Kacem BELGHABA, Moussa BENOUMHANI *et* Sadek BOUROUBI *pour avoir eu la patience et surtout la gentillesse d'avoir bien voulu accepter d'examiner ce travail.*

Je ne saurais oublier de remercier grandement mes amis et collègues les Professeurs Rachid BOUCHENNA *et* Abdelmoumène ZEKIRI *pour leurs lectures très attentives et leurs précieuses remarques qui ont contribué à l'amélioration de la version finale de cette thèse.*

Enfin, mes remerciements vont également à mes collègues et amis les professeurs Abdelhafid BERRACHEDI *et* Rachid BOUMAHDI *pour leurs judicieux conseils et encouragements.*

Table des matières

Notations

1. $\mathbb{N} = \{0, 1, 2, \ldots\}$: ensemble des entiers naturels.
2. $\mathbb{N}^* = \{1, 2, \ldots\}$: ensemble des entiers naturels non nuls.
3. $\mathbb{Z}$: l'ensemble des entiers rationnels.
4. $\mathbb{Q}$: l'ensemble des nombres rationnels.
5. $\mathbb{R}$: l'ensemble des nombres réels.
6. $\mathbb{C}$: l'ensemble des nombres complexes.
7. $\mathbb{P}$: l'ensemble des nombres premiers.
8. $\mathbb{F}_p$: le corps fini à p éléments.
9. $[x^n]\, P(x)$: le terme de degré n du polynôme $P(x)$.
10. $\deg P(x)$: le degré du polynôme $P(x)$.
11. $\mathrm{val}(S(z))$: la valuation de la série formelle $S(z)$.
12. $v_p(n)$: la valuation p-adique de l'entier n. C'est la plus grande puissance de p qui divise n.
13. $\mathbb{C}[x]$: le $\mathbb{C}$-espace vectoriel des polynômes à coefficients complexes.
14. $End(\mathbb{C}[x])$: l'algèbre des endomorphismes du $\mathbb{C}$ -espace vectoriel $\mathbb{C}[x]$.
15. $\mathfrak{D}$: l'opérateur de dérivation.
16. Δ : le premier opérateur de différence finie.
17. $\mathfrak{I}$: l'opérateur d'intégration : $x^n \mapsto \int_{1/2}^{x} t^n dt$
18. $B_n(x)$: n-ième polynôme de Bernoulli.
19. B_n : le n-ième nombre de Bernoulli : $B_n = B_n(0)$.
20. G_n : le n-ième nombre de Genocchi.
21. F_n : le n-ième nombre de Fibonacci.
22. L_n : le n-ième nombre de Lucas.
23. $T_n(x)$:le n-ième polynôme de Stirling.
24. $B_n^{(x)}$: le n-ième polynôme de Nörlund.
25. $s(n, k)$: nombre de Stirling de première espèce (signé).
26. $S(n, k)$: nombre de Stirling de seconde espèce.
27. $x^{\underline{n}} := x(x-1)(x-2)\cdots(x-n+1)$: puissance factorielle descendante .
28. $x^{\overline{n}} := x(x+1)(x+2)\cdots(x+n-1)$: puissance factorielle montante .
29. $\binom{x}{n} := \dfrac{x^{\underline{n}}}{n!}$: polynôme binomial
30. $\binom{x}{n_1, n_2, \ldots, n_k} = \binom{x}{n_1}\binom{x-n_1}{n_2}\cdots\binom{x-n_1-\cdots-n_{k-1}}{n_k}$: polynôme multinomial

31. $\lfloor x \rfloor$: la partie entière d'un nombre réel x, i.e. l'unique entier rationnel k vérifiant : $x - 1 < k \leqslant x$.
32. $\sum_{i \in \varnothing} = 0$: par convention ("somme vide").
33. $\prod_{i \in \varnothing} = 1$: par convention (" produit vide ").
34. $\mathrm{mod}(n, 2)$: le reste de la division euclidienne de l'entier n par 2.
35. $(a, b) \equiv (k, \ell) \pmod{n}$: $a \equiv k \pmod{n}$ et $b \equiv \ell \pmod{n}$.
36. $\left(\frac{n}{p}\right)$: le symbole de Legendre
37. $\mathrm{Sylv}_x(P, Q)$: la matrice de Sylvester des deux polynômes P et Q.
38. $\mathrm{Res}_x(P, Q)$: le résultant des deux polynômes P et Q.
39. $\square$: un carré dans $\mathbb{N}$.

Introduction

Ce travail a pour thème l'étude combinatoire de suites numériques telles que les suites de nombres de Bernoulli, de Genocchi et de Stirling ainsi que l'étude de certaines équations diophantiennes telles que les équations de Pell-Fermat, les équations de Cassels et les équations de type résultant. Cette thèse se compose de quatre chapitres.

Dans le premier chapitre, nous nous intéressons aux suites de Cesàro. Plus précisément, nous démontrons à l'aide du calcul ombral une identité combinatoire vérifiée par toute suite de Cesàro. Cette identité nous permettra de généraliser plusieurs identités connues comportant les nombres de Bernoulli mais aussi de découvrir des identités similaires pour les nombres de Genocchi, les nombres de Fibonacci et les nombres de Lucas. Ce chapitre est composé de deux parties. La première partie est consacrée à l'étude de certaines propriétés des suites de Cesàro. Les suites de Cesàro ont été introduites par Edouard Lucas en 1891 d'une manière symbolique, dans son livre "théorie des nombres" tome 1 [46]. Ce sont les suites $(u_n)_{n\geqslant 0}$ de nombres complexes vérifiant pour tout entier n,

$$u_n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k u_k.$$

Les suites de Cesàro sont parfois appelées suites autoduales ou suites invariantes par la transformation binomiale. La relation qui définit les suites de Cesàro peut être écrite symboliquement $u^n = (1-u)^n$, ce qui se traduit par $L_u\left(x^n\right) = L_u\left((1-x)^n\right)$, où L_u est la forme linéaire définie sur $\mathbb{C}[x]$ par $L_u\left(x^n\right) = u_n$ pour tout $n \geqslant 0$. On démontre que les polynômes appartenant au noyau de L_u, par exemple ceux vérifiant $P(x) + P\left(1-x\right) = 0$, induisent une identité vérifiée par la suite u. Grâce à cette identité, on démontre deux identités combinatoires vérifiées par les suites de Cesàro. Dans la seconde partie du chapitre 1, on donnera une généralisation de plusieurs identités connues portant sur les nombres de Bernoulli. On citera par exemple la relation de Carlitz [10](1968), la relation de Momiyama, [51] (2001), et la relation de Kaneko [39] (1995), mais qui en fait a été démontrée par von Ettingshausen [72] en 1827, et redécouverte, en 1877, par von Seidel [73]. Cette relation apparait même dans le livre de Nielsen [56] publié en 1923.

Dans le chapitre 2, on s'intéresse à certaines propriétés des polynômes de Stirling et des polynômes de Nörlund. Soient $s(n,k)$ les nombres de Stirling de première espèce qui sont les composantes de la factorielle décroissante $x^{\underline{n}} = x\left(x-1\right)\cdots\left(x-n+1\right)$ relativement à la base canonique de $\mathbb{C}[x]$. Il est bien connu que pour k fixé, $s(n,n-k)$ est un polynôme en n. Les polynômes $s(n,n-k)$ sont appelés polynômes de Stirling par D.S. Mitrinović et R.S. Mitrinović ; dans [49] ces derniers auteurs déterminent les polynômes $s(n,n-k)$ pour $k \in \{2,\ldots,13\}$ en en donnant une factorisation partielle sous la forme

$$s(n,n-k) = \frac{1}{m_k}\binom{n}{k+1}\left(x(x-1)\right)^{\bmod{(k,2)}} P_k$$

où pour tout $k \in \{2,\ldots,13\}$, m_k est un entier positif, et P_k est un polynôme primitif de $\mathbb{Z}[x]$. Puis

ils constatent que, pour tout $k \in \{1, \ldots, 6\}$, P_{2k} et P_{2k+1} ont même coefficient constant, et posent la question de savoir si cette propriété est vérifiée de manière générale. Le théorème 2.21, principal résultat du chapitre 2, donne une réponse positive à la question posée par Mitrinović et Mitrinović. La preuve du théorème 2.21 repose essentiellement sur le lien entre les polynômes de Stirling et les polynômes de Nörlund dont les coefficients ont été déterminés explicitement par Liu et Srivastava [43] et dont les dénominateurs ont été déterminés par Adelberg [3].

Le chapitre 3 s'intitule nombre de solutions d'une équation de Cassels du nom du mathématicien anglais J.W.S Cassels (1922-2015) ; c'est une équation diophantienne du type $y^2 = px\left(Ax^2 + C\right)$, où p est un nombre premier, A et C sont des entiers. En effet, en 1985, Cassels [11] a relevé le défi de déterminer dans quels cas la somme de trois cubes consécutifs est un carré ; autrement dit, il s'agit de déterminer toutes les solutions de l'équation diophantienne $(x-1)^3 + x^3 + (x+1)^3 = y^2$. Il réduit ce problème à la détermination des points entiers de la courbe elliptique d'équation $y^2 = 3x(x^2+2)$. En utilisant l'arithmétique de certains corps quartiques, il montre que les solutions en entiers strictement positifs de l'équation précédente sont $(x, y) = (1, 3), (2, 6), (24, 204)$. En utilisant des résultats classiques de Ljunggren [44], Luca et Walsh [45] ont donné une majoration du nombre de solutions de l'équation diophantienne $y^2 = nx(x^2+2)$ où $n > 1$ est un entier. En 2010, [18], L. Chen a considéré le cas où n est un nombre premier impair et il montre que cette dernière équation possède au plus deux solutions en entiers strictement positifs. Récemment en 2014, A.Togbé [69] a considéré une forme plus générale ; il a étudié l'équation diophantienne $y^2 = px(Ax^2+2)$, où p est un nombre premier et A est un entier impair supérieur à 2. Il prouve qu'elle admet au plus 7 solutions en entiers strictement positifs. Dans ce chapitre on démontrera que cette équation possède au plus 6 solutions en entiers strictement positifs si A est impair et au plus 4 solutions en entiers strictement positifs dans le cas où A est pair. Notre preuve repose sur des résultats de Ljunggren [44] ainsi que sur certaines propriétés du symbole de Legendre.

Le chapitre 4 est consacré à l'étude du nombre de solutions d'une équation diophantienne de type résultant. Si $P = a_m (x-\alpha_1)\cdots(x-\alpha_m)$ et $Q = b_m (x-\beta_1)\cdots(x-\beta_n)$ sont deux polynômes à coefficients dans un corps commutatif K. Le résultant de P et Q noté $\mathrm{Res}_x(P, Q)$ est défini comme étant le déterminant de la matrice $\mathrm{Sylv}_x(P, Q)$ qui peut aussi s'exprimer à l'aide des racines de P et de Q par $\mathrm{Res}_x(P, Q) = a_m^n b_n^m \prod_{i=1}^m \prod_{j=1}^n (\alpha_i - \beta_j)$. Le résultant de P et Q s'annule si, et seulement si, leur pgcd dans $K[x]$ est non constant, autrement dit si, et seulement si, P et Q ont des racines communes dans $\overline{K}$. Soient P, Q deux polynômes dans $\mathbb{Z}[x]$, on considère l'équation donnée par $\mathrm{Res}_x(P(x), Q(x)) = a$, où a est un entier rationnel non nul donné. On remarque que cette dernière peut être considérée comme une équation diophantienne dont les inconnues sont les coefficients du polynôme Q. Plusieurs auteurs ont étudié ce type d'équation. On pourra citer par exemple Wirsing [74], Fujiwara [26], Schmidt [64], Schlickewei [63], Pethő [58, 59], Győry [37], Evertse et Győry [25]-[24], Gaàl [27] qui ont démontré que le nombre de polynômes Q, de degré inférieur à celui de P et vérifiant l'équation $\mathrm{Res}_x(P(x), Q(x)) = a$, est fini.

Pour notre part, nous démontrons que si un polynôme P possède au moins trois racines distinctes, alors l'équation $\mathrm{Res}_x\left(P(x), x^2 + sx + t\right) = a$ possède un nombre fini de solutions (s, t) dans $\mathbb{Z}^2$. Pour cela, nous utilisons deux résultats de Runge [61] et de Schinzel [62].

Chapitre 1

Suites de Cesàro

1.1 Introduction

Les suites de Cesàro, du nom du mathématicien italien Ernesto Cesàro (1859-1906), ont été introduites par Edouard Lucas en 1891 à l'aide d'une écriture symbolique. Dans son livre "théorie des nombres" tome 1 (cf. [46]), il écrit : « nous désignerons, sous ce nom, toute suite de nombres $A_0,\ A_1,\ A_2,\ \ldots,\ A_n, \ldots$ tels que l'on a pour tout nombre n, entier et positif, la relation symbolique fondamentale $A^n \doteq (1-A)^n$ »

Cette définition peut être réécrite de la manière suivante :

Définition 1.1. *On appelle suite de Cesàro toute suite $(u_n)_{n\geqslant 0}$ de nombres complexes vérifiant*

$$u_n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k u_k \text{ pour tout } n \geqslant 0. \tag{1.1}$$

En supposant $u_0 = 1$, on a bien $u_1 = \frac{1}{2}$ mais u_2 n'est pas déterminé par la relation précédente. En effet celle-ci ne détermine les nombres u_n pour les indices pairs que lorsque l'on connaît les nombres qui correspondent aux indices impairs, ou inversement.

Proposition 1.2. *Soit $S(z) = \sum_{n\geqslant 0} \frac{u_n}{n!} z^n$ la série génératrice exponentielle associée à une suite $(u_n)_{n\geqslant 0}$. La suite $(u_n)_{n\geqslant 0}$ est une suite de Cesàro si et seulement si*

$$S(z) = e^z S(-z). \tag{1.2}$$

Démonstration. Soit $S(z) = \sum_{n\geqslant 0} \frac{u_n}{n!} z^n$ la série génératrice exponentielle associée à une suite de nombres complexes $(u_n)_{n\geqslant 0}$. On a alors :

$$\begin{aligned}
S(z) = e^z S(-z) &\Longleftrightarrow \sum_{n\geqslant 0} \frac{u_n}{n!} z^n = \left(\sum_{n\geqslant 0} \frac{z^n}{n!}\right)\left(\sum_{n\geqslant 0} \frac{u_n}{n!} (-1)^n z^n\right) \\
&\Longleftrightarrow \sum_{n\geqslant 0} \frac{u_n}{n!} z^n = \sum_{n\geqslant 0} \left(\sum_{k=0}^{n} \frac{u_k}{k!} (-1)^k \frac{1}{(n-k)!}\right) z^n \\
&\Longleftrightarrow \sum_{n\geqslant 0} \frac{u_n}{n!} z^n = \sum_{n\geqslant 0} \left(\sum_{k=0}^{n} \binom{n}{k} (-1)^k u_k\right) \frac{z^n}{n!}
\end{aligned}$$

En égalant les coefficients de z^n dans les deux membres de cette dernière relation, on obtient $u_n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k u_k$. D'où l'équivalence. □

Exemple 1.3 ([6]). *Soit $(B_n)_{n\geqslant 0}$ et $(G_n)_{n\geqslant 0}$ les suites de nombres de Bernoulli et de Genocchi définies par la donnée de leurs séries génératrices exponentielle associée*

$$\frac{z}{e^z-1} = \sum_{n\geqslant 0} B_n \frac{z^n}{n!},$$
$$\frac{2z}{e^z+1} = \sum_{n\geqslant 0} G_n \frac{z^n}{n!}.$$

Alors les suites $((-1)^n B_n)_{n\geqslant 0}$ et $\left(\frac{(-1)^n G_{n+1}}{n+1}\right)_{n\geqslant 0}$ sont des suites de Cesàro.
En effet, soient

$$S_1(z) = \sum_{n\geqslant 0} \frac{(-1)^n B_n}{n!} z^n$$
$$S_2(z) = \sum_{n\geqslant 0} \frac{(-1)^n}{n+1} \frac{G_{n+1}}{n!} z^n$$

les séries génératrices exponentielles associées, alors

$$S_1(z) = \sum_{n\geqslant 0} \frac{(-1)^n B_n}{n!} z^n = \sum_{n\geqslant 0} \frac{B_n}{n!} (-z)^n = \frac{-z}{e^{-z}-1}$$
$$S_2(z) = \sum_{n\geqslant 0} \frac{(-1)^n}{n+1} \frac{G_{n+1}}{n!} z^n = \sum_{n\geqslant 0} \frac{(-1)^n}{(n+1)!} G_{n+1} z^n$$
$$= \frac{1}{z} \sum_{n\geqslant 1} \frac{(-1)^{n+1}}{n!} G_n z^n = \frac{-1}{z} \frac{2z}{e^{-z}+1} = \frac{-2}{e^{-z}+1}.$$

Par suite,

$$e^z S_1(-z) = e^z \frac{z}{e^z-1} = \frac{z}{1-e^{-z}} = S_1(z)$$
$$e^z S_2(-z) = e^z \frac{-2}{e^{-z}+1} = \frac{-2}{1+e^z} = S_2(z).$$

D'après la proposition 1.2, les suites $((-1)^n B_n)_{n\geqslant 0}$ et $\left(\frac{(-1)^n}{n+1} G_{n+1}\right)_{n\geqslant 0}$ sont donc des suites de Cesàro.

Le but de ce chapitre est d'établir un théorème général fournissant des identités pour toute suite de Cesàro. Ce théorème que nous énonçons et prouvons à la section suivante va nous permettre non seulement de généraliser plusieurs identités connues comportant les nombres de Bernoulli mais aussi de découvrir des identités similaires pour les nombres de Genocchi, de Fibonacci et de Lucas. Nous consacrons la troisième section à l'énoncé de ces identités.

1.2 Identités vérifiées par les suites de Cesàro

En 1964, Gian-Carlo Rota [60] a considéré la forme linéaire L définie sur $\mathbb{C}[x]$ par $L(x^n) = \mathcal{B}_n$, où $(\mathcal{B}_n)_{n\geqslant 0}$ désigne la suite des nombres de Bell qui énumèrent les partitions d'ensembles finis,

afin de retrouver la relation de récurrence satisfaite par les nombres de Bell. Dans notre cas, on considère, pour toute suite $u = (u_n)_{n\geqslant 0}$ de nombres complexes, la forme linéaire L_u définie sur $\mathbb{C}[x]$ par $L_u(x^n) = u_n$ pour tout entier $n \geqslant 0$, i.e. :

$$\begin{aligned} L_u : \mathbb{C}[x] &\longrightarrow \mathbb{C} \\ P(x) = \sum a_k x^k &\longmapsto \sum a_k u_k. \end{aligned}$$

Convenons de noter $P(u)$ l'image par L_u d'un polynôme $P(x)$ de $\mathbb{C}[x]$. Ainsi si $P(x) = \sum a_k x^k$, alors $P(u) = \sum a_k u_k$. Posons $e_n(x) = x^n - (1-x)^n$, pour tout $n \geqslant 0$. la proposition suivante va nous permettre de donner une caractérisation simple d'une suite de Cesàro.

Proposition 1.4 (cf.[6]). *Une suite u est de Cesàro si et seulement si $(e_n(u))_{n\geqslant 0}$ est la suite nulle.*

Démonstration. Soit $n \in \mathbb{N}$,

$$e_n(x) = x^n - (1-x)^n = x^n - \sum_{k=0}^{n} \binom{n}{k} (-1)^k x^k.$$

Par suite,

$$e_n(u) = L_u(e_n(x)) = u_n - \sum_{k=0}^{n} \binom{n}{k} (-1)^k u_k.$$

La relation (1.1) permet de conclure que u est une suite de Cesàro si et seulement si pour tout entier n, $e_n(u) = 0$. □

Posons $\mathcal{E} := \{A(x) - A(1-x);\ A \in \mathbb{C}[x]\}$. Il n'est pas difficile de voir que $\mathcal{E}$ est le sous-espace vectoriel de $\mathbb{C}[x]$ engendré par la famille de polynômes $(e_n(x))_{n\geqslant 0}$. Alors on a la proposition suivante.

Proposition 1.5 (cf.[6]). *Soit u une suite de Cesàro, alors pour tout polynôme $P \in \mathcal{E}$, on a $P(u) = 0$.*

Démonstration. Soit u une suite de Cesàro et $P \in \mathcal{E}$, il existe alors un polynôme $A(x) = \sum_{n=0}^{k} a_n x^n$ tel que

$$P(x) = A(x) - A(1-x) = \sum_{n=0}^{k} a_n e_n(x).$$

D'après la proposition 1.4,

$$P(u) = \sum_{n=0}^{k} a_n e_n(u) = 0.$$

D'où le résultat. □

Proposition 1.6 (cf.[6]). *Un polynôme P est dans $\mathcal{E}$ si et seulement si P vérifie la relation*

$$P(x) + P(1-x) = 0.$$

Démonstration. Soit $P(x) \in \mathbb{C}[x]$. Si P est dans $\mathcal{E}$, alors il existe un polynôme A tel que

$$P(x) = A(x) - A(1-x).$$

Par suite,

$$P(x) + P(1-x) = 0.$$

Réciproquement si P est un polynôme vérifiant

$$P(x) + P(1-x) = 0,$$

alors $P(x) = -P(1-x)$. D'où

$$P(x) = \frac{1}{2}\left(P(x) - P(1-x)\right) = \sum_{k=0}^{m} \frac{1}{2} a_k \left(x^n - (1-x)^n\right).$$

Ce qui entraîne que $P(x) \in \mathcal{E}$. □

Une conséquence directe de la proposition précédente est le théorème suivant qui est le principal résultat de ce chapitre.

Théorème 1.7 (cf.[6]). *Soient u une suite de Cesàro, $m \in \mathbb{N}$ et $P(x) = \sum_{k=0}^{m} a_k x^k$ un polynôme à coefficients complexes vérifiant la relation $P(x) + P(1-x) = 0$, alors*

$$\sum_{k=0}^{m} a_k u_k = 0.$$

Démonstration. Soit $P(x) \in \mathbb{C}[x]$ vérifiant $P(x) + P(1-x) = 0$. D'après la proposition 1.6, P est dans $\mathcal{E}$. Par suite, d'après la proposition 1.5, $P(u) = 0$. D'où $\sum_{k=0}^{m} a_k u_k = 0$. □

Ce résultat nous permet de donner une preuve très simple de la relation de Kaneko [39]

Exemple 1.8 (Relation de Kaneko). *Soit u une suite de Cesàro, et soient $n \in \mathbb{N}$, $P^* = x^{n+1}(1-x)^{n+1}$ et $P(x) = \frac{dP^*}{dx}$. On a $P^*(x) - P^*(1-x) = 0$ donc $P(x) + P(1-x) = 0$. Or*

$$P^*(x) = \sum_{k=0}^{n+1} \binom{n+1}{k} (-1)^k x^{n+k+1}.$$

D'où

$$P(x) = \sum_{k=0}^{n+1} \binom{n+1}{k} (-1)^k (n+k+1) x^{n+k}.$$

D'après le théorème 1.7, pour tout entier n, on a

$$\sum_{k=0}^{n+1} \binom{n+1}{k} (-1)^k (n+k+1) u_{n+k} = 0.$$

Dans le cas particulier où $u_n = (-1)^n B_n$ (voir exemple 1.3), on obtient la relation

$$\sum_{k=0}^{n+1} \binom{n+1}{k} (n+k+1) B_{n+k} = 0.$$

On obtient ainsi une relation, appelée relation de Kaneko [39] (1995).

A présent, introduisons deux nouveaux opérateurs qui sont des outils très efficaces pour déterminer des éléments de $\mathcal{E}$ ce qui nous permettra de prouver de nouvelles identités combinatoires. Soient

$\mathfrak{D}$ l'opérateur de dérivation et $\mathfrak{I}$ l'opérateur défini sur $\mathbb{C}[x]$ par :

$$\begin{aligned}\mathfrak{I} : \mathbb{C}[x] &\longrightarrow \mathbb{C}[x] \\ R(x) &\longmapsto \int_{1/2}^{x} R(t)\,dt,\end{aligned}$$

alors on a les deux propositions suivantes.

Proposition 1.9. *Soient $P(x) \in \mathbb{C}[x]$ vérifiant $P(x)+P(1-x)=0$, alors pour tout entier naturel k,*

1. $\left(\mathfrak{D}^{2k}P\right)(x) + \left(\mathfrak{D}^{2k}P\right)(1-x) = 0.$
2. $\left(\mathfrak{I}^{2k}P\right)(x) + \left(\mathfrak{I}^{2k}P\right)(1-x) = 0.$

Démonstration. On fait un raisonnement par récurrence sur k. Pour $k=0$, la relation est vraie par hypothèse sur P. Supposons que $\left(\mathfrak{D}^{2k}P\right)(x) + \left(\mathfrak{D}^{2k}P\right)(1-x) = 0$, donc

$$\mathfrak{D}^2\left(\left(\mathfrak{D}^{2k}P\right)(x) + \left(\mathfrak{D}^{2k}P\right)(1-x)\right) = 0.$$

Par suite,

$$\left(\mathfrak{D}^{2(k+1)}P\right)(x) + \left(\mathfrak{D}^{2(k+1)}P\right)(1-x) = 0.$$

Montrons maintenant que $\left(\mathfrak{I}^{2k}P\right)(x) + \left(\mathfrak{I}^{2k}P\right)(1-x) = 0$ pour tout $k \in \mathbb{N}$. Pour $k=0$, la relation est vérifiée par hypothèse sur P. Supposons que $\left(\mathfrak{I}^{2k}P\right)(x) + \left(\mathfrak{I}^{2k}P\right)(1-x) = 0$. Alors $\mathfrak{I}^2\left(\left(\mathfrak{I}^{2k}P\right)(x) + \left(\mathfrak{I}^{2k}P\right)(1-x)\right) = 0$. Par suite $\left(\mathfrak{I}^{2(k+1)}P\right)(x) + \mathfrak{I}^2\left(\left(\mathfrak{I}^{2k}P\right)(1-x)\right) = 0$. Reste à montrer que $\mathfrak{I}^2\left(\mathfrak{I}^{2k}P\right)(1-x) = \left(\mathfrak{I}^{2(k+1)}P\right)(1-x)$.

$$\mathfrak{I}^2\left(\mathfrak{I}^{2k}P\right)(1-x) = \int_{1/2}^{x}\int_{1/2}^{t}\left(\mathfrak{I}^{2k}P\right)(1-s)\,dsdt.$$

En effectuant le changement de variable $u = 1-s$, on obtient

$$\mathfrak{I}^2\left(\mathfrak{I}^{2k}P\right)(1-x) = -\int_{1/2}^{x}\int_{1/2}^{1-t}\left(\mathfrak{I}^{2k}P\right)(u)\,dudt = -\int_{1/2}^{x}\left(\mathfrak{I}^{2k+1}P\right)(1-t)\,dt.$$

Le changement de variable $v = 1-t$ donne alors :

$$\mathfrak{I}^2\left(\mathfrak{I}^{2k}P\right)(1-x) = \int_{1/2}^{1-x}\left(\mathfrak{I}^{2k+1}P\right)(v)\,dt = \left(\mathfrak{I}^{2(k+1)}P\right)(1-x).$$

□

Proposition 1.10. *Soient $q \in \mathbb{N}$ et $P(x) \in \mathbb{C}[x]$ vérifiant $P(x) + (-1)^q P(1-x) = 0$, alors :*

1. $\left(\mathfrak{D}^q P\right)(x) + \left(\mathfrak{D}^q P\right)(1-x) = 0.$
2. $\left(\mathfrak{I}^q P\right)(x) + \left(\mathfrak{I}^q P\right)(1-x) = 0.$

Démonstration. Pour le cas q pair, la réponse est donnée par la proposition 1.9. Examinons le cas q impair. Si $q = 2k+1$ alors $P(x) - P(1-x) = 0$. Par suite $(\mathfrak{D}P)\,x + (\mathfrak{D}P)(1-x) = 0$ et $(\mathfrak{I}P)(x) + (\mathfrak{I}P)(1-x) = 0$. D'après la proposition 1.9, on a

$$\begin{aligned}\left(\mathfrak{D}^{2k}(\mathfrak{D}P)\right)(x) + \left(\mathfrak{D}^{2k}(\mathfrak{D}P)\right)(1-x) &= 0 \\ \left(\mathfrak{I}^{2k}(\mathfrak{I}P)\right)(x) + \left(\mathfrak{I}^{2k}(\mathfrak{I})\,P\right)(1-x) &= 0.\end{aligned}$$

D'où le résultat. □

Nous adoptons les notations suivantes préconisées par Knuth dans [35] où, pour tous entiers naturels n et m, on pose

$$m^{\underline{n}} = \prod_{j=0}^{n-1}(m-j),$$

avec la convention qu'un produit vide vaut 1.

Théorème 1.11 (cf.[6]). *Soit $(u_n)_{n\geqslant 0}$ une suite de Cesàro. Alors, pour tous entiers naturels n, m et q, on a :*

$$\sum_{k=0}^{m+q}\binom{m+q}{k}(n+k+q)^{\underline{q}}(-1)^k u_{n+k} + (-1)^{q+1}\sum_{k=0}^{n+q}\binom{n+q}{k}(m+k+q)^{\underline{q}}(-1)^k u_{m+k} = 0.$$

Démonstration. Soient u une suite de Cesàro, et $n, m, q \in \mathbb{N}$. Posons

$$P^*(x) = x^{n+q}(1-x)^{m+q} + (-1)^{q+1}(1-x)^{n+q}x^{m+q}$$

et $P(x) = \mathcal{D}^q P^*$. On a

$$\begin{aligned}
P(x) &= \mathfrak{D}^q\left(x^{n+q}(1-x)^{m+q} + (-1)^{q+1}(1-x)^{n+q}x^{m+q}\right)\\
&= \mathfrak{D}^q\left(\sum_{k=0}^{m+q}\binom{m+q}{k}(-1)^k x^{n+k+q} + (-1)^{q+1}\sum_{k=0}^{n+q}\binom{n+q}{k}(-1)^k x^{m+k+q}\right)\\
&= \sum_{k=0}^{m+q}\binom{m+q}{k}(-1)^k(n+k+q)^{\underline{q}}x^{n+k} + (-1)^{q+1}\sum_{k=0}^{n+q}\binom{n+q}{k}(m+k+q)^{\underline{q}}(-1)^k x^{m+k}.
\end{aligned}$$

Or

$$\begin{aligned}
P^*(x) + (-1)^q P^*(1-x) = x^{n+q}(1-x)^{m+q} + (-1)^{q+1}(1-x)^{n+q}x^{m+q}\\
+ (-1)^q\left((1-x)^{n+q}x^{m+q} + (-1)^{q+1}x^{n+q}(1-x)^{m+q}\right) = 0.
\end{aligned}$$

Donc, d'après la proposition 1.10, $P(x) + P(1-x) = 0$. Ce qui entraîne, d'après le Théorème 1.7, que $P(u) = 0$. Par suite

$$\sum_{k=0}^{m+q}\binom{m+q}{k}(n+k+q)^{\underline{q}}(-1)^k u_{n+k} + (-1)^{q+1}\sum_{k=0}^{n+q}\binom{n+q}{k}(m+k+q)^{\underline{q}}(-1)^k u_{m+k} = 0.$$

□

Lemme 1.12. *Pour tous entiers naturels n et m et tout nombre réel x on a :*

$$\int_0^x t^n(x-t)^m\,dt = \frac{m!}{(n+m+1)^{\underline{(m+1)}}}x^{m+n+1}.$$

Démonstration. Posons pour tout entier $n \geqslant 0$, et tout entier $m \geqslant 0$

$$I(n,m) = \int_0^x t^n(x-t)^m\,dt.$$

En effectuant une intégration par parties on obtient

$$I(n,m) = \frac{m}{n+1} I(n+1, m-1).$$

Par suite

$$\begin{aligned} I(n,m) &= \frac{m!}{(n+1)(n+2)\cdots(n+m)} I(n+m,0) \\ &= \frac{m!}{(n+1)(n+2)\cdots(n+m)} \int_0^x t^{n+m} dt \\ &= \frac{m!}{(n+1)(n+2)\cdots(n+m)(n+m+1)} x^{n+m+1} \\ &= \frac{m!}{(n+m+1)^{\underline{(m+1)}}} x^{n+m+1}. \end{aligned}$$

□

Lemme 1.13. *Pour tous entiers n, m, q avec $q \geqslant 1$ et tout nombre réel x on a*

$$\int_0^x t^n (1-t)^m (x-t)^{q-1} dt = (q-1)! \sum_{k=0}^{m} \binom{m}{k} (-1)^k \frac{x^{n+k+q}}{(n+k+q)^{\underline{q}}}.$$

Démonstration.

$$\begin{aligned} \int_0^x t^n (1-t)^m (x-t)^{q-1} dt &= \int_0^x t^n t^k (x-t)^{q-1} dt \\ &= \sum_{k=0}^{m} \binom{m}{k} (-1)^k \left(\int_0^x t^{n+k} (x-t)^{q-1} dt \right). \end{aligned}$$

D'après le Lemme 1.12,

$$\int_0^x t^{n+k} (x-t)^{q-1} dt = \frac{(q-1)!}{(n+k+q)^{\underline{q}}} x^{n+k+q}.$$

□

Théorème 1.14 (cf.[6])**.** *Soit $(u_n)_{n \geqslant 0}$ une suite de Cesàro. Alors, pour tous entiers naturels n, m et q, on a :*

$$\begin{aligned} \sum_{k=0}^{m} \binom{m}{k} (-1)^k \frac{u_{n+k+q}}{(n+k+q)^{\underline{q}}} + (-1)^{q+1} \sum_{k=0}^{n} \binom{n}{k} (-1)^k \frac{u_{m+k+q}}{(m+k+q)^{\underline{q}}} \\ = \sum_{k=0}^{q-1} \frac{n!(m+q-k-1)!}{k!(q-1-k)!(m+n+q-k)!} (-1)^k u_k. \end{aligned}$$

Démonstration. Soient u une suite de Cesàro et $n, m, q \in \mathbb{N}$, $q \geqslant 1$. Posons $P^*(x) = x^n(1-x)^m + (-1)^{q+1} x^m (1-x)^n$, et $P(x) = \mathfrak{I}^q(P^*)$ où $\mathfrak{I}$ est l'opérateur défini sur $\mathbb{C}[x]$ par :

$$\begin{aligned} \mathfrak{I} : \mathbb{C}[x] &\longrightarrow \mathbb{C}[x] \\ R(x) &\longmapsto \int_{1/2}^x R(t)\, dt. \end{aligned}$$

Le polynôme $P(x)$ est par construction l'unique polynôme vérifiant

$$P^{(q)}(x) = P^*(x) \quad \text{et} \quad P\left(\tfrac{1}{2}\right) = P'\left(\tfrac{1}{2}\right) = \cdots = P^{(q-1)}\left(\tfrac{1}{2}\right) = 0.$$

Écrivons le développement de Taylor avec reste intégral du polynôme $P(x)$ au voisinage de $\frac{1}{2}$ à l'ordre $q-1$

$$\begin{aligned} P(x) &= \sum_{k=0}^{q-1} \frac{1}{k!} \left(x-\tfrac{1}{2}\right)^k P^{(k)}\left(\tfrac{1}{2}\right) + \frac{1}{(q-1)!}\int_{1/2}^{x} P^{(q)}(t)\,(x-t)^{q-1}\,dt \\ &= \frac{1}{(q-1)!}\int_{1/2}^{x} P^{*}(t)\,(x-t)^{q-1}\,dt \\ &= \frac{1}{(q-1)!}\int_{0}^{x} P^{*}(t)\,(x-t)^{q-1}\,dt - \frac{1}{(q-1)!}\int_{0}^{1/2} P^{*}(t)\,(x-t)^{q-1}\,dt. \end{aligned} \tag{1.3}$$

Posons

$$\begin{aligned} A(x) &= \frac{1}{(q-1)!}\int_{0}^{x} P^{*}(t)\,(x-t)^{q-1}\,dt, \\ B(x) &= -\frac{1}{(q-1)!}\int_{0}^{1/2} P^{*}(t)\,(x-t)^{q-1}\,dt, \end{aligned}$$

on a alors

$$\mathfrak{I}^{q}(P^{*}) = A(x) + B(x) \tag{1.4}$$

$$A(x) = \frac{1}{(q-1)!}\left(\int_{0}^{x} t^{n}(1-t)^{m}\,(x-t)^{q-1} + (-1)^{q+1}\int_{0}^{x} t^{m}(1-t)^{n}\,(x-t)^{q-1}\,dt\right).$$

D'après le lemme 1.13, on trouve :

$$A(x) = \sum_{k=0}^{m}\binom{m}{k}(-1)^{k}\frac{x^{n+k+q}}{(n+k+q)^{\underline{q}}} + (-1)^{q+1}\sum_{k=0}^{m}\binom{m}{k}(-1)^{k}\frac{x^{n+k+q}}{(n+k+q)^{\underline{q}}}.$$

Calculons maintenant le polynôme $B(x)$.

$$\begin{aligned} -(q-1)!B(x) &= \int_{0}^{1/2} P^{*}(t)\,(x-t)^{q-1}\,dt \\ &= \int_{0}^{1/2} t^{n}(1-t)^{m}\,(x-t)^{q-1}\,dt + \int_{0}^{1/2} t^{m}(1-t)^{n}\,(t-x)^{q-1}\,dt \\ &= \int_{0}^{1} t^{n}(1-t)^{m}\,(x-t)^{q-1}\,dt - \int_{1/2}^{1} t^{n}(1-t)^{m}\,(x-t)^{q-1}\,dt \\ &+ \int_{0}^{1/2} t^{m}(1-t)^{n}\,(t-x)^{q-1}\,dt. \end{aligned}$$

En effectuant dans la seconde intégrale le changement de variable $t \longrightarrow 1-t$ on obtient :

$$\begin{aligned} -(q-1)!B(x) &= \int_{0}^{1} t^{n}(1-t)^{m}\,(x-t)^{q-1}\,dt - \int_{0}^{1/2} (1-t)^{n}\,t^{m}\,(x-1+t)^{q-1}\,dt \\ &+ \int_{0}^{1/2} t^{m}(1-t)^{n}\,(t-x)^{q-1}\,dt \\ &= \int_{0}^{1} t^{n}(1-t)^{m}\,(x-t)^{q-1}\,dt - \int_{0}^{1/2} t^{m}\,(1-t)^{n}\,(t-(1-x))^{q-1}\,dt \\ &+ \int_{0}^{1/2} t^{m}(1-t)^{n}\,(t-x)^{q-1}\,dt. \end{aligned}$$

Posons

$$C(x) = \int_0^{1/2} t^m (1-t)^n \, (t-x)^{q-1} \, dt,$$

$$D(x) = \int_0^1 t^n (1-t)^m \, (x-t)^{q-1} \, dt.$$

Alors

$$-(q-1)!B(x) = D(x) + C(x) - C\,(1-x)\,.$$

De la relation (1.4) on déduit

$$\mathfrak{I}^q\,(P^*) = A(x) + B(x) = A(x) - \frac{1}{(q-1)!}D(x) - \frac{1}{(q-1)!}\,(C(x) - C\,(1-x))\,.$$

D'où

$$A(x) = \mathfrak{I}^q\,(P^*) + \frac{1}{(q-1)!}\,(C(x) - C\,(1-x)) + \frac{1}{(q-1)!}D(x).$$

Or $\mathfrak{I}^q\,(P^*)$ et $\frac{1}{(q-1)!}\,(C(x) - C\,(1-x))$ sont des éléments de $\mathcal{E}$, d'où d'après la proposition 1.5,

$$L_u\left(\mathfrak{I}^q\,(P^*) + \frac{1}{(q-1)!}\,(C(x) - C\,(1-x))\right) = 0.$$

Par suite

$$L_u\,(A(x)) = L_u\left(\frac{1}{(q-1)!}D(x)\right),$$

et la preuve du théorème est complète. □

1.3 Applications et exemples

Les théorèmes 1.11 et 1.14 permettent de retrouver simplement des identités connues comportant les nombres de Bernoulli et les nombres de Genocchi, découvertes par différents auteurs et prouvées par diverses méthodes.

1.3.1 Identités vérifiées par les nombres de Bernoulli

Soit $(B_n)_{n\geqslant 0}$ la suite de nombres de Bernoulli de série génératrice exponentielle associée

$$\sum_{n\geqslant 0} B_n \frac{z^n}{n!} = \frac{z}{e^z - 1} = 1 - \frac{1}{2}z + \frac{1}{6}\frac{z^2}{2!} - \frac{1}{30}\frac{z^4}{4!} + \frac{1}{42}\frac{z^6}{6!} - \frac{1}{30}\frac{z^8}{8!}\cdots.$$

L'application des théorèmes 1.11 et 1.14 à la suite de Cesàro $((-1)^n B_n)_{n\geqslant 0}$ (voir exemple 1.3), fournit le corollaire suivant

Corollaire 1.15 (cf.[6]). *1. Pour tous entiers $n \geqslant 0$, $m \geqslant 0$ et $q \geqslant 0$, on a :*

$$(-1)^n \sum_{k=0}^{m+q} \binom{m+q}{k} (n+k+q)^{\underline{q}} B_{n+k} + (-1)^{m+q+1} \sum_{k=0}^{n+q} \binom{n+q}{k} (m+k+q)^{\underline{q}} B_{m+k} = 0, \quad (1.5)$$

2. Pour tous entiers $n \geqslant 0$, $m \geqslant 0$ et $q \geqslant 1$, on a :

$$(-1)^{n+q}\sum_{k=0}^{m}\binom{m}{k}\frac{B_{n+k+q}}{(n+k+q)^{\underline{q}}}+(-1)^{m+1}\sum_{k=0}^{n}\binom{n}{k}\frac{B_{m+k+q}}{(m+k+q)^{\underline{q}}}$$
$$=\sum_{k=0}^{q-1}\frac{n!(m+q-1-k)!}{k!(q-1-k)!(m+n+q-k)!}B_k. \quad (1.6)$$

Dans tout ce qui suit, on suppose $n \geqslant 0$ et $m \geqslant 0$. La relation (1.5) généralise plusieurs identités connues.

– Pour $m = n$ et $q = 1$, elle permet d'obtenir :

$$\sum_{k=0}^{n+1}\binom{n+1}{k}(n+k+1)B_{n+k}=0.$$

C'est la relation de Kaneko. D'après Cigler [20], elle devrait s'appeler la relation de Kaneko-Ettingshausen-Seidel. Elle fut découverte par von Ettingshausen [72] (1827), redécouverte par von Seidel [73] (1877) puis de nouveau par Kaneko [39] (1995). Cette relation apparait dans le livre de Nielsen [56], (1923). Une relation plus générale, écrite symboliquement, figure aussi en page 240 du livre d'Edouard Lucas [46] (1891). D'autres auteurs se sont intéressés à ce résultat. Ainsi Gessel [32] (2003) en donne une démonstration utilisant le calcul ombral. Chen [17] (2005) la démontre en exploitant des propriétés d'une matrice de Seidel. Chen et Sun [19] (2009) la prouvent en utilisant une extension de l'algorithme de Zeilberger alors que Cigler [20] (2009) reprend, en la modernisant, la démonstration originelle de Seidel.

– Pour $q = 0$, on obtient

$$(-1)^{n}\sum_{k=0}^{m}\binom{m}{k}B_{n+k}+(-1)^{m+1}\sum_{k=0}^{n}\binom{n}{k}B_{m+k}=0.$$

On reconnaît ici la relation de Carlitz [10](1968), établie aussi par Gessel [32] (2003), prouvée également par Wu, Sun et Pan [75] (2004), par Chen [17] (2005) ainsi que par Chen et Sun[19](2009).

– Pour $q = 1$, on obtient la relation prouvée par Momiyama, [51](2001), à l'aide de l'intégrale de Volkenborn et généralisée aux polynômes de Bernoulli par Wu, Sun et Pan [75] (2004). Cette relation a aussi été démontrée par Chen et Sun [19] (2009) :

$$(-1)^{n}\sum_{k=0}^{m+1}\binom{m+1}{k}(n+k+1)B_{n+k}+(-1)^{m}\sum_{k=0}^{n+1}\binom{n+1}{k}(m+k+1)B_{m+k}=0.$$

– Pour $m = n$ et $q = 3$, on retrouve la relation de Chen et Sun [19](2009) :

$$\sum_{k=0}^{n+3}\binom{n+3}{k}(n+k+3)(n+k+2)(n+k+1)B_{n+k}=0.$$

– La relation (1.6) pour $q = 1$, devient la formule de Gelfand [30], (1968), démontrée aussi par

Chen et Sun [19] (2009) :

$$(-1)^{n-1}\sum_{k=0}^{m}\binom{m}{k}\frac{B_{n+k+1}}{(n+k+1)}+(-1)^{m-1}\sum_{k=0}^{n}\binom{n}{k}\frac{B_{m+k+1}}{(m+k+1)}=\frac{m!n!}{(m+n+1)!}.$$

Cette formule a de plus été généralisée aux polynômes de Bernoulli par Chang et Ha [14] (2006).

1.3.2 Identités vérifiées par les nombres de Genocchi

Soit $(G_n)_{n\geqslant 0}$ la suite de nombres de Genocchi de série génératrice exponentielle associée

$$\sum_{n\geqslant 0}G_n\frac{z^n}{n!}=\frac{2z}{e^z+1}=z-\frac{z^2}{2!}+\frac{z^4}{4!}-3\frac{z^6}{6!}+17\frac{z^8}{8!}\cdots.$$

L'application des théorèmes 1.11 et 1.14 à la suite de Cesàro $\left(\frac{(-1)^n}{n+1}G_{n+1}\right)_{n\geqslant 0}$ (voir exemple 1.3), fournit les deux identités suivantes

$$(-1)^n\sum_{k=0}^{m+q}\binom{m+q}{k}(n+k+q)^{\underline{q-1}}G_{n+k+1}$$
$$+(-1)^{m+q+1}\sum_{k=0}^{n+q}\binom{n+q}{k}(m+k+q)^{\underline{q-1}}G_{m+k+1}=0. \quad (1.7)$$

$$(-1)^{n+q}\sum_{k=0}^{m}\binom{m}{k}\frac{G_{n+k+q+1}}{(n+k+q+1)^{\underline{q+1}}}+(-1)^{m+1}\sum_{k=0}^{n}\binom{n}{k}\frac{G_{m+k+q+1}}{(m+k+q+1)^{\underline{q+1}}}$$
$$=\sum_{k=0}^{q-1}\frac{n!(m+q-1-k)!}{(k+1)!(q-1-k)!(m+n+q-k)!}G_{k+1}.$$

En échangeant n en $n-1$ et m en $m-1$, la relation (1.7) permet d'obtenir pour $q=1$,

$$(-1)^n\sum_{k=0}^{m}\binom{m}{k}G_{n+k}+(-1)^m\sum_{k=0}^{n}\binom{n}{k}G_{m+k}=0.$$

Cette dernière relation établie pour $n\geqslant 1$ et $m\geqslant 1$ est en fait vérifiée pour $n\geqslant 0$ et $m\geqslant 0$. Elle permet d'obtenir pour $m=n$ l'identité

$$\sum_{k=0}^{n}\binom{n}{k}G_{2n-k}=0. \quad (1.8)$$

Il est facile de constater que $G_m=0$ pour tout entier m impair supérieur ou égal à 3. Il suffit pour cela de remarquer que la série formelle $\frac{2z}{e^z+1}-z=-z\tanh\left(\frac{z}{2}\right)$ est paire. La relation (1.8) devient pour $n\geqslant 2$

$$\sum_{k=0}^{\left\lfloor\frac{n}{2}\right\rfloor}\binom{n}{2j}G_{2n-2j}=0.$$

On obtient ainsi la relation de Seidel [32].

La relation (8.1) de Chen et Sun [19]

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k}G_{m+k}=\sum_{k=0}^{m}(-1)^k\binom{m}{k}\sum_{j=0}^{n+k}(-1)^j\binom{n+k}{j}G_j,$$

peut s'obtenir trivialement en constatant que le polynôme

$$T(x)=\sum_{k=0}^{n}(-1)^k\binom{n}{k}x^{m+k}-\sum_{k=0}^{m}(-1)^k\binom{m}{k}\sum_{j=0}^{n+k}(-1)^j\binom{n+k}{j}x^j$$

est en fait le polynôme nul. On a en effet

$$T(x)=x^m\,(1-x)^n-(1-x)^n\,(1-(1-x))^m=0.$$

On a donc $T(u)=0$ pour toute suite $(u_n)_{n\geqslant 0}$. Autrement dit

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k}u_{m+k}=\sum_{k=0}^{m}(-1)^k\binom{m}{k}\sum_{j=0}^{n+k}(-1)^j\binom{n+k}{j}u_j.$$

Le cas particulier $u_n=G_n$ donne la relation (8.1) de [19].

1.3.3 Identités vérifiées par les nombres de Fibonacci et les nombres de Lucas

Les suites des nombres de Fibonacci $(F_n)_{n\geqslant 0}$ et de Lucas $(L_n)_{n\geqslant 0}$ vérifient la même relation de récurrence $u_n=u_{n-1}+u_{n-2}$, avec les conditions initiales $F_0=0$, $F_1=1$, $L_0=2$, $L_1=1$. Avec $\alpha=\dfrac{1+\sqrt{5}}{2}$ et $\beta=\dfrac{1-\sqrt{5}}{2}$, on a $F_n=\dfrac{\alpha^n-\beta^n}{\alpha-\beta}$, $L_n=\alpha^n+\beta^n$ et on constate facilement que les séries génératrices exponentielles associées aux suites $\left(\frac{F_{n+1}}{n+1}\right)_{n\geqslant 0}$ et $(L_n)_{n\geqslant 0}$ sont respectivement $\frac{e^{\alpha z}-e^{\beta z}}{(\alpha-\beta)z}$ et $e^{\alpha z}+e^{\beta z}$. On vérifie, à l'aide de la propriété (1.2), que les suites $\left(\frac{F_{n+1}}{n+1}\right)_{n\geqslant 0}$ et $(L_n)_{n\geqslant 0}$ sont des suites de Cesàro. L'application du théorème 1.11 et du théorème 1.14 fournit alors les identités suivantes :

$$\sum_{k=0}^{m+q}\binom{m+q}{k}(n+k+q)^{\underline{q-1}}\,(-1)^k\,F_{n+k+1}$$
$$+(-1)^{q+1}\sum_{k=0}^{n+q}\binom{n+q}{k}(m+k+q)^{\underline{q-1}}(-1)^kF_{m+k+1}=0,$$

$$\sum_{k=0}^{m}\binom{m}{k}(-1)^k\frac{F_{n+k+q+1}}{(n+k+q+1)^{\underline{q+1}}}+(-1)^{q+1}\sum_{k=0}^{n}\binom{n}{k}(-1)^k\frac{F_{m+k+q+1}}{(m+k+q+1)^{\underline{q+1}}}$$
$$=\sum_{k=0}^{q-1}\frac{n!(m+q-1-k)!}{(k+1)!(q-1-k)!(m+n+q-k)!}\,(-1)^k\,F_{k+1},$$

$$\sum_{k=0}^{m+q}\binom{m+q}{k}(n+k+q)^{\underline{q}}(-1)^kL_{n+k}+(-1)^{q+1}\sum_{k=0}^{n+q}\binom{n+q}{k}(m+k+q)^{\underline{q}}(-1)^kL_{m+k}=0,$$

$$\sum_{k=0}^{m}\binom{m}{k}(-1)^k\frac{L_{n+k+q}}{(n+k+q)^{\underline{q}}}+(-1)^{q+1}\sum_{k=0}^{n}\binom{n}{k}(-1)^k\frac{L_{m+k+q}}{(m+k+q)^{\underline{q}}}$$
$$=\sum_{k=0}^{q-1}\frac{n!(m+q-1-k)!}{k!(q-1-k)!(m+n+q-k)!}(-1)^k L_k.$$

Chapitre 2

Polynômes de Stirling et de Nörlund

2.1 Introduction

Étant donné un entier positif n, si on écrit la factorielle décroissante $x^{\underline{n}}$ dans la base canonique de $\mathbb{C}[x]$, on a :

$$x^{\underline{n}} = s(n,0) + s(n,1)x + \cdots + s\,(n,n)\,x^n,$$

les coefficients $s(n,k)$ sont appelés les nombres de Stirling de première espèce. D'après Charles Tweedie (cf. [71]), ils ont été désignés sous ce nom par Niels Nielsen (1865-1931) ([54]) en l'honneur de James Stirling (1692-1770) qui les a introduits dans son traité [67] "*Methodus Differentialis*" en 1730. Il est bien connu que pour k fixé, $s(n,n-k)$ est un polynôme en n (cf. [55]). De manière plus précise, si l'on désigne par $\left(B_n^{(x)}\right)_n$ la suite des polynômes de Nörlund, appelée aussi suite des nombres généralisés de Bernoulli d'ordre x et définie par :

$$\sum_{n\geqslant 0} B_n^{(x)} \frac{z^n}{n!} = \left(\frac{z}{e^z-1}\right)^x$$

et par $(T_k(x))_{k\geqslant 0}$, la suite des polynômes définie par :

$$T_k(x) = \binom{x-1}{k} B_k^{(x)}, \text{ pour } k \geqslant 0,$$

on a, (cf. [34], [33],[50]) :

$$s(n,n-k) = T_k(n).$$

Les polynômes $T_k(x)$ sont appelés polynômes de Stirling par Dragoslav S. Mitrinović et Ružica S. Mitrinović. Dans [49], ces deux auteurs déterminent les polynômes $T_k(x)$, pour $k \in \{1,\ldots,13\}$, en les écrivant sous la forme

$$T_{2k}(x) = \frac{1}{m_{2k}}\binom{x}{2k+1} P_{2k}(x),$$
$$T_{2k+1}(x) = \frac{1}{m_{2k+1}}\binom{x}{2k+2} x(x-1)P_{2k}(x),$$

où $P_k(x)$, $k = 2,3,...,13$, sont des polynômes primitifs de $\mathbb{Z}[x]$ vérifiant pour $1 \leqslant k \leqslant 6$

$$P_{2k}(0) = P_{2k+1}(0). \tag{2.1}$$

On rappelle qu'un polynôme de $\mathbb{Z}[x]$ est dit primitif si tous ses coefficients sont premiers entre

eux. Dans [49], D.S. Mitrinović et R.S. Mitrinović posent la question de savoir si la propriété (2.1) est vérifiée de manière générale pour le couple de polynômes $(P_{2k}(x), P_{2k+1}(x))$, associé au couple de polynômes de Stirling (T_{2k}, T_{2k+1}). Le théorème 2.21 (cf. [7]), principal résultat de ce chapitre, affirme que la propriété (2.1) est en fait bien vérifiée pour tout entier $k \geqslant 1$. Comme corollaire, on obtient ainsi une réponse positive à la question posée par D.S. Mitrinović et R.S. Mitrinović (cf. [49]).

2.2 Nombres de Stirling, définition et propriétés

Soit n un entier positif, on définit la factorielle décroissante notée $x^{\underline{n}}$ par

$$x^{\underline{n}} = \begin{cases} 1 & \text{si } n = 0 \\ x\,(x-1)\cdots(x-n+1) & \text{si } n \geqslant 1 \end{cases} \tag{2.2}$$

Cette suite de polynômes constitue une base du $\mathbb{C}$-espace vectoriel des polynômes $\mathbb{C}[x]$. Les polynômes binomiaux notés $\binom{x}{n}$ sont définis pour tout n par

$$\binom{x}{n} = \frac{x^{\underline{n}}}{n!}.$$

Ils interviennent notamment dans la formule du binôme généralisée, très connue, suivante

$$(1+z)^x = \sum_{n\geqslant 0} \binom{x}{n} z^n, \tag{2.3}$$

et ils forment une base de $\mathbb{C}[x]$, appelée base binomiale.

Définition 2.1 ([22]). *Les nombres de Stirling de première espèce $s(n,k)$ sont les composantes de la factorielle décroissante $x^{\underline{n}}$ relativement à la base canonique de $\mathbb{C}[x]$, et les nombres de Stirling de seconde espèce $S(n,k)$ sont les composantes du monôme x^n dans la base $x^{\underline{n}}$. En d'autres termes, pour tout $(n,k) \in \mathbb{N}^2$*

$$x^{\underline{n}} = \sum_{k\geqslant 0} s(n,k) x^k \tag{2.4}$$

$$x^n = \sum_{k\geqslant 0} S(n,k) x^{\underline{n}}. \tag{2.5}$$

avec la convention que $x^0 = x^{\underline{0}} = 1$.

Ainsi pour tout $n \geqslant 0$

$$s(n,0) = S(n,0) = \delta_{n,0}, \quad s(n,n) = S(n,n) = 1$$

et pour tout $k \geqslant n+1$,

$$s(n,k) = S(n,k) = 0.$$

La valeur absolue du nombre de Stirling de première espèce $|s(n,k)|$ compte le nombre de permutations de S_n qui se décomposent exactement en k cycles disjoints. Alors que le nombre de Stirling de seconde espèce $S(n,k)$ représente le nombre de k-partitions d'un ensemble de cardinal n.

Proposition 2.2 ([21])**.** *Les nombres de Stirling de première espèce $s(n,k)$ satisfont la récurrence "triangulaire" , pour tout entier $n \geqslant 0$ et tout entier $k \geqslant 1$ on a :*

$$s(n+1,k) = s\left(n,k-1\right) - ns(n,k), \tag{2.6}$$

et $s(n,0) = s(0,k) = 0$, sauf $s(0,0) = 1$.

Démonstration. Voir aussi [21] page 49.
Soit $n \geqslant 0$ et $k \geqslant 1$, on a :

$$\begin{aligned}\sum_{k\geqslant 0} s(n+1,k)x^k = x^{\underline{n+1}} = (x-n)\,x^{\underline{n}} &= (x-n)\sum_{k\geqslant 0} s(n,k)x^k \\ &= \sum_{k\geqslant 0} s(n,k)x^{k+1} - n\sum_{k\geqslant 0} s(n,k)x^k \\ &= \sum_{k\geqslant 1} s(n,k-1)x^k - n\sum_{k\geqslant 0} s(n,k)x^k \\ &= -ns(n,0) + \sum_{k\geqslant 1}\left(s(n,k-1) - ns(n,k)\right)x^k.\end{aligned}$$

On en déduit que pour tout $k \geqslant 1$ on a

$$s(n+1,k) = s\left(n,k-1\right) - ns(n,k)$$

et $s\left(n+1,0\right) = -ns(n,0)$. □

On a ici un moyen rapide de calcul des premières valeurs. En particulier, pour tout $n \geqslant 1$,

$$s(n,1) = (-1)^{n-1}\left(n-1\right)!, \quad s(n,n-1) = -\tfrac{1}{2}n^2 + \tfrac{1}{2}n.$$

2.3 Série génératrice de la suite des nombres de Stirling

Proposition 2.3 ([21])**.** *La suite des nombres de Stirling de première espèce $s(n,k)$ a pour série génératrice exponentielle double*

$$\sum_{n,k} s(n,k)\frac{z^n}{n!}x^k = (1+z)^x\,, \tag{2.7}$$

et pour série génératrice exponentielle " verticale "

$$\sum_{n\geqslant k} s(n,k)\frac{z^n}{n!} = \frac{1}{k!}\left(\ln\left(1+z\right)\right)^k. \tag{2.8}$$

Démonstration. D'après la formule du binôme généralisée (2.3),

$$(1+z)^x = \sum_{n\geqslant 0}\binom{x}{n}z^n = \sum_{n\geqslant 0} x^{\underline{n}}\frac{z^n}{n!}.$$

Or, d'après la définition des nombres de Stirling de première espèce (voir Définition 2.1), notamment la relation (2.4), on a

$$x^{\underline{n}} = \sum_{k\geqslant 0} s(n,k)x^k.$$

Par suite

$$(1+z)^x = \sum_{n\geqslant 0}\sum_{k\geqslant 0} s\,(n,k)\,x^k\,\frac{z^n}{n!}.$$

On obtient ainsi la relation (2.7). Pour la preuve de la relation (2.8), il suffit de remarquer que

$$(1+z)^x = \exp\left(x\ln\left(1+z\right)\right),$$

par suite

$$(1+z)^x = \sum_{k\geqslant 0}\left(\ln\left(1+z\right)\right)^k\,\frac{x^k}{k!}.$$

En identifiant le coefficient de z^n dans les deux développements de $(1+z)^x$, on obtient la relation (2.8). □

2.4 Polynômes de Stirling

Dans ce paragraphe, nous allons introduire les polynômes de Stirling, en nous inspirant des travaux de D.S. Mitrinović et R. S. Mitrinović [48] et de ceux de Gessel et Stanley (cf.[34]) qui eux-mêmes se sont inspirés du livre de Charles Jordan [38] "*Calculus of finite differences*". Pour montrer leur existence, ce dernier auteur utilisa le fait que les polynômes de Stirling sont solutions d'une équation aux différences ; une équation qu'il a résolue et qui lui a permis de donner une expression assez simple de ces polynômes.

En effet, si on suppose que pour k fixé il existe un polynôme T_k vérifiant pour tout $n \geqslant k$, $T_k(n) = s(n, n-k)$, alors d'après la relation de récurrence triangulaire (2.6) vérifiée par les nombres de Stirling de première espèce, la suite des polynômes $(T_k)_{k\geqslant 0}$ doit nécessairement vérifier pour tout $n \geqslant k+1$

$$T_{k+1}\left(n+1\right) - T_{k+1}(n) = -nT_k(n) \quad \text{et} \quad T_{k+1}\left(k+1\right) = 0.$$

Par suite,

$$T_{k+1}\left(x+1\right) - T_{k+1}(x) = -xT_k(x) \quad \text{et} \quad T_{k+1}\left(k+1\right) = 0.$$

Autrement dit,

$$\left(\Delta T_{k+1}\right)(x) = -xT_k(x) \quad \text{et} \quad T_{k+1}\left(k+1\right) = 0, \tag{2.9}$$

où Δ est l'opérateur de différence finie défini (cf.[38]) pour tout $P \in \mathbb{C}\left[x\right]$ par :

$$\left(\Delta P\right)(x) = P(x+1) - P(x). \tag{2.10}$$

Voici quelques propriétés de l'opérateur de différence finie Δ .

Proposition 2.4. *Pour tout entier $n \geqslant 1$*

$$\Delta x^{\underline{n}} = n\Delta x^{\underline{n-1}}.$$
$$\Delta\binom{x}{n} = \binom{x}{n-1}.$$

Démonstration. Soit $n \geqslant 1$

$$\begin{aligned}\Delta x^{\underline{n}} &= (x+1)^{\underline{n}} - x^{\underline{n}} = \prod_{j=0}^{n-1}(x+1-j) - \prod_{j=0}^{n-1}(x-j) \\ &= (x+1)\prod_{j=1}^{n-1}(x+1-j) - (x-n+1)\prod_{j=0}^{n-2}(x-j) \\ &= (x+1)\prod_{j=0}^{n-2}(x-j) - (x-n+1)\prod_{j=0}^{n-2}(x-j) \\ &= n\prod_{j=0}^{n-2}(x-j) = nx^{\underline{n-1}}.\end{aligned}$$

La seconde relation est une conséquence directe de la première. □

Proposition 2.5. *Soit P, Q deux polynômes dans $\mathbb{C}[x]$. Si $\Delta P = \Delta Q$ alors il existe un polynôme constant c tel que*

$$P(x) = Q(x) + c.$$

Démonstration. On munit $\mathbb{C}[x]$ de la base $\left(\binom{x}{n}\right)_{n\geqslant 0}$. Posons

$$P(x) = \sum_{k=0}^{n} a_k \binom{x}{k} \quad \text{et} \quad Q(x) = \sum_{k=0}^{m} b_k \binom{x}{k},$$

alors l'égalité $\Delta P = \Delta Q$ entraîne :

$$\sum_{k=1}^{n} a_k \binom{x}{k-1} = \sum_{k=0}^{m} b_k \binom{x}{k-1}.$$

On conclut que $n = m$ et pour tout $k \in \{1, \ldots, n\}$, $a_k = b_k$.
Par suite $P(x) - Q(x) = a_0 - b_0 = c$ □

Proposition 2.6. *Soit $Q \in \mathbb{C}[x]$, il existe un unique polynôme $P \in \mathbb{C}[x]$ vérifiant*

$$\Delta P = Q \text{ et } P(0) = 0.$$

Démonstration. L'unicité du polynôme P est assurée par la proposition 2.5. Reste à montrer l'existence du polynôme P. Comme dans la preuve précédente, on munit $\mathbb{C}[x]$ de la base $\left(\binom{x}{n}\right)_{n\geqslant 0}$. Si on pose

$$Q(x) = \sum_{k=0}^{n} a_k \binom{x}{k},$$

alors

$$P(x) = \sum_{k=0}^{n} a_k \binom{x}{k+1}.$$

En effet, on a bien $P(0) = 0$ et

$$\Delta P = \sum_{k=0}^{n} a_k \Delta\binom{x}{k+1} = \sum_{k=0}^{n} a_k \binom{x}{k} = Q.$$

□

Théorème 2.7. *Il existe une et une seule suite $(T_k)_{k\geqslant 0}$ de polynômes à coefficients dans $\mathbb{Q}$ telle que $T_0(x) = 1$ et pour tout $k \geqslant 1$,*

$$T_k(x+1) - T_k(x) = -xT_{k-1}(x) \text{ et } T_k(0) = 0. \tag{2.11}$$

De plus, ces polynômes vérifient pour tout $k \geqslant 0$ et tout $n \geqslant, k$

$$T_k(n) = s(n, n-k). \tag{2.12}$$

Démonstration. L'existence et l'unicité de la suite $(T_k)_{k\geqslant 0}$ sont données par la proposition 2.6. Avant de montrer par récurrence la relation (2.12), montrons que pour tout $k \geqslant 1$, les entiers $0, \ldots, k$ sont des racines de T_k.

La relation (2.11) donne pour $k = 1$ et $x = 0$

$$T_1(1) - T_1(0) = 0.$$

Or $T_1(0) = 0$, donc

$$T_1(1) = T_1(0) = 0.$$

Soit $k \geqslant 1$, supposons que

$$T_k(k) = \cdots = T_k(1) = T_k(0) = 0.$$

On a pour tout $j \in \{0, \ldots, k\}$,

$$T_{k+1}(j+1) - T_{k+1}(j) = -jT_k(j) = 0,$$

donc la famille $(T_{k+1}(j))_{0\leqslant j\leqslant k+1}$ est constante, et comme, par définition, $T_{k+1}(0) = 0$, on obtient alors

$$T_{k+1}(k+1) = \cdots = T_{k+1}(1) = T_{k+1}(0) = 0.$$

Ainsi pour tout $k \geqslant 1$,

$$T_k(k) = \cdots = T_k(1) = T_k(0) = 0. \tag{2.13}$$

Démontrons maintenant, par récurrence, que pour tout $k \geqslant 0$ et tout $n \geqslant k$,

$$T_k(n) = s(n, n-k).$$

Pour $k = 0$, $T_0 = 1$. Donc pour tout $n \geqslant 0$, $T_0(n) = s(n, n)$.
Soit $k \geqslant 0$, supposons que pour tout $n \geqslant k$,

$$T_k(n) = s(n, n-k) \tag{2.14}$$

et montrons par récurrence sur n que pour tout $n \geqslant k+1$,

$$T_{k+1}(n) = s(n, n-k-1).$$

Pour $n = k+1$, grâce à la relation (2.13), on obtient :

$$T_{k+1}(k+1) = 0 = s(k+1, 0).$$

Soit $n \geqslant k+1$, supposons que

$$T_{k+1}(n) = s\left(n, n-k-1\right) \tag{2.15}$$

alors, d'après la relation (2.11),

$$T_{k+1}\left(n+1\right) = T_{k+1}(n) - nT_k(n),$$

qui donne d'après les hypothèses de récurrence (2.14) et (2.15)

$$T_{k+1}\left(n+1\right) = s\left(n, n-k-1\right) - ns(n, n-k).$$

Reste à appliquer la relation de récurrence triangulaire (2.6) pour obtenir

$$T_{k+1}\left(n+1\right) = s\left(n+1, n-k\right).$$

□

Définition 2.8. *La suite de polynômes $(T_k)_{k\geqslant 0}$ définie dans le théorème 2.7 s'appelle suite de polynômes de Stirling.*

La dernière proposition montre l'existence des polynômes de Stirling mais elle ne fournit aucun moyen rapide pour les déterminer. Sachant que les polynômes de Stirling sont solutions d'une équation aux différences finies $\Delta T_{k+1}(x) = -xT_k(x)$. Nous allons montrer que l'utilisation de la base binomiale $\left(\binom{x}{n}\right)_{n\geqslant 0}$ va nous permettre d'obtenir une relation de récurrence triangulaire vérifiée par les coefficients des polynômes T_k. En effet la relation $\Delta\binom{x}{n} = \binom{x}{n-1}$ (voir proposition 2.4) nous simplifiera énormément les calculs.

Proposition 2.9 ([38] p. 251)**.** *Il existe une suite double d'entiers $c(k,n)$ vérifiant pour tout $n \geqslant 0$,*

$$T_k(x) = \sum_{n\geqslant 0} c\left(k,n\right)\binom{x}{n},$$

où

1. *$c(0,0) = 1$ et pour tout $n \geqslant 1$, $c(0,n) = 0$.*
2. *Pour tout $k \geqslant 1$, $c\left(k,0\right) = c\left(k,1\right) = 0$ et pour tout $n \geqslant 1$*

$$c\left(k,n+1\right) = -n\left(c\left(k-1,n-1\right) + c(k-1,n)\right). \tag{2.16}$$

3. *Si $k \geqslant 1$, $x^{\underline{k}}$ divise $T_k(x)$.*

Démonstration. 1. On a $T_0 = 1$, donc

$$T_0(x) = \sum_{n\geqslant 0} c\left(0,n\right)\binom{x}{n},$$

où $c\left(0,0\right) = 1$ et pour tout $n \geqslant 1$, $c(0,n) = 0$.

2. Soit $k \geqslant 1$, il existe alors une suite de nombres rationnels $c(k,n)$ vérifiant

$$T_k(x) = \sum_{n\geqslant 0} c\left(k,n\right)\binom{x}{n}.$$

La relation $\Delta T_k = -xT_{k-1}$ est équivalente à

$$\sum_{n\geqslant 1} c\,(k,n)\binom{x}{n-1} = -x\sum_{n\geqslant 0} c\,(k-1,n)\binom{x}{n}.$$

Par suite,

$$\begin{aligned}\sum_{n\geqslant 0} c\,(k,n+1)\binom{x}{n} &= -\sum_{n\geqslant 0} c\,(k-1,n)\,(x-n)\binom{x}{n} - \sum_{n\geqslant 0} nc\,(k-1,n)\binom{x}{n}\\ &= -\sum_{n\geqslant 0} c\,(k-1,n)\,(n+1)\binom{x}{n+1} - \sum_{n\geqslant 1} nc\,(k-1,n)\binom{x}{n}\\ &= -\sum_{n\geqslant 1} n\,(c(k-1,n-1)+c(k-1,n))\binom{x}{n}.\end{aligned}$$

On en déduit que pour tout $k \geqslant 1$, $c\,(k,1) = 0$ et pour tout $n \geqslant 1$,

$$c\,(k,n+1) = -n\,(c\,(k-1,n-1) + c\,(k-1,n))\,.$$

3. Montrons par récurrence que pour tout $n \geqslant 1$, et pour tout $1 \leqslant k \leqslant n$, $T_n\,(k) = 0$.
Pour $n = 1$, on a $\Delta T_1(x) = xT_0(x)$. D'où $T_1\,(x+1) - T_1(x) = x$. Pour $x = 0$, sachant que pour tout $n \geqslant 1$, $T_n\,(0) = 0$, on obtient $T_1\,(1) = 0$. L'hypothèse de récurrence est vérifiée pour T_1.
Supposons que pour tout $k \in \{0,\ldots,n\}$, $T_n\,(k) = 0$.
L'égalité $\Delta T_{n+1} = T_n$ entraîne que pour tout $k \in \{1,\ldots,n\}$,

$$T_{n+1}\,(k+1) - T_{n+1}\,(k) = kT_n\,(k) = 0.$$

Donc pour tout $k \in \{0,\ldots,n\}$,

$$T_n\,(k+1) = T_n\,(k)\,.$$

Conclusion

$$T\,(n+1) = T(n) = \cdots = T\,(1) = T\,(0) = 0.$$

□

Grâce à la récurrence triangulaire (2.16) on a pu calculer, sans grande difficulté, mais à l'aide d'un logiciel, les premières valeurs de la suite $(c\,(k,n))_{n,k}$ ainsi que les premières expressions des polynômes de Stirling $T_k(x)$.

$k\backslash n$	0	1	2	3	4	5	6	7	8	9	10	11	12
0	1	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	−1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	2	3	0	0	0	0	0	0	0	0
3	0	0	0	0	−6	−20	−15	0	0	0	0	0	0
4	0	0	0	0	0	24	130	210	105	0	0	0	0
5	0	0	0	0	0	0	−120	−924	−2380	−2520	−945	0	0

$$
\begin{aligned}
T_0(x) &= 1\\
T_1(x) &= -\binom{x}{2}\\
T_2(x) &= 2\binom{x}{3}+3\binom{x}{4}\\
T_3(x) &= -6\binom{x}{4}-20\binom{x}{5}-15\binom{x}{6}\\
T_4(x) &= 24\binom{x}{5}+130\binom{x}{6}+210\binom{x}{7}+105\binom{x}{8}\\
T_5(x) &= -120\binom{x}{6}-924\binom{x}{7}-2380\binom{x}{8}-2520\binom{x}{9}-1050\binom{x}{10}.
\end{aligned}
$$

On remarque, d'après ce dernier tableau, que pour tout $1 \leqslant k \leqslant 5$,

$$c(k,n) = (-1)^k |c(k,n)| \quad \text{et} \quad T_k = \sum_{n=k+1}^{2k} c(k,n) \binom{x}{n}.$$

Plus généralement, on a la proposition suivante.

Proposition 2.10. *Pour tout $k \geqslant 1$,*

$$T_k(x) = \sum_{n=k+1}^{2k} c(k,n) \binom{x}{n}.$$

et pour tout $n \geqslant 0$, $c(k,n) = (-1)^k |c(k,n)|$.

Démonstration. Pour $k = 1$, les deux relations sont vérifiées.
Soit $k \geqslant 1$, supposons que $T_k(x) = \sum_{n=k+1}^{2k} c(k,n) \binom{x}{n}$ et $n \geqslant 0$, $|c(k,n)| = (-1)^k c(k,n)$.
On a, d'après la relation de récurrence triangulaire (2.16)

$$c(k+1,n) = -(n-1)(c(k,n-2) + c(k,n-1)).$$

Par hypothèse de récurrence, pour tout n, $n \leqslant k+1$ ou $n \geqslant 2k+3$,

$$c(k,n-2) = c(k,n-1) = 0.$$

D'où

$$c(k+1,n+1) = 0.$$

Par suite

$$T_{k+1}(x) = \sum_{n=k+2}^{2k+2} c(k+1,n) \binom{x}{n}.$$

De plus, puisque par hypothèse,

$$c(k,n-2) = (-1)^k |c(k,n-2)| \text{ et } c(k,n-1) = |c(k,n-1)|.$$

On obtient finalement :

$$c(k+1,n) = (-1)^{k+1} |c(k+1,n)|.$$

□

2.5 Polynômes de Nörlund

Soit $(B_n)_{n\geqslant 0}$ la suite des nombres de Bernoulli définie par

$$\frac{z}{e^z-1}=\sum_{n\geqslant 0}B_n\frac{z^n}{n!}=1+\sum_{n\geqslant 1}B_n\frac{z^n}{n!}.$$

Il est bien connu que pour tout $n\geqslant 1$

$$B_{2n}\neq 0 \text{ et } B_{2n+1}=0. \tag{2.17}$$

Posons

$$R(z)=\sum_{n\geqslant 1}B_n\frac{z^n}{n!}=-\frac{1}{2}z+\frac{1}{6}\frac{z^2}{2!}-\frac{1}{30}\frac{z^4}{4!}+\frac{1}{42}\frac{z^6}{6!}+\cdots.$$

Définissons la suites double $(\sigma(n,k))_{n,k\geqslant 0}$ par

$$R^k(z)=\sum_{n\geqslant 0}\sigma(n,k)\frac{z^n}{n!}.$$

Comme $\mathrm{val}\,(R)=1$, alors $\mathrm{val}\left(R^k\right)=k$; autrement dit

$$R^k(z)=\sum_{n\geqslant k}\sigma(n,k)\frac{z^n}{n!}.$$

Il n'est pas difficile de voir que la suite double $(\sigma(n,k))_{n,k\geqslant 0}$ est définie par $\sigma(0,0)=1$, pour tout $n\geqslant 1$ $\sigma(n,0)=0$, et pour tout $n,k\geqslant 0$:

$$\sigma\,(n,k+1)=\sum_{h=1}^{n-k}\binom{n}{h}B_h\sigma(n-h,k). \tag{2.18}$$

Donnons quelques premiers termes de la suite $(\sigma(n,k))_{n,k\geqslant 0}$

$k\backslash n$	0	1	2	3	4	5	6
0	1	0	0	0	0	0	0
1	0	$-\frac{1}{2}$	$\frac{1}{6}$	0	$-\frac{1}{30}$	0	$\frac{1}{42}$
2	0	0	$\frac{1}{2}$	$-\frac{1}{2}$	$\frac{1}{6}$	$\frac{1}{6}$	$-\frac{1}{6}$
3	0	0	0	$-\frac{3}{4}$	$\frac{3}{2}$	$-\frac{5}{4}$	$-\frac{1}{3}$
4	0	0	0	0	$\frac{3}{2}$	-5	$\frac{15}{2}$
5	0	0	0	0	0	$-\frac{15}{4}$	$\frac{75}{4}$
6	0	0	0	0	0	0	$\frac{45}{4}$

Puisque On a

$$\frac{z}{e^z-1}=1+R(z),$$

alors

$$\left(\frac{z}{e^z-1}\right)^x = (1+R(z))^x = \sum_{k\geqslant 0}\binom{x}{k}R^k(z)$$
$$= \sum_{k\geqslant 0}\binom{x}{k}\sum_{n\geqslant k}\sigma\left(n,k\right)\frac{z^n}{n!}$$
$$= \sum_{n\geqslant 0}\left(\sum_{k=0}^{n}\sigma(n,k)\binom{x}{k}\right)\frac{z^n}{n!}.$$

Posons pour tout $n \geqslant 0$

$$B_n^{(x)} = \sum_{k=0}^{n}\sigma(n,k)\binom{x}{k}. \tag{2.19}$$

On a donc

$$\left(\frac{z}{e^z-1}\right)^x = \sum_{n\geqslant 0}B_n^{(x)}\frac{z^n}{n!}. \tag{2.20}$$

La suite de polynômes $\left(B_n^{(x)}\right)_{n\geqslant 0}$ s'appelle la suite des polynômes de Nörlund qui ont été introduits dans ([57], Chapitre 6), par Niels E. Nörlund (1885-1981). Ils sont aussi appelés nombres généralisés de Bernoulli d'ordre x.

Voici leurs premières valeurs :

$$\begin{aligned}
B_0^{(x)} &= 1\\
B_1^{(x)} &= -\tfrac{1}{2}x\\
B_2^{(x)} &= \tfrac{1}{6}\binom{x}{1} + \tfrac{1}{2}\binom{x}{2}\\
B_3^{(x)} &= \tfrac{-1}{2}\binom{x}{2} - \tfrac{3}{4}\binom{x}{3}\\
B_4^{(x)} &= -\tfrac{1}{30}x + \tfrac{1}{6}\binom{x}{2} + \tfrac{3}{2}\binom{x}{3} + \tfrac{3}{2}\binom{x}{4}\\
B_5^{(x)} &= \tfrac{1}{6}\binom{x}{2} - \tfrac{5}{4}\binom{x}{3} - 5\binom{x}{4} - \tfrac{15}{4}\binom{x}{5}\\
B_6^{(x)} &= \tfrac{1}{42}x - \tfrac{1}{6}\binom{x}{2} - \tfrac{1}{3}\binom{x}{3} + \tfrac{15}{2}\binom{x}{4} + \tfrac{75}{4}\binom{x}{5} + \tfrac{45}{4}\binom{x}{6}
\end{aligned}$$

i.e. :

$$\begin{aligned}
B_0^{(x)} &= 1\\
B_1^{(x)} &= -\tfrac{1}{2}x\\
B_2^{(x)} &= \tfrac{1}{4}x^2 - \tfrac{1}{12}x\\
B_3^{(x)} &= -\tfrac{1}{8}x^3 + \tfrac{1}{8}x^2\\
B_4^{(x)} &= \tfrac{1}{16}x^4 - \tfrac{1}{8}x^3 + \tfrac{1}{48}x^2 + \tfrac{1}{120}x\\
B_5^{(x)} &= -\tfrac{1}{32}x^5 + \tfrac{5}{48}x^4 - \tfrac{5}{96}x^3 - \tfrac{1}{48}x^2\\
B_6^{(x)} &= \tfrac{1}{64}x^6 - \tfrac{5}{64}x^5 + \tfrac{5}{64}x^4 + \tfrac{13}{576}x^3 - \tfrac{1}{96}x^2 - \tfrac{1}{252}x
\end{aligned}$$

Proposition 2.11. *Pour tout $n \geqslant 0$, $B_n^{(x)}$ est un polynôme à coefficients rationnels de degré n, divisible par x pour $n \geqslant 1$ et de coefficient dominant $\left(-\frac{1}{2}\right)^n$.*

Démonstration. D'après la relation (2.19),

$$B_n^{(x)} = \sum_{k=0}^{n} \frac{\sigma(n,k)}{k!} x^{\underline{k}},$$

donc

$$[x^n]B_n^{(x)} = \frac{\sigma\,(n,n)}{n!}.$$

En utilisant la relation de récurrence (2.18), on obtient que pour tout $n \geqslant 1$

$$\sigma\,(n,n) = \frac{-1}{2} n\sigma(n-1,n-1).$$

On en déduit que pour tout $n \geqslant 0$

$$\sigma\,(n,n) = \left(\frac{-1}{2}\right)^n n!\sigma(0,0).$$

Or $\sigma\,(0,0) = 1$, donc

$$[x^n]B_n^{(x)} = \left(\frac{-1}{2}\right)^n.$$

Par conséquent $\deg\left(B_n^{(x)}\right) = n$.
Soit $n \geqslant 1$, $\sigma\,(n,0)$ est le coefficient constant de $R^n(z)$ qui est nul, vu que $\operatorname{val} R = 1$. Donc, d'après la relation (2.19),

$$B_n^{(x)} = \sum_{k=1}^{n} \sigma(n,k)\binom{x}{k}.$$

Il est par conséquent divisible par x. □

La proposition suivante donne une relation très utile entre les polynômes de Stirling et les polynômes de Nörlund . Elle figure comme "exercice" dans [15], p. 329.

Proposition 2.12. *Soit* $\left(B_n^{(x)}\right)_{n\geqslant 0}$ *la suite des polynômes de Nörlund. On a alors :*

1. $B_0^{(x)} = 1$ *et pour tout* $n \geqslant 1$

$$B_n^{(x+1)} = \left(1 - \frac{n}{x}\right) B_n^{(x)} - nB_{n-1}^{(x)}. \tag{2.21}$$

2. *Pour tout* $n \geqslant 0$

$$\binom{x-1}{n} B_n^{(x)} = T_n(x). \tag{2.22}$$

où $(T_n)_{n\geqslant 0}$ *est la suite des polynômes de Stirling.*

Démonstration. On pose

$$S_x(z) = \left(\frac{z}{e^z - 1}\right)^x = \sum_{n\geqslant 0} B_n^{(x)} \frac{z^n}{n!}.$$

Donc

$$S_{x+1}(z) = \sum_{n\geqslant 0} B_n^{(x+1)} \frac{z^n}{n!},$$

d'où

$$\sum_{n\geqslant 0} nB_n^{(x)}\frac{z^{n-1}}{n!} = \frac{d}{dz}S_x(z) = \frac{x}{z}\frac{(-ze^z+e^z-1)}{e^z-1}\left(\frac{z}{e^z-1}\right)^x$$
$$= -x\left(\frac{z}{e^z-1}\right)^x + \frac{-x}{z}\left(\frac{z}{e^z-1}\right)^{x+1} + \frac{x}{z}\left(\frac{z}{e^z-1}\right)^x.$$

Par conséquent

$$\sum_{n\geqslant 0}\frac{n}{x}B_n^{(x)}\frac{z^n}{n!} = -z\left(\frac{z}{e^z-1}\right)^x - \left(\frac{z}{e^z-1}\right)^{x+1} + \left(\frac{z}{e^z-1}\right)^x.$$

Par suite,

$$\sum_{n\geqslant 0} B_n^{(x+1)}\frac{z^n}{n!} = \sum_{n\geqslant 0} B_n^{(x)}\frac{z^n}{n!} - z\sum_{n\geqslant 0} B_n^{(x)}\frac{z^n}{n!} - \sum_{n\geqslant 0}\frac{n}{x}B_n^{(x)}\frac{z^n}{n!}$$
$$= \sum_{n\geqslant 0}\left(1-\frac{n}{x}\right)B_n^{(x)}\frac{z^n}{n!} - \sum_{n\geqslant 0}(n+1)\,B_n^{(x)}\frac{z^{n+1}}{(n+1)!}$$
$$= \sum_{n\geqslant 0}\left(1-\frac{n}{x}\right)B_n^{(x)}\frac{z^n}{n!} - \sum_{n\geqslant 1} nB_{n-1}^{(x)}\frac{z^n}{n!}$$
$$= B_0^{(x)} + \sum_{n\geqslant 1}\left(\left(1-\frac{n}{x}\right)B_n^{(x)} - nB_{n-1}^{(x)}\right)\frac{z^n}{n!}.$$

Par identification on obtient $B_0^{(x+1)} = B_0^{(x)}$ et pour tout $n \geqslant 1$

$$B_n^{(x+1)} = \left(1-\frac{n}{x}\right)B_n^{(x)} - nB_{n-1}^{(x)}.$$

Posons pour tout $n \geqslant 0$

$$\Gamma_n(x) = \binom{x-1}{n}B_n^{(x)}.$$

D'après la relation de récurrence (2.21),

$$\Gamma_n(x+1) = \binom{x}{n}B_n^{(x+1)} = \binom{x}{n}\left(\left(1-\frac{n}{x}\right)B_n^{(x)} - nB_{n-1}^{(x)}\right)$$
$$= \binom{x-1}{n}B_n^{(x)} - x\binom{x-1}{n-1}B_{n-1}^{x}$$
$$= \Gamma_n(x) - x\Gamma_{n-1}(x).$$

Autrement dit

$$\Delta\Gamma_n(x) = -x\Gamma_{n-1}(x).$$

De plus $\Gamma_0(x) = 1$ et pour tout $n \geqslant 1$, $\Gamma_n(0) = 0$. D'après le théorème 2.7, pour tout $n \geqslant 0$

$$\Gamma_n(x) = T_n(x).$$

□

Dans ([43], Théorèmes 1 et 2), Liu et Srivastava ont déterminé explicitement les coefficients de

$B_n^{(x)}$ en prouvant que le coefficient de x^k dans $B_n^{(x)}$ est donné par

$$[x^k]B_n^{(x)} = (-1)^{j-k}\frac{n!}{k!}\sum \frac{B_{v_1}\cdots B_{v_k}}{(v_1\cdots v_k)v_1!\cdots v_k!} \quad (1 \leqslant k \leqslant n), \tag{2.23}$$

la sommation ayant lieu sur les entiers $\nu_1, ..., \nu_k \geqslant 1$, tels que $\nu_1 + \cdots + \nu_k = n$.

On peut donc en déduire la proposition suivante.

Proposition 2.13 ([7])**.** *Pour $n \geqslant 1$, on a*

$$[x]\left(B_n^{(x)}\right) = (-1)^{n-1}\frac{B_n}{n}, \tag{2.24}$$

$$[x^2]\left(B_{2n+1}^{(x)}\right) = \frac{2n+1}{4n}B_{2n}. \tag{2.25}$$

Démonstration. Soit $n \geqslant 1$.

Pour $k = 2$, la relation (2.23) permet d'écrire :

$$[x^2]B_{2n+1}^{(x)} = (-1)^{2n-1}\frac{(2n+1)!}{2}\sum_{j=1}^{2n}\frac{B_jB_{2n+1-j}}{j\,(2n+1-j)\,j!\,(2n+1-j)!}.$$

Donc

$$[x^2]B_{2n+1}^{(x)} = \frac{-1}{2}\sum_{j=1}^{2n}\binom{2n+1}{j}\frac{B_jB_{2n+1-j}}{j\,(2n+1-j)}. \tag{2.26}$$

On distingue deux cas. Le premier est trivial, il correspond au cas $n = 1$. En effet

$$\begin{aligned}[x^2]B_3^{(x)} &= \frac{-1}{2}\sum_{j=1}^{2}\binom{3}{j}\frac{B_jB_{3-j}}{j\,(3-j)}\\ &= -\frac{3B_1B_2}{2} = \frac{3B_2}{4}.\end{aligned}$$

Supposons maintenant que $n \geqslant 2$. Réécrivons la relation (2.26) en détachant de la somme son premier et son dernier terme.

$$[x^2]B_{2n+1}^{(x)} = \frac{2n+1}{4n}B_{2n} - \frac{1}{2}\sum_{j=2}^{2n-1}\binom{2n+1}{j}\frac{B_jB_{2n+1-j}}{j(2n+1-j)}. \tag{2.27}$$

Ainsi la relation (2.25) est bien vérifiée pour $n \geqslant 2$ en remarquant que les termes figurant sous le signe somme dans la relation (2.27) sont tous nuls ; en effet, car pour $n \geqslant 2$ et $2 \leqslant j \leqslant 2n-1$, l'un au moins des deux nombres de Bernoulli B_j ou B_{2n+1-j} est d'indice impair strictement plus grand que 1 et par suite $B_jB_{2n+1-j} = 0$. □

Proposition 2.14. *Soit $n \geqslant 2$.*

1. *Si n est pair alors $x = 0$ est une racine simple de $B_n^{(x)}$.*
2. *Si n est impair alors $x = 0$ est une racine double de $B_n^{(x)}$.*

Démonstration. Ce résultat a déjà été prouvé par Adelberg (voir [1], Lemma 9.2). On donnera ici une preuve différente utilisant la proposition 2.13. On rappelle que, d'après la proposition 2.11, $B_n^{(0)} = 0$.

Si n est pair , d'après les relations (2.17) et (2.24), $[x]\left(B_n^{(x)}\right) \neq 0$. Par conséquent $x = 0$ est une racine simple. Par contre si $n \geqslant 3$ est impair, d'après les relations (2.17), (2.24) et (2.25), $[x]\left(B_n^{(x)}\right) = 0$ et $\left[x^2\right] B_n^{(x)} \neq 0$, par suite $x = 0$ est une racine double. □

2.6 Dénominateurs communs des coefficients des polynômes de Stirling et de Nörlund

Les polynômes de Narumi $A_n(s,x)$ (cf. [2]) introduits en 1929 par Seimatsu Narumi (cf. [53]), sont définis par :

$$\sum_{n\geqslant 0} A_n(s,x)\frac{z^n}{n!} = \left(\frac{\ln(1+z)}{z}\right)^x (1+z)^s.$$

Dans [1], Adelberg donne une expression explicite des polynômes $A_n(s,x)$. Il montre que pour tout $n \geqslant 0$,

$$A_n(s,x) = \sum_{k=0}^{n} \binom{s}{n-k} c_k(x)$$

avec

$$c_k(x) = (-1)^k n! \sum_{\substack{u=(u_1,\ldots,u_n)\in\mathbb{N}^n \\ w(u)=k}} \binom{x}{d}\binom{d}{u} \frac{1}{2^{u_1}3^{u_2}\cdots(n+1)^{u_n}},$$

où pour tout $u = (u_1, u_2, \ldots, u_n) \in \mathbb{N}^n$, $w(u)$ est le poids du vecteur u défini par

$$w(u) = \sum_{k=1}^{n} k u_k = u_1 + 2u_2 + \cdots + nu_n,$$

$d = d(u) = \sum_{k=1}^{n} u_k$ et $\binom{d}{u} = \binom{d}{u_1,\ldots,u_n}$ est le coefficient multinomial défini par

$$\binom{d}{u_1,\ldots,u_n} = \frac{(u_1+\cdots+u_n)!}{u_1!\cdots u_n!} = \frac{d!}{u_1!\cdots u_n!}.$$

Puis il montre que les polynômes de Nörlund peuvent être obtenus par la relation suivante

$$B_n^{(x+n+1)} = A_n(-1,x).$$

Il obtient, alors, pour tout $n \geqslant 1$ la formule explicite suivante :

$$B_n^{(x)} = (-1)^n n! \sum_{\substack{u=(u_1,\ldots,u_n)\in\mathbb{N}^n \\ w(u)\leqslant n}} \binom{x-n-1}{d} \frac{d!}{u_1!u_2!\cdots u_n!} \frac{1}{2^{u_1}3^{u_2}\cdots(n+1)^{u_n}}. \tag{2.28}$$

Exemple 2.15. *1. Calcul de $B_1^{(x)}$: On a*

$$\begin{aligned} B_1^{(x)} &= -\sum_{\substack{u=u_1\in\mathbb{N} \\ w(u_1)\leqslant 1}} \binom{x-2}{d} \frac{d!}{u_1!}\frac{1}{2^{u_1}} = -\binom{x-2}{0} - \binom{x-1}{1}\frac{1}{2} \\ &= -1 - \frac{1}{2}(x-2) = -\frac{1}{2}x. \end{aligned}$$

2. *Calcul de* $B_2^{(x)}$ *: On a*

$$B_2^{(x)} = (-1)^2 2! \sum_{\substack{u=(u_1,u_2)\in\mathbb{N}^2 \\ w(u)\leqslant 2}} \binom{x-3}{d} \frac{d!}{u_1!u_2!} \frac{1}{2^{u_1}3^{u_2}},$$

L'ensemble des vecteurs $u = (u_1, u_2) \in \mathbb{N}^2$ *de poids* w *inférieur à* 2 *est*

$$W_2 = \{(0,0), (1,0), (2,0), (0,1)\}.$$

Donc

$$\begin{aligned} B_2^{(x)} &= 2! \sum_{(u_1,u_2)\in\mathbb{W}_2} \binom{x-3}{u_1+u_2} \frac{(u_1+u_2)!}{u_1!u_2!} \frac{1}{2^{u_1}3^{u_2}} \\ &= 2! \left(\binom{x-3}{0} + \binom{x-3}{1}\frac{1}{2} + \binom{x-3}{2}\frac{1}{2^2} + \binom{x-3}{1}\frac{1}{3} \right) \\ &= \frac{1}{4}x^2 - \frac{1}{12}x = \frac{1}{12}\left(3x^2 - x\right). \end{aligned}$$

3. *Calcul de* $B_3^{(x)}$ *: On a*

$$B_3^{(x)} = (-1)^3 3! \sum_{\substack{u=(u_1,u_2,u_3)\in\mathbb{N}^3 \\ u_1+2u_2+3u_3\leqslant 3}} \binom{x-4}{u_1+u_2+u_3} \frac{(u_1+u_2+u_3)}{u_1!u_2!u_3!} \frac{1}{2^{u_1}3^{u_2}4^{u_3}}.$$

L'ensemble des vecteurs $u = (u_1, u_2, u_3) \in N^3$ *de poids* w *inférieur à* 3 *est*

$$W_3 = \{(0,0,0), (1,0,0), (2,0,0), (3,0,0), (0,1,0), (1,1,0), (0,0,1)\}.$$

Donc

$$\begin{aligned} B_3^{(x)} &= -3! \sum_{(u_1,u_2,u_3)\in W_3} \binom{x-4}{u_1+u_2+u_3} \frac{(u_1+u_2+u_3)!}{u_1!u_2!u_3!} \frac{1}{2^{u_1}3^{u_2}4^{u_3}} \\ &= -3! \left(\binom{x-4}{0} + \binom{x-4}{1}\frac{1}{2^1} + \binom{x-4}{2}\frac{1}{2^2} + \binom{x-4}{3}\frac{1}{2^3} \right. \\ &\left. + \binom{x-4}{1}\frac{1}{3} + \binom{x-4}{2}\frac{1}{3} + \binom{x-4}{1}\frac{1}{4} \right) \\ &= -\frac{1}{8}x^3 + \frac{1}{8}x^2 = \frac{1}{8}\left(-x^3 + x^2\right). \end{aligned}$$

Pour tout nombre p premier, désignons par $v_p(n)$ la valuation p-adique de n, c'est à dire l'exposant de la plus grande puissance de p divisant n, et pour tout nombre réel x, désignons par $\lfloor x \rfloor$ la partie entière de x, i.e. l'unique entier rationnel j vérifiant : $x - 1 < j \leqslant x$.

En 1999, grâce à la relation explicite (2.28), Adelberg détermina le dénominateur commun des coefficients de $B_k^{(x)}$. Il démontre le théorème suivant.

Théorème 2.16 ([3]). *Soit $n \geqslant 0$, le dénominateur commun des coefficients de $B_n^{(x)}$ est :*

$$d_n = \frac{1}{n!} \prod_{p \text{ premier}} p^{v_p\left(\left(p\left\lfloor \frac{n}{p-1} \right\rfloor\right)!\right)}.$$

Pour tout $n \geqslant 0$, d_n est un entier et $d_n B_n^{(x)}$ est un polynôme primitif de $\mathbb{Z}[x]$.

Démonstration. Voir [3, Corollary 3 p.9]. □

On remarque que pour $p > n+1$, $\left\lfloor \frac{n}{p-1} \right\rfloor = 0$. Par suite $v_p\left(\left(p\left\lfloor \frac{n}{p-1} \right\rfloor\right)!\right) = 0$ pour tout $p > n+1$. Donc d_n est en fait un produit fini.

Proposition 2.17. *Pour tout $n \geqslant 0$,*

$$d_n = \frac{1}{n!} \prod_{p \in \mathbb{P}} p^{\left\lfloor \frac{n}{(p-1)} \right\rfloor + \left\lfloor \frac{n}{p(p-1)} \right\rfloor + \left\lfloor \frac{n}{p^2(p-1)} \right\rfloor + \cdots}.$$

Démonstration. On rappelle la formule de Legendre (cf. [68], p. 31), où pour tout $n \geqslant 0$,

$$v_p(n!) = \sum_{k \geqslant 1} \left\lfloor \frac{n}{p^k} \right\rfloor. \tag{2.29}$$

Donc pour tout nombre premier p tel que $p \leqslant n+1$, il vient :

$$v_p\left(\left(p\left\lfloor \frac{n}{p-1} \right\rfloor\right)!\right) = \sum_{k \geqslant 0} \left\lfloor \frac{1}{p^k} \left\lfloor \frac{n}{p-1} \right\rfloor \right\rfloor. \tag{2.30}$$

Par ailleurs, pour tout nombre réel x et tout entier positif non nul m (cf. [35] p. 77), on a :

$$\left\lfloor \frac{\lfloor x \rfloor}{m} \right\rfloor = \left\lfloor \frac{x}{m} \right\rfloor.$$

En effet, si on suppose que ces deux nombres possèdent des parties entières différentes, alors il existe un entier ℓ vérifiant

$$\frac{\lfloor x \rfloor}{m} < \ell \leqslant \frac{x}{m}.$$

Par conséquent

$$\lfloor x \rfloor < \ell m \leqslant x.$$

Ce qui est en contradiction avec la caractérisation de la partie entière. L'égalité (2.30) donne alors :

$$v_p\left(\left(p\left\lfloor \frac{n}{p-1} \right\rfloor\right)!\right) = \sum_{k \geqslant 0} \left\lfloor \frac{n}{p^k(p-1)} \right\rfloor.$$

Ce qui achève la preuve de la proposition. □

Proposition 2.18. *Soit $n \geqslant 0$, le dénominateur commun D_n des coefficients de $T_n(x)$ vérifie :*

$$D_n = n! d_n = \prod_{p \in \mathbb{P}} p^{\left\lfloor \frac{n}{(p-1)} \right\rfloor + \left\lfloor \frac{n}{p(p-1)} \right\rfloor + \left\lfloor \frac{n}{p^2(p-1)} \right\rfloor + \cdots}.$$

De plus, pour tout $n \geqslant 0$, $n! d_n T_n(x)$ est un polynôme primitif de $\mathbb{Z}[x]$.

Démonstration. Soit $n \geqslant 0$, d'après la proposition 2.12,

$$T_n(x) = \binom{x-1}{n} B_n^{(x)}.$$

En multipliant les deux membres de cette relation par $n!d_n$, on obtient :

$$n!d_nT_n = (x-1)(x-2)\cdots(x-n)\left(d_nB_n^{(x)}\right).$$

D'après le théorème 2.16, $n!d_nT_n(x)$ est donc un produit de polynômes primitifs de $\mathbb{Z}[x]$. Ainsi $n!d_nT_n(x)$ est lui-même un polynôme primitif de $\mathbb{Z}[x]$. □

La suite d'entiers

$$(d_n)_{n\geqslant 0} = (1, 2, 12, 8, 240, 96, 4032, 1152, 34560, 7680, 101376, 18432, 50319360, \ldots)$$

est répertoriée A001898 dans [66]. Soit $(M_n)_{n\geqslant 1}$ la suite définie par

$$M_n = \prod_p p^{\left\lfloor \frac{n-1}{(p-1)} \right\rfloor + \left\lfloor \frac{n-1}{p(p-1)} \right\rfloor + \left\lfloor \frac{n-1}{p^2(p-1)} \right\rfloor + \cdots}.$$

La suite d'entiers $(M_n)_{n\geqslant 0}$, répertoriée A053657 dans [66], a été appelée suite des nombres de Minkowski par Martin Lorenz (cf. [36]). C'est en effet en 1887 que Minkowski (cf. [47]) a prouvé que M_n est égal au plus petit commun multiple des ordres de tous les sous-groupes finis de $GL_n(\mathbb{Q})$. La notation M_n est due à Schur cf. [65]. On a donc, pour tout $n \geqslant 0$,

$$d_n = \frac{1}{n!} M_{n+1}.$$

Le nombre M_n peut aussi être interprété comme la n-ième factorielle de l'ensemble $\mathbb{P}$ des nombres premiers (cf.[8]). Dans [8], Manjul Bhargava montre que si f est un polynôme primitif de degré n à coefficients dans $\mathbb{Z}$ et $d = \operatorname{pgcd}\{f(p) \mid p \in \mathbb{P}\}$ alors d divise M_n. En 1996, Jean-Luc Chabert (cf. [12]) montre que M_n est le dénominateur commun des coefficients de tous les polynômes de $\mathbb{Q}[x]$ à valeurs entières sur l'ensemble des nombres premiers $\mathbb{P}$. En 2007, Jean-Luc Chabert (cf.[13]) montre que la suite $\left((D_n)_{n\geqslant 0}\right)$ répertoriée A075265 dans [66], qui est la suite des dénominateurs communs des coefficients des polynômes $(A_n(x))_{\geqslant 0}$ définis par

$$\left(-\frac{\ln(1-z)}{z}\right)^x = \sum_{n\geqslant 0} A_n(x) z^n,$$

vérifie, pour tout $n \geqslant 0$, $D_n = M_{n+1}$. Chabert (cf.[13]) a retrouvé le résultat démontré précédement par Adelberg (cf.[3]). En effet, grâce à l'égalité (2.8) et à la proposition 2.12, on peut encore montrer que pour $n \geqslant 0$, on a :

$$(-1)^n n! x A_n(x-n) = (x-n) B_n^{(x)}.$$

2.7 Factorisation partielle des polynômes de Nörlund et de Stirling

Proposition 2.19 (cf.[7]). *Il existe une suite $(P_n)_{n\geqslant 2}$ de polynômes primitifs de $\mathbb{Z}[x]$ telle que pour $n \geqslant 1$, on a*

$$B_{2n}^{(x)} = \frac{1}{d_{2n}} x P_{2n}(x), \tag{2.31}$$

$$B_{2n+1}^{(x)} = \frac{1}{d_{2n+1}} x^2 (x-1) P_{2n+1}(x). \tag{2.32}$$

où pour tout $n \geqslant 0$,

$$d_n = \frac{1}{n!} \prod_{p\in\mathbb{P}} p^{\left\lfloor \frac{n}{(p-1)} \right\rfloor + \left\lfloor \frac{n}{p(p-1)} \right\rfloor + \left\lfloor \frac{n}{p^2(p-1)} \right\rfloor + \cdots}.$$

Démonstration. Soit $n \geqslant 1$. D'après le théorème 2.16, $d_n B_n^{(x)}$ est un polynôme primitif de $\mathbb{Z}[x]$, où, d'après la proposition 2.17,

$$d_n = \frac{1}{n!} \prod_{p\in\mathbb{P}} p^{\left\lfloor \frac{n}{(p-1)} \right\rfloor + \left\lfloor \frac{n}{p(p-1)} \right\rfloor + \left\lfloor \frac{n}{p^2(p-1)} \right\rfloor + \cdots}.$$

D'une part on sait, d'après la proposition 2.14, que pour tout $n \geqslant 1$, $B_{2n}^{(x)}$ est divisible par x et $B_{2n+1}^{(x)}$ est divisible par x^2. D'autre part, d'après la définition des polynômes de Nörlund (voir relation (2.20)), $B_n^{(1)} = B_n$. Par suite, pour tout $n \geqslant 1$,

$$B_{2n+1}^{(1)} = B_{2n+1} = 0.$$

Il en résulte que le polynôme primitif $d_n B_n^{(x)}$ est divisible dans $\mathbb{Z}[x]$ par le polynôme primitif $x(x(x-1))^{\bmod (n,2)}$ pour $n \geqslant 2$, où $\bmod(n,2)$ désigne le reste de la division euclidienne de l'entier n par 2. Le quotient $P_n(x)$ de ces deux polynômes est donc aussi un polynôme primitif de $\mathbb{Z}[x]$. Par conséquent, il existe une suite $(P_n(x))_{n\geqslant 2}$ de polynômes primitifs de $\mathbb{Z}[x]$ telle que pour tout $n \geqslant 2$,

$$d_n B_n^{(x)} = x(x(x-1))^{\bmod (n,2)} P_n(x). \tag{2.33}$$

□

Grâce à cette proposition, on peut déduire une factorisation partielle des polynômes de Stirling.

Proposition 2.20. *Pour tout $n \geqslant 2$,*

$$T_n(x) = \frac{n+1}{d_n} \binom{x}{n+1} (x(x-1))^{\bmod (n,2)} P_n(x),$$

où $(P_n)_{n\geqslant 0}$ est la suite des polynômes primitifs de $\mathbb{Z}[x]$ définie dans la proposition 2.19 et pour tout $n \geqslant 0$

$$d_n = \frac{1}{n!} \prod_{p\in\mathbb{P}} p^{\left\lfloor \frac{n}{(p-1)} \right\rfloor + \left\lfloor \frac{n}{p(p-1)} \right\rfloor + \left\lfloor \frac{n}{p^2(p-1)} \right\rfloor + \cdots}.$$

Démonstration. On rappelle, d'après la proposition 2.12, que pour tout $n \geqslant 2$,

$$T_n(x) = \binom{x-1}{n} B_n^{(x)}.$$

En multipliant les deux membres de la relation (2.33) par $\frac{1}{d_n}\binom{x-1}{n}$, on obtient :

$$T_n(x) = \frac{1}{d_n}\binom{x-1}{n} x(x(x-1))^{\bmod (n,2)} P_n(x),$$

autrement dit,

$$T_n(x) = \frac{n+1}{d_n}\binom{x}{n+1} (x(x-1))^{\bmod (n,2)} P_n(x).$$

□

En 1960, (cf. [49]) D. S. Mitrinović et R. S. Mitrinović ont déterminé une factorisation partielle des polynômes de Stirling $T_n(x)$ pour $n \in \{2, \ldots, 13\}$,

$$\begin{aligned}
T_2(x) &= \tfrac{1}{4}\binom{x}{3} P_2(x), & T_3(x) &= \tfrac{1}{2}\binom{x}{4} x(x-1) P_3(x),\\
T_4(x) &= \tfrac{1}{48}\binom{x}{5} P_4(x), & T_5(x) &= \tfrac{1}{16}\binom{x}{6} x(x-1) P_5(x),\\
T_6(x) &= \tfrac{1}{576}\binom{x}{7} P_6(x), & T_7(x) &= \tfrac{1}{144}\binom{x}{8} x(x-1) P_7(x),\\
T_8(x) &= \tfrac{1}{3840}\binom{x}{9} P_8(x), & T_9(x) &= \tfrac{1}{768}\binom{x}{10} x(x-1) P_9(x),\\
T_{10}(x) &= \tfrac{1}{9216}\binom{x}{11} P_{10}(x), & T_{11}(x) &= \tfrac{1}{1536}\binom{x}{12} x(x-1) P_{11}(x),\\
T_{12}(x) &= \tfrac{1}{3870\,720}\binom{x}{13} P_{12}(x), & T_{13}(x) &= \tfrac{1}{552\,960}\binom{x}{14} x(x-1) P_{13}(x),
\end{aligned}$$

et calculé, pour $2 \leqslant n \leqslant 13$, les expressions des polynômes $P_n(x)$:

$$\begin{aligned}
P_2(x) &= 3x - 1,\\
P_3(x) &= -1,\\
P_4(x) &= 15x^3 - 30x^2 + 5x + 2,\\
P_5(x) &= -3x^2 + 7x + 2,\\
P_6(x) &= 63x^5 - 315x^4 + 315x^3 + 91x^2 - 42x - 16,\\
P_7(x) &= -9x^4 + 54x^3 - 51x^2 - 58x - 16,\\
P_8(x) &= 135x^7 - 1260x^6 + 3150x^5 - 840x^4 - 2345x^3 - 540x^2 + 404x + 144,\\
P_9(x) &= -15x^6 + 165x^5 - 465x^4 - 17x^3 + 648x^2 + 548x + 144,
\end{aligned}$$

$$\begin{aligned}
P_{10}(x) &= 99x^9 - 1485x^8 + 6930x^7 - 8778x^6 - 8085x^5 + 8195x\\
&\quad +11\,792x^3 + 2068x^2 - 2288x - 768,\\
P_{11}(x) &= -9x^8 + 156x^7 - 834x^6 + 1080x^5 + 1927x^4 - 1252x^3\\
&\quad -4156x^2 - 3056x - 768,\\
P_{12}(x) &= 12\,285x^{11} - 270\,270x^{10} + 2027\,025x^9 - 5495\,490x^8\\
&\quad +315\,315x^7 + 12\,882\,870x^6 + 5760\,755x^5 - 14\,444\,430x^4\\
&\quad -15\,875\,860x^3 - 2037\,672x^2 + 3327\,584x + 1061\,376,\\
P_{13}(x) &= -945x^{10} + 23\,625x^9 - 201\,600x^8 + 609\,210x^7 + 113\,715x^6\\
&\quad -2207\,175x^5 - 1817\,786x^4 + 3161\,188x^3 + 6544\,568x^2\\
&\quad +4388\,960x + 1061\,376.
\end{aligned}$$

Ils ont remarqué que pour $k \in \{1, 2, 3, 4, 5, 6\}$, les polynômes $P_{2k}(x)$ et $P_{2k+1}(x)$ ont le même terme constant, autrement dit,

$$P_{2k}(0) = P_{2k+1}(0).$$

Ils ont alors proposé ([49], p. 4) le problème d'examiner si ces relations avaient encore lieu en général

pour tout $k \geqslant 1$. Le théorème suivant apporte donc une réponse positive à ce problème.

Théorème 2.21 ([7]). *Il existe une suite $(P_n)_{n\geqslant 2}$ de polynômes primitifs de $\mathbb{Z}[x]$ et une suite d'entiers $(m_n)_{n\geqslant 1}$ telles que pour $n \geqslant 1$, on a*

$$T_{2n}(x) = \frac{1}{m_{2n}}\binom{x}{2n+1}P_{2n}(x),$$
$$T_{2n+1}(x) = \frac{1}{m_{2n+1}}\binom{x}{2n+2}x\,(x-1)\,P_{2n+1}(x),$$

où pour tout $n \geqslant 1$,

$$m_n = \frac{1}{(n+1)!}\prod_{p\in\mathbb{P}} p^{\left\lfloor \frac{n}{p-1}\right\rfloor+\left\lfloor \frac{n}{p(p-1)}\right\rfloor+\left\lfloor \frac{n}{p^2(p-1)}\right\rfloor+\cdots}.$$

De plus, on a :

$$P_{2n}\,(0) = P_{2n+1}(0). \tag{2.34}$$

Démonstration. Soit $n \geqslant 1$, posons $m_n = \frac{d_n}{n+1}$ où $(d_n)_{n\geqslant 0}$ est la suite d'entiers définie dans le théorème 2.16 par

$$d_n = \frac{1}{n!}\prod_{p\in\mathbb{P}} p^{\left\lfloor \frac{n}{(p-1)}\right\rfloor+\left\lfloor \frac{n}{p(p-1)}\right\rfloor+\left\lfloor \frac{n}{p^2(p-1)}\right\rfloor+\cdots}.$$

D'après la proposition 2.20,

$$T_n(x) = \frac{1}{m_n}\binom{x}{n+1}(x(x-1))^{\bmod (n,2)}P_n(x).$$

Montrons que pour tout $n \geqslant 0$, m_n est un entier ; pour cela il suffit de montrer que pour tout nombre premier p, $v_p\,(m_n) \geqslant 0$. On a

$$v_p\,(m_n) = \sum_{k\geqslant 0}\left\lfloor \frac{n}{p^k\,(p-1)}\right\rfloor - v_p\,(n!)\,.$$

En utilisant la formule de Legendre (voir relation (2.29)), on obtient

$$\begin{aligned} v_p\,(m_n) &= \sum_{k\geqslant 0}\left\lfloor \frac{n}{p^k\,(p-1)}\right\rfloor - \sum_{k\geqslant 1}\left\lfloor \frac{n}{p^k}\right\rfloor \\ &= \sum_{k\geqslant 0}\left(\left\lfloor \frac{n}{p^k(p-1)}\right\rfloor - \left\lfloor \frac{n+1}{p^{k+1}}\right\rfloor\right). \end{aligned}$$

Montrons que cette somme est à termes positifs. Autrement dit, montrons que pour tout nombre premier $p \leqslant n+1$ et pour tout $k \geqslant 0$,

$$\left\lfloor \frac{n}{p^k(p-1)}\right\rfloor - \left\lfloor \frac{n+1}{p^{k+1}}\right\rfloor \geqslant 0.$$

Pour tout nombre premier $p \leqslant n+1$ et pour tout entier $k \geqslant 0$, on a

$$\frac{n}{p^k(p-1)} - \frac{n+1}{p^{k+1}} = \frac{n+1-p}{p^{k+1}(p-1)} \geqslant 0,$$

et par conséquent,

$$\left\lfloor \frac{n}{p^k(p-1)}\right\rfloor - \left\lfloor \frac{n+1}{p^{k+1}}\right\rfloor \geqslant 0.$$

Il en résulte que m_n est un entier. Ce résultat peut aussi être obtenu comme conséquence direct de ([8, Lemma 13]).

Reste à montrer que pour tout $n \geqslant 1$,

$$P_{2n}(0) = P_{2n+1}(0).$$

D'après la proposition 2.19,

$$B_{2n}^{(x)} = \frac{1}{d_{2n}} x P_{2n}(x)$$
$$B_{2n+1}^{(x)} = \frac{1}{d_{2n+1}} x^2 (x-1) P_{2n+1}(x).$$

On en déduit que

$$P_{2n}(0) = [x](d_{2n} B_{2n}^{(x)}), \quad P_{2n+1}(0) = [x^2](-d_{2n+1} B_{2n+1}^{(x)}).$$

À la lumière du lemme 2.13, ces deux dernières relations deviennent

$$P_{2n}(0) = -d_{2n} \frac{B_{2n}}{2n}, \quad P_{2n+1}(0) = -\frac{(2n+1)}{2} d_{2n+1} \frac{B_{2n}}{2n}. \tag{2.35}$$

Montrons que pour tout $n \geqslant 1$,

$$d_{2n} = \frac{2n+1}{2} d_{2n+1}.$$

On a d'après la proposition 2.17,

$$d_{2n} = \frac{1}{(2n)!} \prod_{p \in \mathbb{P}} p^{\sum_{k \geqslant 0} \left\lfloor \frac{2n}{p^k(p-1)} \right\rfloor} \quad \text{et} \quad d_{2n+1} = \frac{1}{(2n+1)!} \prod_{p \in \mathbb{P}} p^{\sum_{k \geqslant 0} \left\lfloor \frac{2n+1}{p^k(p-1)} \right\rfloor}.$$

Par suite,

$$\frac{(2n+1)d_{2n+1}}{2d_{2n}} = \frac{1}{2} \prod_{p \in \mathbb{P}} p^{\sum_{k \geqslant 0} \left\lfloor \frac{2n+1}{p^k(p-1)} \right\rfloor - \left\lfloor \frac{2n}{p^k(p-1)} \right\rfloor}.$$

On en déduit que pour tout nombre premier p,

$$v_p\left(\frac{(2n+1)d_{2n+1}}{2d_{2n}}\right) = -v_p(2) + \sum_{k \geqslant 0} \left(\left\lfloor \frac{2n+1}{p^k(p-1)} \right\rfloor - \left\lfloor \frac{2n}{p^k(p-1)} \right\rfloor \right).$$

Il n'est pas difficile de voir que pour tous entiers naturels non nuls x et y :

$$\left\lfloor \frac{x+1}{y} \right\rfloor - \left\lfloor \frac{x}{y} \right\rfloor = \begin{cases} 1 \text{ si } y \text{ divise } x+1, \\ 0 \text{ sinon.} \end{cases}$$

Il en résulte que si $p \geqslant 3$, $p^k(p-1)$ est alors un entier pair et il ne peut donc pas diviser $2n+1$, par conséquent,

$$v_p\left(\frac{(2n+1)d_{2n+1}}{2d_{2n}}\right) = 0.$$

Si $p = 2$, on a

$$v_2\left(\frac{(2n+1)d_{2n+1}}{2d_{2n}}\right) = -1 + \sum_{k\geqslant 0}\left(\left\lfloor\frac{2n+1}{2^k}\right\rfloor - \left\lfloor\frac{2n}{2^k}\right\rfloor\right)$$
$$= \sum_{k\geqslant 1}\left(\left\lfloor\frac{2n+1}{2^k}\right\rfloor - \left\lfloor\frac{2n}{2^k}\right\rfloor\right) = 0.$$

Par suite, on a pour tout nombre premier p,

$$v_p\left(\frac{(2n+1)d_{2n+1}}{2d_{2n}}\right) = 0,$$

ce qui équivaut à affirmer que

$$\frac{(2n+1)d_{2n+1}}{2d_{2n}} = 1.$$

Autrement dit,

$$d_{2n} = \frac{2n+1}{2}d_{2n+1}.$$

On en déduit $P_{2k+1}(0) = P_{2k}(0)$, ce qui établit la relation (2.34). La démonstration du théorème est terminée. □

Chapitre 3

Nombre de solutions d'une équation de Cassels

3.1 Introduction

Au XIX^{e} siècle, plusieurs auteurs se sont intéressés à la résolution de l'équation diophantienne

$$x^3 + y^3 + z^3 = u^2. \tag{3.1}$$

Parmi eux, on pourra citer V. Bouniakowsky [9] qui donna, en 1853, l'identité

$$(3\lambda)^3 + (2 - \lambda^3)^3 + (\lambda^3 + 1)^3 = \left(3(\lambda^3 + 1)\right)^2, \tag{3.2}$$

ce qui a fourni une infinité de solutions de l'équation (3.1). En 1866 E. Catalan donna une autre famille de solutions de l'équation (3.1). Il prouva l'identité suivante :

$$\left(a^4 + 2ab^3\right)^3 + \left(b^4 + 2a^3b\right)^3 + \left(3a^2b^2\right)^3 = \left(7a^3b^3 + a^6 + b^6\right)^2. \tag{3.3}$$

Pour plus de complément sur l'historique de l'équation (3.1), on pourra consulter le livre de Leonard Dickson [23, p. 566], "History of the theory of numbers. Vol. II : Diophantine analysis". Les identités (3.2) et (3.3) fournissent une infinité de solutions de l'équation (3.1), mais pas toutes les solutions. En 1916, A. Gérardin [31] a dressé un tableau, malheureusement encore non exhaustif, de solutions de l'équation (3.1). En 1985, Cassels [11] s'est intéressé à cette même équation diophantienne (3.1) dans le cas particulier où x, y et z sont trois nombres entiers consécutifs. Dans [11], Cassels écrit qu'il a relevé le défi de déterminer dans quels cas la somme de trois cubes consécutifs est un carré ; autrement dit, cela revient à déterminer toutes les solutions de l'équation diophantienne

$$(x-1)^3 + x^3 + (x+1)^3 = y^2, \quad (x, y) \in \mathbb{N}^*.$$

Cassels réduit le problème à la détermination des points entiers de la courbe elliptique d'équation

$$y^2 = 3x(x^2 + 2).$$

En utilisant l'arithmétique de certains corps quartiques, il montre que les seuls points entiers de la courbe elliptique précédente sont :

$$\{(0,0),(1,3),(1,-3),(2,6),(2,-6),(24,204),(24,-204)\}.$$

En utilisant des résultats classiques de Ljunggren [44] et leur généralisation, (voir [4, 16, 78, 80]), Luca et Walsh [45] ont étudié l'équation diophantienne

$$y^2 = nx(x^2+2),$$

où n est un entier strictement supérieur à 1. En désignant par $\omega(n)$ le nombre de facteurs premiers distincts de n, ces derniers ont prouvé que l'équation diophantienne précédente possède au plus $3 \cdot 2^{\omega(n)} - 1$ solutions en entiers strictement positifs. En 2010 [18], L. Chen a considéré le cas où n est un nombre premier impair et il a montré que l'équation diophantienne

$$y^2 = nx(x^2+2)$$

possède au plus deux solutions en entiers strictement positifs. Récemment, en 2014, Alain Togbé [69] a considéré une forme encore plus générale ; l'équation diophantienne :

$$y^2 = px(Ax^2+2), \tag{3.4}$$

où p est un nombre premier et $A > 1$ un entier impair. Il prouve que pour tout nombre premier p et tout entier positif impair $A > 1$, l'équation diophantienne (3.4) possède au plus 7 solutions en entiers strictement positifs.

En utilisant des résultats obtenus à l'aide du logiciel MAGMA, A. Togbé énonce la conjecture suivante sur la majoration du nombre de solutions de l'équation (3.4).

Conjecture 3.1 ([69])**.** *Soient p un nombre premier impair et A un entier impair supérieur à 2. Alors :*

1. *Si $(A,p) \equiv (1,1)$, $(1,5)$, $(1,7)$, $(3,1)$, $(3,3)$, $(3,7)$, $(5,1)$, $(5,5)$, $(5,7)$, $(7,3)$, ou $(7,5)$ (mod 8), alors l'équation diophantienne (3.4) possède au plus une solution en entiers strictement positifs.*
2. *Si $(A,p) \equiv (1,3)$ ou $(7,1)$ (mod 8), alors l'équation diophantienne (3.4) possède au plus deux solutions en entiers strictement positifs.*
3. *Si $(A,p) \equiv (3,5)$ ou $(7,7)$ (mod 8), alors l'équation diophantienne (3.4) possède au plus trois solutions en entiers strictement positifs.*

Dans ce chapitre on améliore la majoration du nombre de solutions de l'équation diophantienne (3.4) donnée par A. Togbé [69], ce qui nous permettra de prouver une partie de la Conjecture 3.1. Pour cela, nous avons besoin d'établir des résultats concernant quelques types d'équations diophantiennes quadratiques et quartiques.

3.2 Etude des équations $x^2 - dy^2 = 1$ et $x^2 - dy^4 = 1$

Une équation de Pell-Fermat est une équation diophantienne de la forme

$$x^2 - dy^2 = \pm 1, \tag{3.5}$$

où $d \neq \square$ est un entier strictement positif. Résoudre l'équation diophantienne (3.5) revient à expliciter les éléments du groupe des unités de l'anneau $\mathbb{Z}[\sqrt{d}]$. On note indifféremment (x, y) où $x + y\sqrt{d}$ une solution de l'équation (3.5). On remarque que si $(x, y) \in \mathbb{Z}^2$ est solution de l'équation (3.5) alors $(\pm x, \pm y)$ est aussi solution de l'équation (3.5). De plus si $x > 0$ et $y > 0$ alors $x + y\sqrt{d} > 1$ et $-x - y\sqrt{d} < -1$ et par conséquent leurs inverses $x - y\sqrt{d}$ et $-x + y\sqrt{d} \in]-1, 1[$. Résoudre donc l'équation de Pell-Fermat (3.5) revient à déterminer l'ensemble de ses solutions en entiers strictement positifs. Posons alors :

$$G = \left\{ x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]; \quad x^2 - dy^2 = \pm 1 \right\}$$
$$G_+ = \left\{ x + y\sqrt{d} \in G; \ x > 0 \text{ et } y > 0 \right\}$$

Si $x + y\sqrt{d}$ et $x' + y'\sqrt{d}$ sont deux éléments de G_+ alors on a l'équivalence suivante :

$$x \leqslant x' \Longleftrightarrow y \leqslant y' \Longleftrightarrow x + y\sqrt{d} \leqslant x' + y'\sqrt{d}.$$

Ainsi G_+ est totalement ordonné. Il possède un plus petit élément qui correspond à la solution, en entiers strictement positifs, minimale de l'équation (3.5). Et on a le résultat suivant.

Théorème 3.2. *Soit* $\varepsilon = \min G_+$, *alors*

$$G_+ = \{\varepsilon^n; \quad n \in \mathbb{N}^*\}$$

Démonstration. Soit $\gamma = x + y\sqrt{d} \in G_+$. La suite $(\varepsilon^n)_{n \geqslant 1}$ étant strictement croissante, il existe alors $n \geqslant 1$ tel que $\varepsilon^n \leqslant \gamma < \varepsilon^{n+1}$. Les deux nombres γ et ε sont tous deux des unités de $\mathbb{Z}[\sqrt{d}]$, par conséquent $\gamma\varepsilon^{-n}$ est aussi une unité de $\mathbb{Z}[\sqrt{d}]$. Comme $1 \leqslant \gamma\varepsilon^{-n} < \varepsilon$, alors $\gamma\varepsilon^{-n} \notin G_+$, autrement dit, $\gamma\varepsilon^{-n} = 1$. Par conséquent $\gamma = \varepsilon^n$. □

Le nombre ε s'appelle l'unité fondamentale de l'anneau $\mathbb{Z}[\sqrt{d}]$ ou la solution fondamentale de l'équation $x^2 - dy^2 = \pm 1$.

La principale méthode qui permet la détermination de la solution fondamentale ε repose sur le développement en fraction continue de $\sqrt{d}$. Rappelons brièvement la notion de fraction continue. Étant donné un nombre réel irrationnel x, considérons les suites $(a_n)_{n \geqslant 0}$, $(x_n)_{n \geqslant 0}$ définies par $x_0 = x$, $a_n = \lfloor x_n \rfloor$ et pour tout $n \geqslant 0$,

$$x_n = a_n + \frac{1}{x_{n+1}}.$$

Il s'en suit que :

$$x = x_0 = a_0 + \frac{1}{x_1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{x_2}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{x_3}}}.$$

De manière plus générale, on a pour tout $n \geqslant 0$,

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n + \cfrac{1}{x_{n+1}}}}}}}.$$

Cette expression s'appelle une fraction continue. Elle est souvent notée

$$[a_0; a_1, a_2, \ldots, a_n, x_{n+1}].$$

Pour tout $n \geqslant 0$, le nombre rationnel

$$\frac{p_n}{q_n} = [a_0; a_1, a_2, \ldots, a_n]$$

s'appelle la réduite de x de rang n. La suite $\left(\frac{p_n}{q_n}\right)_{n\geqslant 0}$ est convergente vers x et elle vérifie [40, Theorem 9, p.9]

$$\left|\frac{p_n}{q_n} - x\right| \leqslant \frac{1}{q_n^2}.$$

Autrement dit,

$$x = \lim_{n \longrightarrow +\infty} [a_0; a_1, \ldots, a_n].$$

On écrit alors

$$x = [a_0; a_1, a_2, \ldots, a_n, a_{n+1}, \ldots].$$

C'est le développement en fraction continue de x.

Une fraction continue $[a_0; a_1, a_2, \ldots, a_n, a_{n+1}, \ldots]$ est dite périodique s'il existe des entiers $k \geqslant 0$ et $m > 0$ tel que pour tout entier $n \geqslant k$, $a_{n+m} = a_n$. Comme dans le cas du développement décimal, une fraction continue $[a_0; a_1, a_2, \ldots, a_n, a_{n+1}, \ldots]$ périodique sera notée

$$[a_0; a_1, a_2, \ldots, a_{k-1}, \overline{a_k, a_{k+1}, \ldots a_{k+m}}].$$

Théorème 3.3 ([40, Theorem 28, p.48])**.** *Le développement en fraction continue d'un nombre réel x est périodique si, et seulement si, le nombre x est un nombre irrationnel quadratique.*

Plus précisément, [77, Remark 1.3.4, p. 60] si $d \neq \square$ alors le développement en fraction continue de $\sqrt{d}$ est de la forme :

$$\sqrt{d} = [a_0; \overline{a_1, a_2, \ldots, a_{m-1}, 2a_0}].$$

Exemple 3.4. *Soit $d = 5$. Calculons les premiers termes des suites $(a_n)_{n\geqslant 0}$ et $(x_n)_{n\geqslant 0}$*

$$\begin{aligned}
x_0 &= \sqrt{5} \quad \text{et} \quad a_0 = \left\lfloor \sqrt{5} \right\rfloor = 2,\\
x_1 &= \frac{1}{x_0 - a_0} = \frac{1}{\sqrt{5} - 2} = \sqrt{5} + 2 \quad \text{et} \quad a_1 = \lfloor x_1 \rfloor = 4,\\
x_2 &= \frac{1}{x_1 - a_1} = \frac{1}{\sqrt{5} - 2} = x_1 \quad \text{et} \quad a_2 = \lfloor x_2 \rfloor = a_1.
\end{aligned}$$

On en déduit que pour tout $n \geqslant 1$, $x_n = x_1$ et $a_n = a_1$. On obtient ainsi

$$\sqrt{5} = [2, \overline{4}].$$

Le théorème suivant donne la valeur de la solution fondamentale de l'équation de Pell-Fermat (3.5) en fonction de la parité de la période m du développement en fraction continue de $\sqrt{d}$.

Théorème 3.5 ([77]). *Soient $d \neq \square$ un entier strictement positif et m la période du développement en fraction continue de $\sqrt{d} = [a_0; \overline{a_1, a_2, \ldots, a_{m-1}, a_m}]$ et*

$$\frac{p_{m-1}}{q_{m-1}} = [a_0; a_1, a_2, \ldots, a_{m-1}] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \cfrac{1}{a_{m-2} + \cfrac{1}{a_{m-1}}}}}},$$

alors la solution fondamentale ε de l'équation $x^2 - dy^2 = \pm 1$ est donnée par

$$\varepsilon = p_{m-1} + q_{m-1}\sqrt{d}.$$

De plus

1. *Si m est pair alors*
   $\pm\left(p_{m-1} \pm q_{m-1}\sqrt{d}\right)^n$, pour $n \in \mathbb{N}$, sont les solutions de l'équation $x^2 - dy^2 = 1$.
   L'équation $x^2 - dy^2 = -1$ ne possède pas de solutions.
2. *Si m est impair alors*
   $\pm\left(p_{m-1} \pm q_{m-1}\sqrt{d}\right)^{2n}$, pour $n \in \mathbb{N}$, sont les solutions de l'équation $x^2 - dy^2 = 1$.
   $\pm\left(p_{m-1} \pm q_{m-1}\sqrt{d}\right)^{2n+1}$, pour $n \in \mathbb{N}$, sont les solutions de l'équation $x^2 - dy^2 = -1$.

Exemple 3.6. *Résolution de l'équation diophantienne*

$$x^2 - 23y^2 = 1 \tag{3.6}$$

Le développement en fraction continue de $\sqrt{23}$ est donné par $\sqrt{23} = [4, \overline{1, 3, 1, 8}]$. Le développement est périodique de période $m = 4$. Soit $\frac{p_3}{q_3}$ la troisième réduite de $\sqrt{23}$.

$$\frac{p_3}{q_3} = [4; 1, 3, 1] = 4 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1}}} = \frac{24}{5}.$$

Pour $n \in \mathbb{N}$, $\pm\left(24 \pm 5\sqrt{23}\right)^n$ sont les solutions de l'équation (3.6). L'équation $x^2 - 23y^2 = -1$ ne possède pas de solutions.

Soit $D \neq \square$ un entier strictement positif et soit $\varepsilon = T_1 + U_1\sqrt{D}$ la solution fondamentale de l'équation de Pell-Fermat $x^2 - dy^2 = 1$. On pose $\varepsilon^k = T_k + U_k\sqrt{D}$ pour $k \geqslant 1$. En 2005, Togbé, Voutier, et Walsh ont démontré le résultat suivant dans [70].

Théorème 3.7 (cf. [70]). *Soit $D \neq \square$ un entier strictement positif. Alors il existe au plus deux solutions en entiers strictement positifs (X, Y) de l'équation $X^2 - DY^4 = 1$. Plus précisément :*

1. *Si l'équation $X^2 - DY^4 = 1$ possède deux solutions en entiers strictement positifs (X_1, Y_1) et (X_2, Y_2) avec $Y_1 < Y_2$, alors ${Y_1}^2 = U_1$ et ${Y_2}^2 = U_2$, sauf si $D = 1785$ ou $D = 16 \cdot 1785$, et dans ces deux cas : ${Y_1}^2 = U_1$ mais ${Y_2}^2 = U_4$.*
2. *Si l'équation $X^2 - DY^4 = 1$ possède seulement une solution en entiers strictement positifs (X, Y), alors $Y^2 = U_\ell$, où ℓ est le plus grand diviseur sans facteur carré de U_1, et on a $\ell = 1$ ou 2 ou p pour un certain nombre premier $p \equiv 3 \pmod 4$.*

Le corollaire suivant apporte encore plus de précision au théorème précédent dans le cas où D est pair.

Corollaire 3.8 ([29]). *Soit $D \neq \square$ un entier strictement positif. Supposons que $D = 2d$ où d est un entier différent de $8 \cdot 1785$. Alors l'équation $X^2 - DY^4 = 1$ possède au plus une solution en entiers strictement positifs (X, Y).*

Démonstration. Supposons que l'équation $X^2 - DY^4 = 1$ possède deux solutions en entiers strictement positifs (X_1, Y_1) et (X_2, Y_2) avec $Y_1 < Y_2$. Alors d'après le théorème 3.7

$$ {Y_1}^2 = U_1,\ {Y_2}^2 = U_2,\ \text{et } U_2 = 2T_1U_1. $$

Par suite,

$$ {Y_2}^2 = 2T_1{Y_1}^2. $$

En notant ν_2 la valuation 2-adique, on en déduit que

$$ 2\nu_2(Y_2) = 1 + \nu_2(T_1) + 2\nu_2(Y_1). \tag{3.7} $$

Puisque $\varepsilon = T_1 + U_1\sqrt{D}$ est de norme 1 dans $\mathbb{Z}[\sqrt{D}]$ et $D = 2d$, alors ${T_1}^2 - 2d{U_1}^2 = 1$. Par suite, T_1 est impair. Autrement dit $\nu_2(T_1) = 0$. Ce qui contredit la relation (3.7). □

Exemple 3.9. *Considérons l'équation diophantienne*

$$ X^2 - 5Y^4 = 1. $$

Commençons par déterminer la solution fondamentale de l'équation

$$ x^2 - 5y^2 = 1. $$

Puisque $\sqrt{5}$ possède le développement en fraction continue périodique suivant :

$$ \sqrt{5} = [2, \overline{4}]. $$

Alors d'après le théorème 3.5, la solution fondamentale $\varepsilon = T_1 + U_1\sqrt{5}$ de l'équation $x^2 - 5y^2 = 1$ est donnée par $T_1 + U_1\sqrt{5} = \left(2 + \sqrt{5}\right)^2 = 9 + 4\sqrt{5}$. $\varepsilon^2 = T_2 + U_2\sqrt{5} = 161 + 72\sqrt{5}$. Puisque $U_1 = 4$ est un carré alors $U_2 = 72$ n'est pas un carré, alors d'après le théorème 3.7 l'unique solution en entiers strictement positifs de l'équation $X^2 - 5Y^4 = 1$ est $(9, 2)$.

3.3 Etude de l'équation diophantienne $ax^2 - by^2 = 1$

Soient $a, b \in \mathbb{N}^* \setminus \{1\}$. Supposons que l'équation

$$ax^2 - by^2 = 1 \tag{3.8}$$

possède au moins une solution en entiers strictement positifs, alors d'après le théorème de Bézout, $\text{pgcd}(a, b) = 1$ et $ab \neq \square$. On supposera donc dans toute la suite de cette section que $\text{pgcd}(a, b) = 1$ et $ab \neq \square$.

À chaque solution (x, y), on associe $z = z(x, y) = x\sqrt{a} + y\sqrt{b} \in \mathbb{Z}\sqrt{a} + \mathbb{Z}\sqrt{b}$. Posons

$$M = \mathbb{Z}\sqrt{a} + \mathbb{Z}\sqrt{b} = \left\{ x\sqrt{a} + y\sqrt{b};\ x, y \in \mathbb{Z} \right\}.$$

Comme $\text{pgcd}(a, b) = 1$ alors M est le $\mathbb{Z}$-module libre engendré par $\left\{\sqrt{a}, \sqrt{b}\right\}$. Soit $\mathcal{N}$ l'application norme définie par :

$$\begin{aligned} \mathcal{N} : M &\longrightarrow \mathbb{Z} \\ z = x\sqrt{a} + y\sqrt{b} &\longmapsto \left(x\sqrt{a} + y\sqrt{b}\right)\left(x\sqrt{a} - y\sqrt{b}\right). \end{aligned}$$

Alors (x, y) est une solution de l'équation $ax^2 - by^2 = 1$ si et seulement si $z \in M$ et $\mathcal{N}(z) = 1$. Il est clair que si (x, y) est une solution, alors $(\pm x, \pm y)$ est aussi solution. Intéressons-nous donc aux solutions en entiers strictement positifs de l'équation (3.8). Posons alors

$$\begin{aligned} S &= \{z \in M; \quad \mathcal{N}(z) = 1\} \\ S_+ &= \left\{ z = x\sqrt{a} + y\sqrt{b} \in S; \quad x > 0 \text{ et } y > 0 \right\}. \end{aligned}$$

Si $x\sqrt{a} + y\sqrt{b}$ et $x'\sqrt{a} + y'\sqrt{b}$ sont deux éléments de S_+ alors on a l'équivalence suivante :

$$x \leqslant x' \Longleftrightarrow y \leqslant y' \Longleftrightarrow x\sqrt{a} + y\sqrt{b} \leqslant x'\sqrt{a} + y'\sqrt{b}.$$

Ainsi S_+ est totalement ordonné. Il possède un plus petit élément qui correspond à la solution, en entiers strictement positifs, minimale de l'équation (3.8). La solution $\alpha = \min S_+$ est appelée solution fondamentale de l'équation (3.8).

Proposition 3.10. *Soient $a, b \in \mathbb{N}^* \setminus \{1\}$. Supposons que l'équation* (3.8) *possède au moins une solution. Soit alors $\alpha = x_1\sqrt{a} + y_1\sqrt{b}$ la solution fondamentale de l'équation* (3.8)*. Alors il existe deux suites d'entiers strictement positifs $(x_n)_{n\geqslant 1}$ et $(y_n)_{n\geqslant 1}$ vérifiant pour tout entier $n \geqslant 1$:*

$$\alpha^{2n-1} = x_{2n-1}\sqrt{a} + y_{2n-1}\sqrt{b}, \tag{3.9}$$

$$\alpha^{2n} = x_{2n} + y_{2n}\sqrt{ab}, \tag{3.10}$$

$$\frac{1}{\alpha^{2n-1}} = x_{2n-1}\sqrt{a} - y_{2n-1}\sqrt{b}, \tag{3.11}$$

$$\frac{1}{\alpha^{2n}} = x_{2n} - y_{2n}\sqrt{ab}, \tag{3.12}$$

$$ax_{2n-1}^2 - by_{2n-1}^2 = 1, \tag{3.13}$$
$$x_{2n}^2 - aby_{2n}^2 = 1. \tag{3.14}$$

Démonstration. Par hypothèse, α est solution de l'équation $ax^2 - by^2 = 1$. Donc $\mathcal{N}(\alpha) = 1$. Par suite, $\frac{1}{\alpha} = x_1\sqrt{a} - y_1\sqrt{b}$. En développant, grâce à la formule du binôme les deux expressions $\left(x_1\sqrt{a} \pm y_1\sqrt{b}\right)^n$, en séparant les cas n pair et n impair, on montre qu'il existe deux suites d'entiers strictement positifs $(x_n)_{n\geqslant 1}$ et $(y_n)_{n\geqslant 1}$ vérifiant pour tout entier $n \geqslant 1$

$$\alpha^{2n-1} = x_{2n-1}\sqrt{a} + y_{2n-1}\sqrt{b}, \quad \alpha^{2n} = x_{2n} + y_{2n}\sqrt{ab},$$
$$\frac{1}{\alpha^{2n-1}} = x_{2n-1}\sqrt{a} - y_{2n-1}\sqrt{b} \quad \frac{1}{\alpha^{2n}} = x_{2n} - y_{2n}\sqrt{ab}.$$

En multipliant les deux équations (3.10) et (3.12) membre à membre, on obtient que pour tout entier $n \geqslant 1$, $x_{2n}^2 - aby_{2n}^2 = 1$. De la même manière, en multipliant les deux équations (3.9) et (3.11), on obtient que pour tout entier $n \geqslant 1$, $ax_{2n-1}^2 - by_{2n-1}^2 = 1$ □

On déduit de la relation (3.13) que les puissances impaires de α sont des solutions de l'équation (3.8), autrement dit

$$\{\alpha^{2n-1}; \quad n \geqslant 1\} \subset S_+.$$

Le théorème suivant montre que la seconde inclusion est aussi vérifiée.

Théorème 3.11. *Soient $a, b \in \mathbb{N}^* \setminus \{1\}$. Supposons que l'équation (3.8) possède au moins une solution. Soit alors $\alpha = x_1\sqrt{a} + y_1\sqrt{b}$ la solution fondamentale de l'équation (3.8). Alors, avec les notations précédentes on a*

$$S_+ = \left\{\alpha^{2n-1}; \quad n \in \mathbb{N}^*\right\}.$$

Démonstration. Soit $\gamma = k\sqrt{a} + \ell\sqrt{b} \in S_+$. Donc $\mathcal{N}(\gamma) = 1$ et $\gamma \geqslant \alpha > 1$. La suite $\left(\alpha^{2n-1}\right)_{n\geqslant 1}$ étant strictement croissante, il existe alors un entier $n \geqslant 1$ tel que :

$$\alpha^{2n-1} \leqslant \gamma < \alpha^{2n+1}.$$

On en déduit que

$$\alpha^{-1} \leqslant \gamma\alpha^{-2n} < \alpha. \tag{3.15}$$

D'après la relation (3.12),

$$\begin{aligned}\gamma\alpha^{-2n} &= \left(k\sqrt{a} + \ell\sqrt{b}\right)\left(x_{2n} - y_{2n}\sqrt{ab}\right) \\ &= \left(kx_{2n} - b\ell y_{2n}\right)\sqrt{a} + \left(\ell x_{2n} - aky_{2n}\right)\sqrt{b} \in M\end{aligned}$$

De plus, d'après la relation (3.14), $\mathcal{N}(\gamma\alpha^{-2n}) = 1$. On en déduit que $\gamma\alpha^{-2n} \in S$. Comme $\alpha = \min S_+$, alors d'après l'inégalité (3.15), $\gamma\alpha^{-2n} \notin S_+$, autrement dit $\alpha^{-1} \leqslant \gamma\alpha^{-2n} \leqslant 1$. Par suite, $1 \leqslant \gamma^{-1}\alpha^{2n} \leqslant \alpha$. Le nombre 1 n'étant pas un élément de S, on conclut que $1 < \gamma^{-1}\alpha^{2n} \leqslant \alpha$. De la minimalité de α, on déduit que $\gamma = \alpha^{2n-1}$. □

Théorème 3.12. *Soient $a, b \in \mathbb{N}^* \setminus \{1\}$. Supposons que l'équation (3.8) possède au moins une solution. Soit alors $\alpha = x_1\sqrt{a} + y_1\sqrt{b}$ la solution fondamentale de l'équation (3.8), alors α^2 est la solution fondamentale de l'équation de Pell-Fermat $X^2 - abY^2 = 1$.*

Démonstration. Soit $\varepsilon = T + U\sqrt{ab}$ la solution fondamentale de l'équation

$$X^2 - abY^2 = 1. \tag{3.16}$$

D'après la proposition 3.10, α^2 est solution de l'équation de Pell-Fermat (3.16). Par conséquent $1 < \varepsilon \leqslant \alpha^2$. Supposons que $\alpha^2 \neq \varepsilon$. Posons alors $\gamma = \varepsilon\alpha^{-1}$. On a $\alpha^{-1} < \gamma < \alpha$, $\mathcal{N}(\gamma) = 1$ et $\gamma = (Tx_1 - Uby_1)\sqrt{a} + (Uax_1 - Ty_1)\sqrt{b} \in M$. La minimalité de α entraîne que $\alpha^{-1} < \gamma \leqslant 1$. D'où $1 \leqslant \gamma^{-1} < \alpha$. En utilisant encore une fois la minimalité de α, on en déduit que nécessairement $\gamma = 1$. Ce qui est absurde vu que $1 \notin S$. □

Exemple 3.13. *Considérons l'équation* $15X^2 - 11Y^2 = 1$, $a = 15$, $b = 11$, $ab = 165$.

– *On commence par la résolution de l'équation* $x^2 - 165y^2 = 1$.
On a

$$\sqrt{165} = [12; \overline{1, 5, 2, 5, 1, 24}].$$

Soit $\frac{p_5}{q_5}$ *la* 5^e *réduite de* $\sqrt{165}$. *Alors*

$$\frac{p_5}{q_5} = [12; 1, 5, 2, 5, 1] = 12 + \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{2 + \cfrac{1}{5 + \cfrac{1}{1}}}}} = \frac{1079}{84}.$$

La solution fondamentale ε *de l'équation* $x^2 - 165y^2 = 1$ *est donc :*

$$\varepsilon = 1079 + 84\sqrt{165}$$

– *La solution fondamentale* $\alpha = x_1\sqrt{15} + y_1\sqrt{11}$ *de l'équation* $15X^2 - 11Y^2 = 1$, *si elle existe, vérifie donc*

$$\alpha^2 = \varepsilon = 1079 + 84\sqrt{165},$$

autrement dit

$$\begin{cases} 15x_1^2 + 11y_1^2 = 1079 \\ 2x_1y_1 = 84. \end{cases} \tag{3.17}$$

En y joignant l'équation $15x_1^2 - 11y_1^2 = 1$, *on obtient le système équivalent suivant*

$$\begin{cases} 15x_1^2 + 11y_1^2 = 1079 \\ 15x_1^2 - 11y_1^2 = 1. \end{cases}$$

On obtient ainsi $x_1 = 6$ *et* $y_1 = 7$. *Autrement dit* $\alpha = 6\sqrt{15} + 7\sqrt{11}$.

Exemple 3.14. *Considérons l'équation*

$$13X^2 - 4Y^4 = 1.$$

Posons $x = X$ *et* $y = Y^2$. *Alors le couple* (x, y) *est solution de l'équation*

$$13x^2 - 4y^2 = 1. \tag{3.18}$$

Soit $\varepsilon = T + U\sqrt{52}$ *la solution fondamentale de l'équation de Pell-Fermat* $t^2 - 52u^2 = 1$. *En développant* $\sqrt{52}$ *en fraction continue, on obtient*

$$\sqrt{52} = [7; \overline{4, 1, 2, 1, 4, 14}].$$

Soit $\frac{p_5}{q_5}$ *la* 5^e *réduite de* $\sqrt{52}$.

$$\frac{p_5}{q_5} = [7; 4, 1, 2, 1, 4] = 7 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{4}}}}} = \frac{649}{90}.$$

Par suite $\varepsilon = 649 + 90\sqrt{52}$. *D'après le théorème 3.12, si l'équation* (3.18) *possède une solution, alors la solution fondamentale* $\alpha = x_1\sqrt{13} + 2y_1$ *vérifie* $\alpha^2 = 649 + 90\sqrt{52}$. *Donc*

$$\begin{cases} 13x_1^2 + 4y_1^2 = 649 \\ 13x_1^2 - 4y_1^2 = 1 \end{cases} \iff \begin{cases} 26x_1^2 = 650 \\ 8y_1^2 = 648 \end{cases} \iff \begin{cases} x_1 = 5 \\ y_1 = 9 \end{cases}$$

$(5, 9)$ *est une solution de l'équation* (3.18). *On conclut que* $(5, 3)$ *est solution de l'équation* $13X^2 - 4Y^4 = 1$.

En 1954, Ljunggren [44] a démontré le résultat suivant.

Théorème 3.15 ([44])**.** *Soit* $a > 1$ *et* b *deux entiers strictement positifs. L'équation*

$$aX^2 - bY^4 = 1.$$

possède au plus une solution en entiers strictement positifs (X, Y).

Grâce à ce théorème on peut affirmer que $(5, 3)$ est l'unique solution en entiers strictement positifs de l'équation $13X^2 - 4Y^4 = 1$.

3.4 Etude des équations $ax^2 - by^2 = 2$ et $ax^2 - by^4 = 2$

Soit a et b deux entiers positifs impairs. Supposons que l'équation

$$ax^2 - by^2 = 2. \tag{3.19}$$

possède au moins une solution en entiers strictement positifs (x, y). Alors $ab \neq \square$ et on a le résultat suivant :

Lemme 3.16. *Soient* a *et* b *deux entiers positifs impairs. Si l'équation* (3.19) *possède une solution en entiers strictement positifs* (x, y) *alors :*

1. x *et* y *sont tous deux impairs.*
2. $\text{pgcd}(a, b) = \text{pgcd}(a, y) = \text{pgcd}(x, b) = \text{pgcd}(x, y) = 1$.

Démonstration. En réduisant l'équation (3.19) modulo 2, on en déduit que x et y sont de même parité. Si l'on suppose que x et y sont tous deux pairs, alors il existe deux entiers x' et y' tels que $x = 2x'$ et $y = 2y'$. Par suite,

$$4ax'^2 - 4by'^2 = 2.$$

D'où $2(ax'^2 - 2by'^2) = 1$, ce qui est absurde. □

On associe à tout $(x, y) \in \mathbb{Z}^2$ le réel $z(x, y)$ défini par

$$z(x, y) = \frac{x\sqrt{a} + y\sqrt{b}}{\sqrt{2}} \in \mathbb{Z}\frac{\sqrt{a}}{\sqrt{2}} + \mathbb{Z}\frac{\sqrt{b}}{\sqrt{2}}.$$

Posons

$$M = \mathbb{Z}\frac{\sqrt{a}}{\sqrt{2}} + \mathbb{Z}\frac{\sqrt{b}}{\sqrt{2}} = \left\{ \frac{x\sqrt{a} + y\sqrt{b}}{\sqrt{2}};\ \ x, y \in \mathbb{Z} \right\}.$$

M est le $\mathbb{Z}$-module libre engendré par $\left\{ \frac{\sqrt{a}}{\sqrt{2}}, \frac{\sqrt{b}}{\sqrt{2}} \right\}$. Soit $\mathcal{N}$ l'application norme définie par :

$$\begin{aligned} \mathcal{N} : M &\longrightarrow \mathbb{Q} \\ \frac{x\sqrt{a} + y\sqrt{b}}{\sqrt{2}} &\longmapsto \left(\frac{x\sqrt{a} + y\sqrt{b}}{\sqrt{2}} \right) \left(\frac{x\sqrt{a} - y\sqrt{b}}{\sqrt{2}} \right). \end{aligned}$$

Alors (x, y) est solution de l'équation (3.19) si et seulement si

$$\mathcal{N}(z(x, y)) = 1.$$

Il est clair que si (x, y) est une solution (3.19), alors $(\pm x, \pm y)$ est aussi solution. Intéressons-nous donc aux solutions en entiers strictement positifs de l'équation (3.19). Posons alors

$$\begin{aligned} S &= \{ z \in M;\quad \mathcal{N}(z) = 1 \}, \\ S_+ &= \left\{ z = \frac{x\sqrt{a} + y\sqrt{b}}{\sqrt{2}} \in S;\quad x > 0 \text{ et } y > 0 \right\}. \end{aligned}$$

Si $\frac{x\sqrt{a} + y\sqrt{b}}{\sqrt{2}}$ et $\frac{x'\sqrt{a} + y'\sqrt{b}}{\sqrt{2}}$ sont deux éléments de S_+ alors on a l'équivalence suivante :

$$x \leqslant x' \Longleftrightarrow y \leqslant y' \Longleftrightarrow \frac{x\sqrt{a} + y\sqrt{b}}{\sqrt{2}} \leqslant \frac{x'\sqrt{a} + y'\sqrt{b}}{\sqrt{2}}.$$

Ainsi S_+ est totalement ordonné. Il possède un plus petit élément qui correspond à la solution, en entiers strictement positifs, minimale de l'équation (3.19). La solution $\alpha = \min S_+$ est appelée solution fondamentale de l'équation (3.19).

Proposition 3.17. *Soient a et b deux entiers positifs impairs. Supposons que l'équation* (3.19) *possède au moins une solution. Soit alors $\alpha = \frac{x_1\sqrt{a} + y_1\sqrt{b}}{\sqrt{2}}$ la solution fondamentale de l'équation* (3.19). *Alors il existe deux suites d'entiers strictement positifs $(x_n)_{n\geqslant 1}$ et $(y_n)_{n\geqslant 1}$ vérifiant pour tout entier*

$n \geqslant 1$:

$$\alpha^{2n-1} = \frac{x_{2n-1}\sqrt{a} + y_{2n-1}\sqrt{b}}{\sqrt{2}}, \tag{3.20}$$

$$\alpha^{2n} = x_{2n} + y_{2n}\sqrt{ab}, \tag{3.21}$$

$$\frac{1}{\alpha^{2n-1}} = \frac{x_{2n-1}\sqrt{a} - y_{2n-1}\sqrt{b}}{\sqrt{2}}, \tag{3.22}$$

$$\frac{1}{\alpha^{2n}} = x_{2n} - y_{2n}\sqrt{ab}. \tag{3.23}$$

$$ax_{2n-1}^2 - by_{2n-1}^2 = 2, \tag{3.24}$$

$$x_{2n}^2 - aby_{2n}^2 = 1. \tag{3.25}$$

Démonstration. Par hypothèse, α est solution de l'équation $ax^2 - by^2 = 2$. Donc

$$\frac{x_1\sqrt{a} + y_1\sqrt{b}}{\sqrt{2}} \frac{x_1\sqrt{a} - y_1\sqrt{b}}{\sqrt{2}} = 1.$$

Par suite,

$$\frac{1}{\alpha} = \frac{x_1\sqrt{a} - y_1\sqrt{b}}{\sqrt{2}}.$$

Un simple raisonnement par récurrence permet de prouver les relations (3.20) à (3.25). □

On déduit de la relation (3.24) que les puissances impaires de α sont des solutions de l'équation (3.19), autrement dit

$$\{\alpha^{2n-1}; \quad n \geqslant 1\} \subset S_+.$$

Le théorème suivant montre que la seconde inclusion est également vérifiée.

Théorème 3.18. *Soient a et b deux entiers positifs impairs. Supposons que l'équation* (3.19) *possède au moins une solution. Soit alors $\alpha = \frac{x_1\sqrt{a} + y_1\sqrt{b}}{\sqrt{2}}$ la solution fondamentale de l'équation* (3.19)*. Alors, avec les notations précédentes on a*

$$S_+ = \{\alpha^{2n-1}; \quad n \in \mathbb{N}^*\}.$$

Démonstration. Soit $\gamma = \frac{k\sqrt{a} + \ell\sqrt{b}}{\sqrt{2}} \in S_+$. Vu que $\alpha > 1$, la suite $(\alpha^n)_{n\geqslant 1}$ est strictement croissante, il existe donc un entier k vérifiant

$$\alpha^{2k-1} \leqslant \gamma < \alpha^{2k+1}.$$

Par suite,

$$\alpha^{-1} \leqslant \alpha^{-2k}\gamma < \alpha$$

D'après la proposition 3.17, $\alpha^{-2k} = x_{2k} - y_{2k}\sqrt{ab}$. D'où

$$\alpha^{-2k}\gamma = \frac{(kx_{2k} - b\ell y_{2k})\sqrt{a} + (\ell x_{2k} - aky_{2k})\sqrt{b}}{\sqrt{2}}.$$

Comme $\mathcal{N}\left(\alpha^{-2k}\gamma\right) = 1$ et $\alpha^{-2k}\gamma < \alpha$, de la minimalité de α on en déduit que

$$\alpha^{-1} \leqslant \alpha^{-2k}\gamma \leqslant 1.$$

Comme $\sqrt{2} \notin \mathbb{Q}\left(\sqrt{a}, \sqrt{b}\right)$ alors $\alpha^{-2k}\gamma \neq 1$, par suite

$$1 < \left(\alpha^{-2k}\gamma\right)^{-1} \leqslant \alpha.$$

De la minimalité de α, on déduit que $\left(\beta^{2k}\gamma\right)^{-1} = \alpha$, autrement dit, $\gamma = \alpha^{2k-1}$. □

Théorème 3.19. *Soient a, b deux entiers positifs impairs. Supposons que l'équation* (3.19) *possède au moins une solution en entiers strictement positifs (x, y). Soit $\alpha = \frac{x_1\sqrt{a} + y_1\sqrt{b}}{\sqrt{2}}$ la solution fondamentale de l'équation* (3.19) *alors α^2 est la solution fondamentale de l'équation de Pell-Fermat $X^2 - abY^2 = 1$.*

Démonstration. Soit $\varepsilon = T + U\sqrt{ab}$ la solution fondamentale de l'équation

$$X^2 - abY^2 = 1. \tag{3.26}$$

D'après la proposition 3.17, α^2 est solution de l'équation de Pell-Fermat (3.26). Par conséquent $1 < \varepsilon \leqslant \alpha^2$. Supposons que $\alpha^2 \neq \varepsilon$. Posons alors $\gamma = \varepsilon\alpha^{-1}$. On a $\alpha^{-1} < \gamma < \alpha$, $\mathcal{N}(\gamma) = 1$ et

$$\begin{aligned}\gamma &= \left(T + U\sqrt{ab}\right)\frac{x_1\sqrt{a} - y_1\sqrt{b}}{\sqrt{2}} \\ &= \frac{(Tx_1 - Uby_1)\sqrt{a} + (aUx_1 - Ty_1)\sqrt{b}}{\sqrt{2}} \in M.\end{aligned}$$

La minimalité de α entraîne que $\alpha^{-1} < \gamma \leqslant 1$. D'où $1 \leqslant \gamma^{-1} < \alpha$. En utilisant encore une fois la minimalité de α, on en déduit que nécessairement $\gamma = 1$, ce qui est absurde vu que $1 \notin S$. □

Exemple 3.20. *Soit à résoudre l'équation diophantienne*

$$15x^2 - 37y^2 = 2. \tag{3.27}$$

On considère alors l'équation de Pell-Fermat

$$X^2 - 555Y^2 = 1. \tag{3.28}$$

En développant $\sqrt{555}$ en fraction continue, on obtient

$$\sqrt{555} = [23; \overline{1, 1, 3, 1, 3, 1, 1, 46}].$$

Soit $\varepsilon = T + U\sqrt{52}$ la solution fondamentale de l'équation (3.28)*. Alors d'après le théorème 3.5*

$\varepsilon = p_7 + q_7\sqrt{555}$ où $\frac{p_7}{q_7}$ est la 7^e réduite de $\sqrt{555}$.

$$\frac{p_7}{q_7} = 23 + \cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{1}}}}}}} = \frac{1814}{77}.$$

On en déduit que $\varepsilon = 1814 + 77\sqrt{555}$. D'après le théorème 3.19, si l'équation (3.27) *possède une solution, alors la solution fondamentale $\alpha = \frac{x_1\sqrt{15} + y_1\sqrt{37}}{\sqrt{2}}$ vérifie*

$$\alpha^2 = \varepsilon = 1814 + 77\sqrt{555}.$$

Donc (x_1, y_1) est solution du système suivant :

$$\begin{cases} 15x_1^2 + 37y_1^2 = 2 \cdot 1814 \\ 15x_1^2 - 37y_1^2 = 2. \end{cases}$$

On en déduit que $x_1 = 11$ et $y_1 = 7$. Le nombre $\alpha = \frac{11\sqrt{15} + 7\sqrt{37}}{\sqrt{2}}$ est donc la solution fondamentale de l'équation (3.27).

$$S_+ = \left\{ \left(\frac{11\sqrt{15} + 7\sqrt{37}}{\sqrt{2}} \right)^{2n-1} ; \quad n \in \mathbb{N}^* \right\}.$$

Intéressons-nous maintenant à l'équation diophantienne

$$ax^2 - by^4 = 2, \tag{3.29}$$

où a et b sont deux entiers positifs impairs. Il est clair que si (x, y) est une solution de l'équation (3.19) alors (x, y^2) est une solution de l'équation $aX^2 - bY^2 = 2$. D'après la proposition 3.17, les solutions en entiers strictement positifs de l'équation $aX^2 - bY^2 = 2$ sont les termes de la suite $(x_{2n-1}, y_{2n-1})_{n\in\mathbb{N}^*}$. Par conséquent, résoudre l'équation (3.29) revient à déterminer les indices k impairs tels que $y_k = \square$. En 1953, Ljunggren [44] montre que l'équation (3.29) possède au plus deux solutions en entiers strictement positifs. Plus précisément, il montre le résultat suivant :

Théorème 3.21 ([45, Theorem L2])**.** *Soient a et b deux entiers positifs impairs. Supposons que l'équation* (3.19) *possède au moins une solution. Soit alors $\alpha = \frac{x_1\sqrt{a} + y_1\sqrt{b}}{\sqrt{2}}$ la solution fondamentale de l'équation* (3.19)*. Avec les notations précédentes. Si $y_1 = v^2\ell$ où ℓ est sans facteur carré, alors l'équation $y_k = \square$ entraîne $k = \ell$ ou $k = 3\ell$*

En 2001, Luca et Walsh (cf. [45]) améliore ce résultat en prouvant que nécessairement $\ell = 1$. Ces derniers auteurs prouvent le résultat suivant :

Théorème 3.22 ([45])**.** *Soient a, b deux entiers positifs impairs. Supposons que l'équation diophantienne $ax^2 - by^2 = 2$ possède au moins une solution, soit alors $\alpha = \frac{x_1\sqrt{a} + y_1\sqrt{b}}{\sqrt{2}}$ sa solution fondamentale. Alors, avec les notations précédentes :*

1. *Si $y_1 \neq \square$, alors l'équation* (3.29) *ne possède pas de solutions.*
2. *Si $y_1 = \square$ et $y_3 \neq \square$, alors $(x_1, \sqrt{y_1})$ est l'unique solution en entiers strictement positifs de l'équation* (3.29).
3. *Si $y_1 = \square$ et $y_3 = \square$, alors $(x_1, \sqrt{y_1})$ et $(x_3, \sqrt{y_3})$ sont les seules solutions en entiers strictement positifs de l'équation* (3.29).

Exemple 3.23. *Considérons l'équation diophantienne*

$$5x^2 - 3y^4 = 2.$$

La solution fondamentale de l'équation $5X^2 - 3Y^2 = 2$ est

$$\alpha = \frac{\sqrt{5} + \sqrt{3}}{\sqrt{2}}.$$

On en déduit que

$$x_1 = 1, \quad y_1 = 1, \quad x_3 = 7 \quad \text{et} \quad y_3 = 9.$$

D'après le théorème 3.22 $(x_1, \sqrt{y_1}) = (1, 1)$ et $(x_3, \sqrt{y_3}) = (7, 3)$ sont les seules solutions en entiers strictement positifs de l'équation $5x^2 - 3y^4 = 2$.

Exemple 3.24. *Considérons l'équation diophantienne*

$$3x^2 - 25y^4 = 2.$$

Déterminons la solution fondamentale de l'équation diophantienne

$$3X^2 - 25Y^2 = 2. \tag{3.30}$$

Pour cela, commençons par déterminer la solution fondamentale de l'équation de Pell-Fermat

$$t^2 - 75u^2 = 1. \tag{3.31}$$

En développant $\sqrt{75}$ en fraction continue, on obtient

$$\sqrt{75} = [8; \overline{1, 1, 1, 16}].$$

Soit $\varepsilon = T + U\sqrt{52}$ la solution fondamentale de l'équation (3.31). *Alors d'après le théorème 3.5, $\varepsilon = 26 + 3\sqrt{75}$. Par ailleurs, le théorème 3.19 montre que si l'équation* (3.30) *possède une solution, alors sa solution fondamentale*

$$\alpha = \frac{x_1\sqrt{3} + 5y_1}{\sqrt{2}} = \sqrt{\varepsilon} = \frac{3\sqrt{3} + 5}{\sqrt{2}}.$$

Par suite,

$$\alpha^3 = \frac{153\sqrt{3} + 53 \cdot 5}{\sqrt{2}}.$$

On en déduit que

$$x_1 = 3, \quad y_1 = 1, \quad x_3 = 153 \quad \text{et} \quad y_3 = 53.$$

D'après le théorème 3.22, $(x, y) = (x_1, \sqrt{y_1}) = (3, 1)$ *est l'unique solution en entiers strictement positifs de l'équation* $3x^2 - 25y^4 = 2$.

3.5 Nombre de solutions de l'équation $y^2 = px\left(Ax^2 + 2\right)$

En 2014, A.Togbé [69] a considéré l'équation diophantienne : $y^2 = px(Ax^2 + 2)$, où p est un nombre premier et A est un entier impair supérieur à 2. Il prouve le théorème suivant.

Théorème 3.25. *Pour tout nombre premier* p *et tout entier positif impair* $A > 1$*, l'équation diophantienne* $y^2 = px(Ax^2 + 2)$ *possède au plus* 7 *solutions en entiers strictement positifs.*

Dans cette section, on utilisera des propriétés bien connues du symbole de Legendre afin d'améliorer la majoration du nombre de solutions de l'équation diophantienne $y^2 = px(Ax^2 + 2)$ considérée dans le théorème 3.25, et de fournir une preuve partielle de la Conjecture 3.1, d'Alain Togbé [69].

Soient $m, n \in \mathbb{Z}$. On dit que m est un résidu quadratique modulo n s'il existe $k \in \mathbb{Z}$ tel que l'on ait

$$m \equiv k^2 \pmod{n}.$$

Dans ce cas, on dit aussi que m est un carré modulo n.

Définition 3.26. *Soient* p *un nombre premier et* n *un entier rationnel. Le symbole de Legendre noté* $\left(\frac{n}{p}\right)$ *est l'entier défini comme suit :*

$$\left(\frac{n}{p}\right) := \begin{cases} 0 & \text{si } p \text{ divise } n, \\ -1 & \text{si } n \text{ n'est pas un résidu quadratique modulo } p, \\ 1 & \text{si } p \text{ ne divise pas } n \text{ et } n \text{ est un résidu quadratique modulo } p. \end{cases}$$

Le symbole de Legendre ne dépend que de la classe de n modulo p et vérifie les deux propositions suivantes. On notera $\mathbb{F}_p$ le corps fini à p éléments.

Proposition 3.27 ([42])**.** *Soit* p *un nombre premier impair. On a :*

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

Ainsi, -1 *est un résidu quadratique modulo* p *si et seulement si :*

$$p \equiv 1 \pmod{4}.$$

Démonstration. Supposons que -1 est un résidu quadratique modulo p, alors il existe $x \in (\mathbb{F}_p)^*$ tel que $-1 = x^2$. Par suite, x est un élément de $(\mathbb{F}_p)^*$ d'ordre 4. D'où 4 divise $p - 1$ qui est l'ordre du groupe $(\mathbb{F}_p)^*$. Par conséquent $p \equiv 1 \pmod{4}$. Supposons que $4 \mid (p - 1)$. Comme $(\mathbb{F}_p)^*$ est un groupe cyclique alors il possède un élément x d'ordre 4. Autrement dit $(x^2)^2 = 1$ et $x^2 \neq 1$. D'où $x^2 = -1$. Ainsi -1 est résidu quadratique modulo p. □

Proposition 3.28 ([42] p.181)**.** *Soit* p *un nombre premier impair. On a*

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

Ainsi, 2 est un résidu quadratique modulo p si et seulement si

$$p \equiv 1 \pmod 8 \quad ou \quad p \equiv 7 \pmod 8.$$

Démonstration. Soit ζ une racine primitive 8^{e} de l'unité dans $\overline{\mathbb{F}_p}$. Alors $\zeta^8 = 1$ et $\zeta^4 = -1$. Par suite $\zeta^{-2} = -\zeta^2$. Par conséquent, en posant $\phi = \zeta + \zeta^{-1}$, on obtient :

$$\phi^2 = \zeta^2 + \zeta^{-2} + 2 = 2.$$

On en déduit que 2 est résidu quadratique modulo p si et seulement si $\phi \in \mathbb{F}_p$. Or

$$\mathbb{F}_p = \left\{ a \in \overline{\mathbb{F}_p}; \quad a^p = a \right\}.$$

Calculons alors ϕ^p. Sachant que $\zeta^8 = 1$ et $\zeta^4 = -1$ alors

$$\zeta^p = \begin{cases} \zeta & \text{si } p \equiv 1 \pmod 8 \\ -\zeta^{-1} & \text{si } p \equiv 3 \pmod 8 \\ -\zeta & \text{si } p \equiv 5 \pmod 8 \\ \zeta^{-1} & \text{si } p \equiv 7 \pmod 8 \end{cases}$$

Par conséquent,

$$\phi^p = \zeta^p + \zeta^{-p} = \begin{cases} \phi & \text{si } p \equiv \pm 1 \pmod 8 \\ -\phi & \text{si } p \equiv \pm 3 \pmod 8 \end{cases}$$

On en déduit que 2 est résidu quadratique modulo p si et seulement si $p \equiv \pm 1 \pmod 8$. □

Le théorème suivant constitue le résultat principal de ce chapitre.

Théorème 3.29 ([29])**.** *Soient p un nombre premier et $A > 1$ un entier impair. Considérons l'équation diophantienne*

$$y^2 = px\left(Ax^2 + 2\right). \tag{3.32}$$

1. *Si $p = 2$, alors l'équation diophantienne* (3.32) *possède au plus une solution en entiers strictement positifs (x, y)*
2. *Supposons p impair et $\left(\frac{-2A}{p}\right) \neq 1$.*
   (a) *Si $(A, p) \equiv (7, 1)$ ou $(7, 7) \pmod 8$, alors l'équation diophantienne* (3.32) *possède au plus trois solutions en entiers strictement positifs (x, y).*
   (b) *L'équation diophantienne* (3.32) *possède au plus une solution en entiers strictement positifs (x, y) dans tous les autres cas.*
3. *Supposons p est impair et $\left(\frac{-2A}{p}\right) = 1$.*
   (a) *Si $(A, p) \equiv (1, 5)$, $(1, 7)$, $(3, 3)$, $(5, 5)$, $(7, 3)$, ou $(7, 5) \pmod 8$, alors l'équation diophantienne* (3.32) *possède au plus une solution en entiers strictement positifs (x, y).*
   (b) *Si $(A, p) \equiv (1, 1)$, $(3, 1)$, $(3, 7)$, $(5, 1)$, $(5, 3)$, ou $(5, 7) \pmod 8$, alors l'équation diophantienne* (3.32) *possède au plus deux solutions en entiers strictement positifs (x, y).*
   (c) *Si $(A, p) \equiv (1, 3)$ ou $(3, 5) \pmod 8$, alors l'équation diophantienne* (3.32) *possède au plus trois solutions en entiers strictement positifs (x, y).*

(d) Si $(A,p) \equiv (7,7) \pmod 8$*, alors l'équation diophantienne* (3.32) *possède au plus quatre solutions en entiers strictement positifs* (x,y)*.*

(e) Si $(A,p) \equiv (7,1) \pmod 8$*, alors l'équation diophantienne* (3.32) *possède au plus six solutions en entiers strictement positifs* (x,y)*.*

Démonstration. Supposons $p = 2$ et soit $A > 1$ un entier impair.
Soient x et y des entiers strictement positifs tels que

$$y^2 = 2x(Ax^2 + 2). \tag{3.33}$$

Alors

$$2\nu_2(y) = 1 + \nu_2(x) + \nu_2(Ax^2 + 2). \tag{3.34}$$

Si l'on suppose que x est impair, alors $Ax^2 + 2$ l'est aussi, ce qui contredit la relation (3.34). Donc $\nu_2(x) \geqslant 1$ et $\nu_2(Ax^2 + 2) = 1$. Il vient de la relation (3.34) que $\nu_2(x)$ est nécessairement pair, d'où $\nu_2(x) \geqslant 2$ et par suite $\nu_2(y) \geqslant 2$. Il existe alors des entiers positifs w, z tels que $x = 4z$ et $y = 4w$. On obtient alors :

$$w^2 = z(8Az^2 + 1). \tag{3.35}$$

Puisque $\text{pgcd}(z, 8Az^2 + 1) = 1$, alors il existe des entiers strictement positifs u et v tels que $z = u^2$, $8Az^2 + 1 = v^2$, et

$$v^2 - 8Au^4 = 1. \tag{3.36}$$

D'après le corollaire 3.8, cette dernière équation possède au plus une solution $(u, v) \in \mathbb{N}^* \times \mathbb{N}^*$.

Considérons maintenant le cas où p est un premier impair et soit $A > 1$ un entier impair. Soient x et y deux entiers strictement positifs tels que

$$y^2 = px(Ax^2 + 2). \tag{3.37}$$

On remarque que

$$\text{pgcd}(x, Ax^2 + 2) = \begin{cases} 1 & \text{si } x \text{ est impair} \\ 2 & \text{si } x \text{ est pair.} \end{cases}$$

On considérera alors deux cas selon la parité de x.

Supposons d'abord que x soit pair, alors il existe un entier positif z tel que $x = 2z$. On obtient donc :

$$y^2 = 4pz(2Az^2 + 1). \tag{3.38}$$

Puisque p est premier alors il existe un entier strictement positif w tel que $y = 2pw$. Ce qui entraîne que :

$$pw^2 = z(2Az^2 + 1). \tag{3.39}$$

Or $\text{pgcd}(z, 2Az^2 + 1) = 1$, donc il existe deux entiers strictement positifs u et v vérifiant l'une des conditions suivantes :
ou bien $z = pu^2$, $2Az^2 + 1 = v^2$, et

$$v^2 - 2Ap^2u^4 = 1, \tag{3.40}$$

ou bien $z = u^2$, $2Az^2 + 1 = pv^2$, et

$$pv^2 - 2Au^4 = 1. \tag{3.41}$$

Supposons maintenant que x soit impair, alors $\text{pgcd}(x, Ax^2+2) = 1$.
Puisque p est premier, il existe alors un entier strictement positif w tel que $y = pw$.
On obtient alors :

$$pw^2 = x(Ax^2+2). \tag{3.42}$$

Or $\text{pgcd}(x, Ax^2+2) = 1$, il existe donc deux entiers strictement positifs u et v vérifiant l'une des conditions suivantes :
ou bien $x = pu^2$, $Ax^2+2 = v^2$, et alors :

$$v^2 - Ap^2u^4 = 2, \tag{3.43}$$

ou bien $x = u^2$, $Ax^2+2 = pv^2$, et alors :

$$pv^2 - Au^4 = 2. \tag{3.44}$$

Nous allons considérer chacune des équations (3.40), (3.41), (3.43) et (3.44) séparément pour déterminer le nombre de solutions en entiers strictement positifs de l'équation diophantienne (3.32).

1. Commençons par l'équation (3.40). Soit $D = 2Ap^2$, d'après le corollaire 3.8, l'équation (3.40) possède au plus une solution en entiers strictement positifs (u, v).
2. On peut déduire directement du Théorème 3.15 que l'équation (3.41) possède au plus une solution en entiers strictement positifs (u, v). Il découle de cette équation que v est impair, donc $v^2 \equiv 1 \pmod 8$ et que u est pair si et seulement si $p \equiv 1 \pmod 8$. Si $p \equiv 3, 5,$ ou $7 \pmod 8$, alors u est nécessairement impair et dans ce cas $p - 2A \equiv 1$ ($\pmod 8$. Par conséquent, l'équation (3.41) possède une solution seulement si $(A, p) \equiv (1,1), (3,1), (5,1), (7,1), (1,3), (5,3), (3,7),$ ou $(7,7) \pmod 8$. De plus, l'équation (3.41) possède une solution seulement si $\left(\frac{-2A}{p}\right) = 1$.
3. D'après le théorème 3.22, l'équation (3.43) possède au plus deux solutions en entiers strictement positifs. Supposons que l'équation (3.43) possède une solution (u, v) en entiers strictement positifs, D'après le lemme 3.16, u et v sont nécessairement impairs. On en déduit que $u^4 \equiv 1 \pmod 8$, $v^2 \equiv 1 \pmod 8$ et $p^2 \equiv 1 \pmod 8$. En réduisant la relation (3.43) modulo 8 et modulo p, on obtient :

   $$1 - A \equiv 2 \pmod 8 \text{ et } v^2 \equiv 2 \pmod p. \tag{3.45}$$

   Par suite,

   $$A \equiv 7 \pmod 8 \text{ et } \left(\frac{2}{p}\right) = 1. \tag{3.46}$$

   Or $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, donc $\left(\frac{2}{p}\right) = 1$ si et seulement si $p \equiv 1 \pmod 8$ ou $p \equiv 7 \pmod 8$. Par conséquent, l'équation (3.43) possède une solution en entiers seulement si $(A, p) \equiv (7,1)$ ou $(7,7) \pmod 8$.
4. D'après le Théorème 3.22, l'équation (3.44) possède au plus deux solutions en entiers strictement positifs. Supposons que l'équation (3.44) possède une solution en entiers strictement positifs (u, v), alors d'après le lemme 3.16, u et v sont nécessairement impairs, d'où $u^4 \equiv \pmod 8$ et $v^2 \equiv 1 \pmod 8$. En réduisant la relation (3.44) modulo 8 on obtient $p - A \equiv 2 \pmod 8$. Par conséquent, l'équation (3.44) possède une solution en entiers seulement si $(A, p) \equiv (1,3), (3,5), (5,7),$ ou $(7,1) \pmod 8$.

Supposons maintenant que l'équation (3.44) possède deux solutions en entiers strictement positifs, et soit (a_1, b_1) la solution, en entiers strictement positifs, minimale de l'équation :

$$pX^2 - AY^2 = 2, \tag{3.47}$$

alors

$$p{a_1}^2 - A{b_1}^2 = 2. \tag{3.48}$$

Soit

$$\alpha = \frac{a_1\sqrt{p} + b_1\sqrt{A}}{\sqrt{2}}, \tag{3.49}$$

d'où

$$\alpha^3 = \frac{a_3\sqrt{p} + b_3\sqrt{A}}{\sqrt{2}}$$

avec

$$a_3 = \frac{pa_1^3 + 3Aa_1b_1^2}{2} \text{ et } b_3 = \frac{3{a_1}^2pb_1 + {b_1}^3A}{2}. \tag{3.50}$$

Alors (a_3, b_3) est solution de l'équation (3.47), et vérifie

$$p{a_3}^2 - A{b_3}^2 = 2. \tag{3.51}$$

Puisqu'on a supposé que l'équation (3.44) possède deux solutions en entiers strictement positifs, alors, d'après le théorème 3.22, $b_1 = \square$ et $b_3 = \square$. Il existe donc deux entiers strictement positifs B_1 et B_3 tels que :

$$b_1 = {B_1}^2 \quad \text{et} \quad b_3 = {B_3}^2$$

et

$$3{a_1}^2p{B_1}^2 + {B_1}^6A = 2{B_3}^2. \tag{3.52}$$

En réduisant la relation (3.52) modulo p, on obtient :

$$B_1^6A \equiv 2B_3^2 \pmod{p}.$$

par suite,

$$\left(\frac{2B_3^2}{p}\right) = \left(\frac{AB_1^6}{p}\right), \tag{3.53}$$

d'où

$$\left(\frac{2}{p}\right)\left(\frac{B_3^2}{p}\right) = \left(\frac{A}{p}\right)\left(\frac{B_1^6}{p}\right).$$

Or (a_1, b_1) et (a_3, b_3) sont solutions de l'équation (3.47) et par conséquent, d'après le lemme 3.16, on a

$$\text{pgcd}\,(p, b_1) = 1 \text{ et } \text{pgcd}(p, b_3) = 1. \tag{3.54}$$

De même

$$\text{pgcd}\,(p, B_1) = 1 \text{ et } \text{pgcd}(p, B_3) = 1.$$

Par conséquent $\left(\frac{B_3^2}{p}\right) = \left(\frac{B_1^6}{p}\right) = 1$. On en déduit donc que $\left(\frac{2}{p}\right) = \left(\frac{A}{p}\right)$. La réduction de la relation (3.48) modulo p, donne $-Ab_1^2 \equiv 2 \pmod{p}$. Donc $-2Ab_1^2 \equiv 4 \pmod{p}$. D'où

$\left(\frac{-2A}{p}\right)\left(\frac{b_1^2}{p}\right) \equiv \left(\frac{4}{p}\right)$. Comme p est impair alors $\left(\frac{4}{p}\right) = 1$. D'après (3.54), on obtient

$$\left(\frac{2}{p}\right) = \left(\frac{-A}{p}\right). \tag{3.55}$$

Les relations (3.53) et (3.55) donnent

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

Il s'en suit que

$$p \equiv 1 \pmod 4,$$

donc

$$p \equiv 1 \pmod 8 \text{ ou } p \equiv 5 \pmod 8.$$

En conclusion, l'équation (3.44) possède au plus deux solutions en entiers strictement positifs seulement si

$$(A, p) \equiv (3, 5) \text{ ou } (7, 1) \pmod 8,$$

et elle possède au plus une solution en entiers strictement positifs seulement si $(A, p) \equiv (1, 3)$ ou $(5, 7) \pmod 8$.
De plus, l'équation (3.44) possède une solution en entiers seulement si $\left(\frac{-2A}{p}\right) = 1$.

Puisque le nombre de solutions en entiers strictement positifs des équations (3.41) et (3.44) dépend de la valeur de $\left(\frac{-2A}{p}\right)$, nous supposerons d'abord que $\left(\frac{-2A}{p}\right) \neq 1$. Alors les équations (3.41) et (3.44) ne possèdent pas de solutions, l'équation (3.40) possède au plus une solution en entiers strictement positifs ; et (3.43) possède au plus deux solutions en entiers strictement positifs seulement si $(A, p) \equiv (7, 1)$ où $(7, 7) \pmod 8$. Par conséquent si $\left(\frac{-2A}{p}\right) \neq 1$, l'équation (3.4) possède au plus trois solutions en entiers strictement positifs si $(A, p) \equiv (7, 1)$ ou $(7, 7) \pmod 8$, et elle possède au plus une solution en entiers strictement positifs dans tous les autres cas.

Supposons maintenant que $\left(\frac{-2A}{p}\right) = 1$. Alors l'équation (3.41) possède au plus une solution en entiers strictement positifs.

Si $A \equiv 1 \pmod 8$, alors l'équation (3.40) possède au plus une solution, l'équation (3.41) possède au plus une solution seulement si $p \equiv 1$ ou $3 \pmod 8$, l'équation (3.43) ne possède pas de solutions, et l'équation (3.44) possède au plus une solution en entiers strictement positifs seulement si $p \equiv 3 \pmod 8$.

Si $A \equiv 3 \pmod 8$, alors l'équation (3.40) possède au plus une solution , (3.41) possède au plus une solution et seulement si $p \equiv 1$ ou $7 \pmod 8$, (3.43) ne possède pas de solutions, et (3.44) possède au plus deux solutions et seulement si $p \equiv 5 \pmod 8$.

Si $A \equiv 5 \pmod 8$, alors l'équation (3.40) possède au plus une solution, (3.41) possède au plus une solution et seulement si $p \equiv 1$ ou $3 \pmod 8$, (3.43) ne possède pas de solutions, et (3.44) possède au plus une solution et seulement si $p \equiv 7 \pmod 8$.
Si $A \equiv 7 \pmod 8$, alors l'équation (3.40) possède au plus une solution, (3.41) possède au plus une solution seulement si $p \equiv 1$ ou $7 \pmod 8$, (3.43) possède au plus deux solutions seulement si $p \equiv 1$

ou 7 (mod 8), et (3.44) possède au plus une solution seulement si $p \equiv 1 \pmod 8$. □

Le théorème suivant donne une majoration du nombre de solutions de l'équation diophantienne $y^2 = px(Ax^2 + 2)$ dans le cas où A est un entier pair.

Théorème 3.30 ([29]). *Soit p un nombre premier et soit $A > 1$ un nombre entier pair. Considérons l'équation diophantienne*

$$y^2 = px(Ax^2 + 2) \tag{3.56}$$

1. *Si $p = 2$, alors l'équation diophantienne* (3.56) *possède au plus deux solutions en entiers strictement positifs (x, y). De plus, si $A \equiv 0 \pmod 4$ et $A \neq 2^6 \cdot 1785$, alors l'équation diophantienne* (3.56) *possède au plus une solution en entiers strictement positifs (x, y).*
2. *Supposons que $\left(\frac{-2A}{p}\right) \neq 1$, où p est un nombre premier impair.*
   (a) *Si $A \equiv 0 \pmod 4$, alors l'équation diophantienne* (3.56) *possède au plus une solution en entiers strictement positifs (x, y).*
   (b) *Si $A \equiv 2 \pmod 4$, alors l'équation diophantienne* (3.56) *possède au plus deux solutions en entiers strictement positifs (x, y).*
3. *Supposons que $\left(\frac{-2A}{p}\right) = 1$, où p est un nombre premier impair.*
   (a) *Si $(A, p) \equiv (0, 3) \pmod 4$, alors l'équation diophantienne* (3.56) *possède au plus une solution en entiers strictement positifs (x, y).*
   (b) *Si $(A, p) \equiv (0, 1) \pmod 4$, alors l'équation diophantienne* (3.56) *possède au plus deux solutions en entiers strictement positifs (x, y).*
   (c) *Si $(A, p) \equiv (2, 3) \pmod 4$, alors l'équation diophantienne* (3.56) *possède au plus trois solutions en entiers strictement positifs (x, y).*
   (d) *Si $(A, p) \equiv (2, 1) \pmod 4$, alors l'équation diophantienne* (3.56) *possède au plus quatre solutions en entiers strictement positifs (x, y).*

Démonstration. Soit (x, y) une solution en entiers strictement positifs de l'équation (3.56). A est un entier pair supérieur à 1, il existe alors un entier strictement positif A' tel que $A = 2A'$.

Supposons que $p = 2$, alors

$$y^2 = 2x(2A'x^2 + 2),$$

et y est nécessairement pair. Il existe alors un entier strictement positif w tel que $y = 2w$. On obtient alors

$$w^2 = x(A'x^2 + 1).$$

Puisque $\text{pgcd}(x, A'x^2 + 1) = 1$, il existe alors deux entiers strictement positifs u et v tels que

$$x = u^2,\ A'x^2 + 1 = v^2$$

et

$$v^2 - A'u^4 = 1. \tag{3.57}$$

Cette dernière équation ne possède pas de solutions si $A' = \square$ et possède au plus deux solutions en entiers strictement positifs d'après le théorème 3.7. De plus, si A' est pair et $A' \neq 2^5 \cdot 1785$, alors d'après le corollaire 3.8, l'équation (3.57) possède au plus une solution en entiers strictement positifs.

Supposons que p soit un nombre premier impair, alors $2p \mid y$. Par suite, il existe un entier strictement positif w tel que $y = 2pw$. On obtient alors

$$2pw^2 = x(A'x^2 + 1).$$

Puisque $\text{pgcd}(x, A'x^2 + 1) = 1$, alors il existe deux entiers strictement positifs u et v tels que $x = 2pu^2$, $A'x^2 + 1 = v^2$, et alors :

$$v^2 - 4A'^2u^4 = 1, \tag{3.58}$$

ou $x = 2u^2$, $A'x^2 + 1 = pv^2$ et alors :

$$pv^2 - 4A'u^4 = 1, \tag{3.59}$$

ou $x = u^2$, $A'x^2 + 1 = 2pv^2$ et alors :

$$2pv^2 - A'u^4 = 1, \tag{3.60}$$

ou $x = pu^2$, $A'x^2 + 1 = 2v^2$ et alors :

$$2v^2 - A'u^4 = 1. \tag{3.61}$$

Si $A' = \square$, alors l'équation (3.58) ne possède pas de solutions ; sinon elle possède au plus une solution en entiers strictement positifs d'après le corollaire 3.8.

D'après le théorème 3.15, chacune des équations (3.59), (3.60), et (3.61) possède au plus une solution en entiers strictement positifs. L'équation (3.59) possède au moins une solution seulement si $p \equiv 1 \pmod 4$ et $\left(\frac{-A'}{p}\right) = 1$, l'équation (3.60) possède au moins une solution seulement si A' est impair et $\left(\frac{-A'}{p}\right) = 1$ et l'équation (3.61) possède une solution seulement si A' est impair. Puisque le nombre de solutions des équations (3.59) et (3.60) dépend de la valeur de $\left(\frac{-A'}{p}\right) = \left(\frac{-2A}{p}\right)$, on supposera d'abord que $\left(\frac{-2A}{p}\right) \neq 1$, et alors les équations (3.59) et (3.60) ne possèdent pas de solutions en entiers strictement positifs.

Si $A \equiv 0 \pmod 4$, alors l'équation (3.58) possède au plus une solution en entiers strictement positifs, (3.59) ne possède pas de solution, (3.60) ne possède pas de solutions et (3.61) ne possède pas de solution.

Si $A \equiv 2 \pmod 4$, alors l'équation (3.58) possède au plus une solution en entiers strictement positifs, (3.59) ne possède pas de solution, (3.60) ne possède pas de solutions et (3.61) possède au plus une solution en entiers strictement positifs.

Supposons maintenant que $\left(\frac{-2A}{p}\right) = 1$. Alors les équations (3.59) et (3.60) possèdent au plus une solution en entiers strictement positifs.
Si $A \equiv 0 \pmod 4$, alors l'équation (3.58) possède au plus une solution en entiers strictement positifs, (3.59) possède au plus une solution et seulement si $p \equiv 1 \pmod 4$, (3.60) ne possède pas de solution et (3.61) ne possède pas de solution.

Si $A \equiv 2 \pmod 4$, alors l'équation (3.58) possède au plus une solution en entiers strictement positifs, (3.59) possède au plus une solution et seulement si $p \equiv 1 \pmod 4$, (3.60) possède au plus une solution en entiers strictement positifs et (3.61) possède au plus une solution en entiers strictement positifs. □

Remarque 3.31. *Le théorème 3.29 implique que la Conjecture 3.1 est vraie si* $(A, p) \equiv (1, 5)$, $(1, 7)$, $(3, 3)$, $(3, 5)$, $(5, 3)$, $(7, 3)$ *ou* $(7, 5) \pmod 8$.

Chapitre 4

Nombre de solutions de l'équation $\mathrm{Res}_x\left(P\left(x\right), x^2+sx+t\right)=a$

4.1 Introduction

Soient

$$P(x)=a_m(x-\alpha_1)\cdots(x-\alpha_m)\in\mathbb{Z}[x],$$

où a_m est entier rationnel non nul et $\alpha_1,\ldots,\alpha_m$ sont les racines de P dans $\mathbb{C}$ et

$$Q(x)=x_nx^n+x_{n-1}x^{n-1}+\cdots+x_0\in\mathbb{Z}[x],$$

alors le résultant des deux polynômes P et Q peut être défini par

$$\mathrm{Res}_x(P(x),Q(x))=a_m^n\prod_{i=1}^{m}(x_n\alpha_i^n+x_{n-1}\alpha_i^{n-1}+\cdots+x_0). \tag{4.1}$$

On considère l'équation

$$\mathrm{Res}_x(P(x),Q(x))=a, \tag{4.2}$$

où a est un entier rationnel non nul donné. On remarque que cette dernière peut être considérée comme une équation diophantienne dont les inconnues sont les coefficients du polynôme Q. Plusieurs auteurs ont étudié ce type d'équation. On pourra citer par exemple Wirsing [74], Fujiwara [26], Schmidt [64], Schlickewei [63], Pethő [58, 59], Győry [37], Evertse et Győry [25]-[24] et enfin Gaàl [27] qui a prouvé que le nombre de polynômes Q, de degré inférieur au degré de P, vérifiant l'équation (4.2) est fini.

En 1971, Wirsing [74] a montré que si n et m sont des entiers strictement positifs vérifiant

$$2n\left(1+\frac{1}{3}+\cdots+\frac{1}{2n-1}\right)<m,$$

alors il existe un nombre fini de polynômes $Q\in\mathbb{Z}[x]$ de degré n vérifiant l'équation (4.2). Un peu plus tard, Fujiwara [26] montre que si le polynôme P est irréductible dans $\mathbb{Q}[x]$ et $2n<m$ alors l'équation (4.2) possède un nombre fini de solutions $Q\in\mathbb{Z}[x]$ de degré n.

De plus, en 1973, Schmidt [64] montre que la condition d'irréductibilité du polynôme P peut être remplacée par la condition que si $R\in\mathbb{Z}[x]$ est un polynôme non constant divisant le polynôme P alors $\deg R>n$.

Soient A un sous-anneau de $\mathbb{Q}$ de type fini, a un élément de A non nul et A^* le groupe des unités de A. Si m et n sont deux entiers strictement positifs tels que $2n < m$ et $P \in A[x]$ est un polynôme de degré m dont toutes les racines sont simples, ne possédant pas de facteur non constant dans $A[x]$ de degré inférieur ou égal à n, alors Schlickewei [63] a prouvé qu'il n'existe qu'un nombre fini de polynômes $Q \in A[x]$, à un facteur inversible près, de degré n vérifiant

$$\mathrm{Res}_x(P(x), Q(x)) \in a \cdot A^*.$$

Győry [37] a démontré que si $Q(x)$ est un polynôme unitaire, alors la condition $m \geqslant 2n$ peut être remplacée par la condition $m > 2n$. En 2002, Gaàl [27] a développé un algorithme qui permet de résoudre l'équation (4.2) quand $P \in \mathbb{Z}[x]$ est un polynôme irréductible de degré $m \geqslant 3$ et $Q = x^2 + x_1 x + x_2 \in \mathbb{Z}[x]$. Récemment, Gaàl et Posht [28] ont prolongé le résultat de Gaàl à tout polynôme unitaire $Q \in \mathbb{Z}[x]$ de degré $n \geqslant 2$.

En 1887, Runge [61] a montré que si $f(x, y)$ est un polynôme à coefficients entiers de degré n, irréductible dans $\mathbb{Q}[x, y]$ et que l'équation $f(x, y) = 0$ possède une infinité de solutions entières, alors sa partie homogène $f^+(x, y)$ de degré n est, à un facteur constant près, une puissance d'une forme irréductible.

Ce résultat a été amélioré en 1969 par Schinzel [62] qui prouva que, à un facteur constant prés, $f^+(x, y)$ est une puissance d'une forme linéaire ou d'une forme quadratique non définie.

Dans ce chapitre, on prouve, en utilisant le résultat de Schinzel [62], que pour tout entier rationnel non nul a, l'équation

$$\mathrm{Res}_x \left(P(x), x^2 + sx + t\right) = a$$

possède un nombre fini de solutions (s, t) dans $\mathbb{Z}^2$.

4.2 Résultant de deux polynômes

Soient K un corps commutatif, m et n deux entiers naturels. Considérons deux polynômes $P(x), Q(x) \in K[x]$ de degrés respectifs m et n.

$$P(x) = a_0 + a_1 x + \cdots + a_m x^m$$
$$Q(x) = b_0 + b_1 x + \cdots + b_n x^n$$

Pour tout entier naturel ℓ on pose

$$\mathbb{P}_\ell = \{f \in K[x]; \deg f < \ell\}.$$

$\mathbb{P}_\ell$ est un K-espace vectoriel de dimension ℓ. On considère l'application linéaire

$$\begin{aligned} \varphi : \mathbb{P}_n \times \mathbb{P}_m &\longrightarrow \mathbb{P}_{n+m} \\ (f, g) &\longmapsto fP + gQ \end{aligned}$$

On munit $\mathbb{P}_n \times \mathbb{P}_m$ de la base $\left(x^{n-1}, 0\right), \left(x^{n-2}, 0\right), \ldots, (1, 0), \left(0, x^{m-1}\right), \ldots, (0, 1)$ et $\mathbb{P}_{n+m}$ de la base $x^{n+m-1}, \ldots, 1$. La matrice de l'application φ relativement à ces bases est alors la matrice carrée

$S = (S_{ij})_{n+m \leqslant i,j \leqslant n+m}$ de taille $n+m$ où :

$$S_{ij} = \begin{cases} a_{m+j-i} & \text{si } 1 \leqslant j \leqslant n \quad \text{et} \quad j \leqslant i \leqslant m+j \\ b_{j-i} & \text{si } n+1 \leqslant j \leqslant n+m \quad \text{et} \quad j-n \leqslant i \leqslant j \\ 0 & \text{sinon,} \end{cases}$$

autrement dit :

$$S = \begin{pmatrix} a_m & 0 & \cdots & \cdots & 0 & b_n & 0 & \cdots & \cdots & 0 \\ a_{m-1} & a_m & \ddots & & \vdots & b_{n-1} & b_n & \ddots & & \vdots \\ \vdots & a_{m-1} & \ddots & \ddots & \vdots & \vdots & b_{n-1} & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 & \vdots & \vdots & \ddots & \ddots & 0 \\ a_1 & \vdots & & \ddots & a_m & b_1 & \vdots & & \ddots & b_n \\ a_0 & a_1 & & & a_{m-1} & b_0 & b_1 & & & b_{n-1} \\ 0 & a_0 & \ddots & & \vdots & 0 & b_0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & a_1 & \vdots & & \ddots & \ddots & b_1 \\ 0 & \cdots & \cdots & 0 & a_0 & 0 & \cdots & \cdots & 0 & b_0 \end{pmatrix},$$

où les coefficients de P sont reproduits sur $n = \deg Q$ colonnes tandis que ceux de Q le sont sur $m = \deg P$ colonnes.

Exemple 4.1. *Considérons deux polynômes $P(x), Q(x) \in K[x]$ de degrés respectifs 3 et 2. Posons $P(x) = a_0 + a_1x + a_2x^2 + a_3x^3$ et $Q(x) = b_0 + b_1x + b_2x^2$. Alors la matrice de Sylvester $\mathrm{Sylv}_x(P,Q)$ est donné par :*

$$\mathrm{Sylv}_x(P,Q) = \begin{pmatrix} a_3 & 0 & b_2 & 0 & 0 \\ a_2 & a_3 & b_1 & b_2 & 0 \\ a_1 & a_2 & b_0 & b_1 & b_2 \\ a_0 & a_1 & 0 & b_0 & b_1 \\ 0 & a_0 & 0 & 0 & b_0 \end{pmatrix}$$

Les coefficients de P sont reproduits sur $2 = \deg Q$ colonnes tandis que ceux de Q le sont sur $3 = \deg P$ colonnes.

Définition 4.2 ([41])**.** *Soient K un corps commutatif et P et Q deux éléments de $K[x]$. La matrice S ci-dessus est appelée matrice de Sylvester de P et Q et est notée $\mathrm{Sylv}_x(P,Q)$. Son déterminant est appelé résultant de P et Q et est noté $\mathrm{Res}_x(P,Q)$. Si $\deg P = \deg Q = 0$ alors $\mathrm{Sylv}_x(P,Q)$ est la matrice vide de déterminant $\mathrm{Res}_x(P,Q) = 1$. De plus, par convention, $\mathrm{Res}_x(P,0) = \mathrm{Res}_x(0,P) = 0$ si $P = 0$ ou $\deg P \geqslant 1$ et $\mathrm{Res}(P,0) = \mathrm{Res}(0,Q) = 1$ si P est de degré 0.*

Proposition 4.3. *Soient $P, Q \in K[x]$ de degrés respectifs $m, n \geqslant 0$ et $\lambda \in K$. Alors*

1. $\mathrm{Res}_x(\lambda, P) = \lambda^m$.
2. $\mathrm{Res}_x(P,P) = 0$.
3. $\mathrm{Res}_x(P, \lambda Q) = \lambda^m \mathrm{Res}_x(P,Q)$.
4. $\mathrm{Res}_x(P,Q) = (-1)^{mn} \mathrm{Res}_x(Q,P)$

Démonstration. Il suffit d'utiliser les propriétés élémentaires du déterminant. □

Proposition 4.4. *Soient $P, Q \in K[x]$ de degrés respectifs $m, n \geqslant 1$. Alors $\mathrm{Res}_x(P,Q) = 0$ si, et seulement s'il existe $U, V \in K[x]$, non nuls, de degré respectifs k et ℓ tels que $k < n$, $\ell < m$ et $UP - VQ = 0$.*

Démonstration. Le résultant $\mathrm{Res}_x(P,Q)$ est le déterminant de la matrice de Sylvester $\mathrm{Sylv}_x(P,Q)$ qui, rappelons le, est la matrice associée à l'application linéaire φ définie de $\mathbb{P}_n \times \mathbb{P}_m$ vers $\mathbb{P}_{n+m}$ par $\varphi(f,g) = fP + gQ$. Par conséquent, $\mathrm{Res}_x(P,Q)$ est nul si et seulement si le noyau de φ contient un élément non nul (U,V). □

On peut en déduire le résultat suivant.

Proposition 4.5. *Soient $P, Q \in K[x]$ de degrés respectifs $m, n \geqslant 1$. Pour que le résultant $\mathrm{Res}_x(P,Q)$ soit nul, il faut et il suffit que, P et Q aient un facteur commun non constant dans $K[X]$.*

Démonstration. D'après la proposition précédente, $\mathrm{Res}_x(P,Q) = 0$ équivaut à l'existence de $U, V \in K[x]$ non nuls, tels que $UP + VQ = 0$, $\deg U < \deg Q$ et $\deg V < \deg P$. Supposons que $(P,Q) = 1$ alors l'égalité $UP = -VQ$ entraîne que $P \mid V$, ce qui contredit $\deg V < \deg P$. □

Comme le résultant est une fonction des coefficients des polynômes P et Q, on peut aussi l'exprimer en fonction de leurs racines. On a le résultat suivant.

Théorème 4.6 ([41, Proposition 8.3])**.** *Soient K un corps commutatif et m et n deux entiers naturels. Considérons deux polynômes $P(x), Q(x) \in K[x]$ de degrés respectifs m et n. On note respectivement par $\alpha_1, \ldots, \alpha_m$, $\beta_1, \ldots, \beta_n$ les racines de P et Q dans $\overline{K}$. Alors*

$$\begin{aligned}\mathrm{Res}_x(P,Q) &= a_m^n b_n^m \prod_{i=1}^{m}\prod_{j=1}^{n}(\alpha_i - \beta_j)\\ &= a_m^n \prod_{i=1}^{m} Q(\alpha_i) = (-1)^{nm} b_n^m \prod_{j=1}^{n} P(\beta_j)\end{aligned}$$

Grâce à ce théorème, on peut déduire la proposition suivante.

Proposition 4.7. *Soient K un corps commutatif et $f, g, Q \in K[x]$. Alors*

$$\mathrm{Res}_x(fg, Q) = \mathrm{Res}_x(f,Q)\,\mathrm{Res}_x(g,Q).$$

Démonstration. On note respectivement $\alpha_1, \ldots, \alpha_k$, $\beta_1, \ldots, \beta_\ell$ les racines de f et g dans $\overline{K}$ et f_k et g_ℓ les coefficients dominants de f et g. Autrement dit,

$$\begin{aligned}f(x) &= f_k(x-\alpha_1)\cdots(x-\alpha_k),\\ g(x) &= g_\ell(x-\beta_1)\cdots(x-\beta_\ell).\end{aligned}$$

Notons m le degré de Q, alors d'après le théorème 4.6,

$$\begin{aligned}\mathrm{Res}_x(fg,Q) &= (f_k g_\ell)^m \prod_{i=1}^{k} Q(\alpha_i) \prod_{i=1}^{\ell} Q(\beta_i)\\ &= \left(f_k^m \prod_{i=1}^{k} Q(\alpha_i)\right)\left(g_\ell^m \prod_{i=1}^{\ell} Q(\beta_i)\right)\\ &= \mathrm{Res}_x(f,Q)\,\mathrm{Res}_x(g,Q).\end{aligned}$$

□

Proposition 4.8. *Soient K un corps commutatif, et P et Q deux éléments de $K[x]$ de degrés respectifs $m, n \geqslant 1$. Soit r le reste de la division euclidienne de P par Q alors*

$$\mathrm{Res}_x(P,Q) = (-1)^{nm} b_n^{n-\deg r}\, \mathrm{Res}_x(Q,r),$$

où b_n est le coefficient dominant de Q.

Démonstration. On note $\beta_1, \ldots, \beta_n$ les racines de Q dans $\overline{K}$. Alors

$$\begin{aligned}\mathrm{Res}_x\left(P,Q\right) &= (-1)^{nm} b_n^m \prod_{j=1}^{n} P\left(\beta_j\right) = (-1)^{nm} b_n^m \prod_{j=1}^{n} r\left(\beta_j\right) \\ &= (-1)^{nm} b_n^m \frac{1}{b_n^{\deg r}}\, \mathrm{Res}_x(Q,r).\end{aligned}$$

D'où le résultat. □

Le résultant est un outil dont les applications sont multiples. L'une d'elles est le calcul du discriminant d'un polynôme.

Définition 4.9. *Soit $P(x) = a_m x^m + \ldots + a_0 \in K[x]$; on appelle discriminant de P l'élément* $\mathrm{Dis}(P)$ *défini par*

$$\mathrm{Dis}(P) = (-1)^{\frac{m(m-1)}{2}} \frac{1}{a_m}\, \mathrm{Res}_x(P,P').$$

Exemple 4.10. *Si $P(x) = x^3 + px + q$, alors $P'(x) = 3x^2 + p$*

$$\mathrm{Sylv}_x(P,P') = \begin{pmatrix} 1 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 3 & 0 \\ p & 0 & p & 0 & 3 \\ q & p & 0 & p & 0 \\ 0 & q & 0 & 0 & p \end{pmatrix}$$

Par suite

$$\mathrm{Dis}(P) = -\det(\mathrm{Sylv}_x(P,P')) = -4p^3 - 27q^2.$$

4.3 Le polynôme $R(s,t) = \mathrm{Res}_x(P(x), x^2 + sx + t)$

Dans tout ce qui suit, $P(x) = a_m(x-\alpha_1)\cdots(x-\alpha_m)$ est un polynôme à coefficients entiers de degré m où $\alpha_1, \ldots, \alpha_m$ les racines de P dans $\mathbb{C}$ et $R(s,t)$ le polynôme défini par :

$$R(s,t) = \mathrm{Res}_x(P(x), x^2 + sx + t).$$

Lemme 4.11 ([5])**.** *Soient $A(s,t),\ B(s,t) \in \mathbb{Z}[s,t]$ tels que*

$$P(x) = (x^2 + sx + t)q(s,t,x) + A(s,t)x + B(s,t).$$

Alors

$$R(s,t) = B^2(s,t) + tA^2(s,t) - sA(s,t)B(s,t).$$

Démonstration. Soient γ, $\beta = -s-\gamma$ les racines du polynôme x^2+sx+t dans une clôture algébrique de $\mathbb{Q}(s,t)$. Alors d'après le théorème 4.6 on a

$$\begin{aligned} R(s,t) &= \mathrm{Res}_x\left(x^2+sx+t, P(x)\right) = P(\gamma)P(\beta) \\ &= (A\gamma+B)(A\beta+B) = tA^2+B^2-sAB. \end{aligned}$$

□

Proposition 4.12 ([5])**.**

$$R(s,-x^2-sx) = P(x)P(-s-x).$$

Démonstration. D'après le théorème 4.6

$$R(s,t) = a_m^2 \prod_{k=1}^{m} \left(\alpha_k^2 + s\alpha_k + t\right).$$

Par suite,

$$\begin{aligned} R(s,-x^2-sx) &= a_m^2 \prod_{k=1}^{m} \left(\alpha_k^2 + s\alpha_k - x^2 - sx\right) \\ &= a_m^2 \prod_{k=1}^{m} \left(x-\alpha_k\right)\left(-x-s-\alpha_k\right) \\ &= \left(a_m \prod_{k=1}^{m} \left(x-\alpha_k\right)\right)\left(a_m \prod_{k=1}^{m} \left(-x-s-\alpha_k\right)\right) \\ &= P(x)P\left(-x-s\right). \end{aligned}$$

□

Proposition 4.13 ([5])**.** *Il existe une suite unique de polynômes* $u_0(s,t)$, $u_1(s,t), \ldots, u_m(s,t)$ *à coefficients dans* $\mathbb{Z}$ *tels que*

$$P(x)P(-s-x) = u_0(s,t) + u_1(s,t)(x^2+sx+t) + \cdots + u_m(s,t)(x^2+sx+t)^m,$$

avec $u_0(s,t) = R(s,t)$ *et* $u_m(s,t) = (-1)^m a_m^2$.

Démonstration. D'après la proposition 4.12

$$P(x)P(-s-x) = R(s,-x^2-sx).$$

Or, d'après le lemme 4.11, $R(s,t) \in \mathbb{Z}[s,t]$. Par conséquent, le polynôme $R(s,t)$ s'écrit et de manière unique sous la forme $R(s,t) = \sum_{i=0}^{m} r_i(s)t^i$ où pour tout $i \in \{0,\ldots,m\}, r_i(s) \in \mathbb{Z}[s]$. On en déduit que :

$$\begin{aligned} P(x)P(-s-x) &= \sum_{i=0}^{m} (-1)^i r_i(s)\left(x^2+sx+t-t\right)^i \\ &= \sum_{k=0}^{m} \left(\sum_{i=k}^{m} \binom{i}{k} (-1)^k t^{i-k} r_i(s)\right)\left(x^2+sx+t\right)^k. \end{aligned}$$

Il suffit alors de poser pour tout $k \in \{0, \ldots, m\}$, $u_k(t,s) = \sum_{i=k}^{m} \binom{i}{k} (-1)^k t^{i-k} r_i(s)$. □

De cette proposition, on peut déduire immédiatement le résultat suivant.

Proposition 4.14 ([5]). *L'équation* $\mathrm{Res}_x(P(x), x^2 + sx + t) = a$ *possède une solution* $(s^*, t^*) \in \mathbb{Z}^2$ *si, et seulement si,*

$$P(x)P(-s^* - x) - a \equiv 0 \pmod{x^2 + s^* x + t^*}.$$

4.4 L'irréductibilité du polynôme $R(s,t) - a$

Dans cette section, nous allons étudier l'irréductibilité du polynôme $R(s,t) - a$, où a est un entier non nul. Rappelons qu'un polynôme f à coefficients dans un corps commutatif K est dit absolument irréductible s'il est irréductible sur sa clôture algébrique $\overline{K}$.

Théorème 4.15 ([5]). *Soient* a *un entier non nul,* $P(x) \in \mathbb{Z}[x]$ *un polynôme séparable de degré* m *et* $Q(s,x) \in \mathbb{Z}[s,x]$ *un polynôme de la forme*

$$Q(s,x) = Q_n s^n + Q_{n-1}(x) s^{n-1} + \cdots + Q_0(x),$$

avec $n \geqslant 1$ *et* $Q_n \in \mathbb{Z} \setminus \{0\}$. *Alors le polynôme* $P(x)Q(s,x) - a$ *est absolument irréductible.*

Démonstration. Soit $A(s,x) = A_k(x)s^k + A_{k-1}(x)s^{k-1} + \cdots + A_0(x)$ et $B(s,x) = B_\ell(x)s^\ell + B_{\ell-1}(x)s^{\ell-1} + \cdots + B_0(x)$ deux polynômes dans $\overline{\mathbb{Q}}[x,s]$ tels que $k \geqslant \ell$, $k + \ell = n$ et

$$P(x)Q(s,x) - a = A(s,x)B(s,x). \tag{4.3}$$

Supposons que $\ell \geqslant 1$. En identifiant les coefficients de s^j, pour $j = 0, 1, \ldots, n$, on obtient

$$\begin{aligned}
P(x)Q_n, \quad &= A_k(x)B_\ell(x) \\
P(x)Q_{n-1}(x) \quad &= A_k(x)B_{\ell-1}(x) + A_{k-1}(x)B_\ell(x), \\
&\cdots \\
P(x)Q_j(x) = \quad &\sum_{\substack{u+v=j \\ u \leqslant k,\, v \leqslant \ell}} A_u(x)B_v(x), \quad \text{avec} \quad j = n-2, \ldots, 1, \\
&\cdots \\
P(x)Q_0(x) - a = \quad &A_0(x)B_0(x).
\end{aligned} \tag{4.4}$$

Comme $P(x)$ est un polynôme séparable, alors $(A_k(x), B_\ell(x)) = 1$. On en déduit, d'après la seconde équation du système (4.4), que $A_k(x) | A_{k-1}(x)$ et que $B_\ell(x) | B_{\ell-1}(x)$. On déduit d'après les équations suivantes du système (4.4) que pour tout $j = 0, \ldots, k$ et $h = 0, \ldots, \ell - 1$, $A_k(x) | A_j(x)$ et $B_\ell(x) | B_h(x)$. Ce qui contredit la dernière équation du système (4.4). Par conséquent $\ell = 0$, autrement dit $B(s,x) = B(x)$ et $k = n \geqslant 1$. En égalant les coefficients de s^n et ceux de s^0 dans l'équation (4.3), on obtient

$$a = B(x) \left(\frac{1}{Q_n} Q_0(x) A_n(x) - A_0(x) \right).$$

On conclut que $B(x)$ est un polynôme constant. □

On déduit de ce théorème les deux corollaires suivants.

Corollaire 4.16 ([5]). *Soit $a \in \mathbb{Z} \setminus \{0\}$ et $P(x) \in \mathbb{Z}[x]$ un polynôme séparable, alors le polynôme $P(x)P(-s-x) - a$ est absolument irréductible.*

Démonstration. Posons $Q(s,x) = P(-s-x)$. Si $P(x) = a_0 + a_1 x + \cdots a_m x^m$ alors

$$Q(s,x) = \sum_{i=0}^{m} a_i(-s-x)^i.$$

Par la formule du binôme, on en déduit que

$$Q(s,x) = \sum_{i=0}^{m} a_i \sum_{k=1}^{i} \binom{i}{k} (-1)^i x^{i-k} s^k.$$

En permutant les deux signes somme on obtient :

$$Q(s,x) = \sum_{k=0}^{m} \left(\sum_{i=k}^{m} a_i \binom{i}{k} (-1)^i x^{i-k} \right) s^k.$$

Pour tout $k \in \{1, \ldots, m\}$, posons

$$Q_k = \sum_{i=k}^{m} a_i \binom{i}{k} (-1)^i x^{i-k}.$$

Alors $Q_m = (-1)^m a_m \in \mathbb{Z} \setminus \{0\}$.
On déduit du théorème 4.15 que le polynôme $P(x)P(-s-x) - a$ est absolument irréductible. □

Corollaire 4.17 ([5]). *Soit $a \in \mathbb{Z} \setminus \{0\}$ et $P(x) \in \mathbb{Z}[x]$ un polynôme séparable, alors le polynôme $R(s,t) - a$ est absolument irréductible.*

Démonstration. Supposons que $R(s,t) - a$ est réductible dans $\overline{\mathbb{Q}}[s,t]$. Alors il existe deux polynômes non constants f et g à coefficients dans $\overline{\mathbb{Q}}$ tels que

$$R(s,t) = f(s,t)g(s,t).$$

Or d'après la proposition 4.12, $R(s, -x^2 - sx) - a = P(x)P(-s-x) - a$, par conséquent

$$P(x)P(-s-x) - a = f(s, -x^2 - sx)g(s, -x^2 - sx).$$

Ce qui contredit le corollaire 4.16. On conclut que le polynôme $R(s,t) - a$ est absolument irréductible.
□

4.5 Application de la méthode de Runge

Dans cette section, nous utilisons la méthode de Runge pour montrer que, pour tout entier rationnel non nul a, l'équation

$$\mathrm{Res}_x \left(P(x), x^2 + sx + t \right) = a$$

possède un nombre fini de solutions entières (s,t).
Si $f(x,y) = \sum_{i,j} a_{ij} x^i y^j \in \mathbb{Q}[x,y]$ est un polynôme non nul, alors le degré de f est l'entier n défini

par :

$$n = \max\{i + j; \quad a_{ij} \neq 0\}.$$

Définition 4.18. *Soit $f(x, y) = \sum_{i,j} a_{ij} x^i y^j \in \mathbb{Q}[x, y]$ un polynôme non nul de degré n. La partie homogène de f, notée f^+, est le polynôme de $\mathbb{Q}[x, y]$ défini par :*

$$f^+(x, y) = \sum_{i+j=n} a_{ij} x^i y^j.$$

Exemple 4.19. *Soit $f(x, y) = 1 + x + y + 2xy + 3x^2 - 2y^2 + x^3 + 2y^3 - xy^2 - 2x^2y$. Le polynôme f est de degré 3 et on a*

$$f^+(x, y) = x^3 + 2y^3 - xy^2 - 2x^2y.$$

En 1887, Runge [61] démontre le théorème suivant.

Théorème 4.20. *Soit $f(x, y)$ un polynôme à coefficients entiers de degré n, irréductible dans $\mathbb{Q}[x, y]$. Si la partie homogène de f de degré n est réductible dans $\mathbb{Q}[x, y]$ mais n'est pas à un facteur constant près une puissance d'un polynôme irréductible. Alors l'équation $f(x, y) = 0$ possède un nombre fini de solutions entières.*

Ce théorème a été amélioré par Schinzel [62], en 1969.

Théorème 4.21 ([52, Theorem 21])**.** *Soit $F(x, y) \in \mathbb{Z}[x, y]$ un polynôme de degré n irréductible dans $\mathbb{Q}[x, y]$ et soit $F^+(x, y)$ sa partie homogène de degré n. Si $F(x, y) = 0$ possède un nombre infini de solutions entières, alors, à un facteur constant près, $F^+(x, y)$ est une puissance d'une forme linéaire ou d'une forme quadratique irréductible non définie.*

Lemme 4.22 ([5])**.** *Soit $P(x) \in \mathbb{Z}[x]$, $R(s, t) = \mathrm{Res}_x(P(x), x^2 + sx + t)$ et $R^+(s, t)$ la partie homogène de $R(s, t)$ de degré m. Alors*

$$R^+(s, t) = a_m(-s)^m P(-t/s),$$

où $m = \deg P$ et a_m est le coefficient dominant de P.

Démonstration. Soient $\alpha_1, \ldots, \alpha_m$ les racines du polynôme P dans $\mathbb{C}$. On a alors

$$P(x) = a_m \prod_{i=1}^{m} (x - \alpha_i).$$

D'après le théoréme 4.6,

$$R(s, t) = \mathrm{Res}_x \left(P(x), x^2 + sx + t\right) = a_m^2 \prod_{i=1}^{m} (\alpha_i^2 + s\alpha_i + t).$$

Par suite,

$$\begin{aligned} R^+(s, t) &= a_m^2 \prod_{i=1}^{m} (s\alpha_i + t) = a_m^2 \prod_{i=1}^{m} (-s) \left(-\alpha_i - \frac{t}{s}\right) \\ &= (-s)^m a_m \cdot a_m \prod_{i=1}^{m} \left(-\alpha_i - \frac{t}{s}\right) = a_m(-s)^m P(-\frac{t}{s}). \end{aligned}$$

□

Théorème 4.23. *Soit $a \in \mathbb{Z} \setminus \{0\}$ et $P(x)$ un polynôme à coefficients entiers, séparable et de degré $m \geqslant 3$. Alors l'équation*

$$\mathrm{Res}_x\left(P(x), x^2 + sx + t\right) = a \tag{4.5}$$

possède un nombre fini de solutions entières.

Démonstration. Par hypothèse, P est un polynôme séparable. Posons $F(s,t) = R(s,t) - a$, d'après le corollaire 4.17, $F(s,t)$ est absolument irréductible. Le polynôme $F(s,t)$ est de degré m et sa partie homogène de degré m, $F^+(s,t)$, est donnée par

$$F^+(s,t) = R^+(s,t).$$

D'après le lemme 4.22, on a

$$F^+(s,t) = a_m(-s)^m P\left(\frac{-t}{s}\right), \tag{4.6}$$

où a_m est le coefficient dominant de P.
Supposons qu'il existe $\lambda, \mu, \nu \in \mathbb{Z}$ et un entier positif k tels que

$$F^+(s,t) = \lambda(\mu s + \nu t)^k.$$

Alors, d'après la relation (4.6), $k = m$ et on a

$$a_m P\left(-\frac{t}{s}\right) = \lambda\left(\nu\frac{-t}{s} - \mu\right)^m.$$

Par suite,

$$a_m P(x) = \lambda(\nu x - \mu)^m.$$

Ce qui contredit l'hypothèse de séparabilité de P. On conclut que $F^+(s,t)$ ne peut s'écrire, à la multiplication près par une constante, comme une puissance d'une forme linéaire.
Supposons maintenant qu'il existe $\lambda, \mu, \nu, \omega \in \mathbb{Z}$ et un entier positif k tels que

$$F^+(s,t) = \lambda(\mu s^2 + \omega st + \nu t^2)^k.$$

Alors, d'après la relation (4.6), m est pair, $k = \frac{m}{2}$ et on a

$$a_m P\left(-\frac{t}{s}\right) = \lambda\left(\mu - \omega\frac{t}{s} + \nu\frac{t^2}{s^2}\right)^k.$$

Par suite

$$a_m P(x) = \lambda(\mu + \omega x + \nu x^2)^k.$$

Ce qui contredit l'hypothèse P séparable. On conclut que $F^+(s,t)$ ne peut s'écrire, à la multiplication près par une constante, comme une puissance d'une forme quadratique.
Les conditions du théorème 4.21 sont donc satisfaites et par conséquent, l'équation (4.5) possède un nombre fini de solutions entières. □

Lemme 4.24. *Soit $f(x) = P(x)D(x) \in \mathbb{Z}[x]$, où $D = \mathrm{pgcd}(f, f')$. Alors le polynôme P est séparable et f et P possèdent les mêmes racines.*

Démonstration. Il existe deux polynômes P et Q à coefficients entiers tels que $f = DP$, $f' = DQ$ et $\mathrm{pgcd}(P, Q) = 1$. Soit alors une racine α de P dans $\mathbb{C}$ de multiplicité k. Alors il existe un entier

m tel que α soit racine de f de multiplicité m et racine de $f' = DQ$ de multiplicité $m-1$. Or $\text{pgcd}(P,Q) = 1$, donc $(x-\alpha)^{m-1}$ divise le polynôme D. Par conséquent f est divisible par $(x-\alpha)^{m+k-1}$. Par suite, $m+k-1 \leqslant m$. Autrement dit $k \leqslant 1$. On conclut que P est un polynôme séparable.
Soit α une racine de f de multiplicité m. Supposons que $P(\alpha) \neq 0$, alors α est racine de D de multiplicité m. Par suite $(x-\alpha)^m$ divise f'. Ce qui est absurde. □

Théorème 4.25 ([5]). *Soit $b \in \mathbb{Z} \setminus \{0\}$ et $f(x) \in \mathbb{Z}[x]$ possédant au moins trois racines distinctes dans $\mathbb{C}$. Si $\deg f - \deg\left(\text{pgcd}\left(f, f'\right)\right) \geqslant 3$ alors l'équation*

$$\text{Res}_x\left(f(x), x^2 + sx + t\right) = b \tag{4.7}$$

possède un nombre fini de solutions entières.

Démonstration. Soient $D = \text{pgcd}(f, f')$ et $P \in \mathbb{Z}[x]$ tel que $f = DP$. D'après la proposition 4.7,

$$\text{Res}_x(f(x), x^2 + sx + t) = \text{Res}_x\left(P(x), x^2 + sx + t\right) \text{Res}_x\left(D(x), x^2 + sx + t\right).$$

Si (s,t) est une solution de l'équation (4.7) alors il existe un diviseur a de b tel que :

$$\text{Res}_x\left(P(x), x^2 + sx + t\right) = a. \tag{4.8}$$

Or, d'après le lemme 4.24, P est un polynôme séparable, possédant au moins trois racines distinctes, donc $\deg P \geqslant 3$. Par conséquent, d'après le théorème 4.23 l'équation (4.8), possède un nombre fini de solutions entières. Comme b ne possède qu'un nombre fini de diviseurs, alors l'équation (4.7) possède, elle aussi, un nombre fini de solutions entières. □

Conclusion et perspectives

Le travail présenté dans cette thèse porte sur l'étude combinatoire de suites numériques remarquables telles que les suites de nombres de Bernoulli, de Genocchi et de Stirling ainsi que sur l'étude de certaines équations diophantiennes telles que les équations de Pell-Fermat, les équations de Cassels et les équations de type résultant.

Dans le chapitre 1, nous avons démontré, en utilisant une méthode symbolique, une identité combinatoire vérifiée par toute suite de Cesàro. Cette identité nous a permis de généraliser plusieurs identités concernant les nombres de Bernoulli et de découvrir de nouvelles identités similaires pour les nombres de Genocchi, les nombres de Fibonacci et les nombres de Lucas.

Dans le chapitre 2, nous avons rappelé la définition des polynômes de Stirling et des polynômes de Nörlund en fournissant un algorithme de calcul rapide de ces polynômes. Nous avons donné une expression explicite des coefficients des polynômes de Nörlund et des dénominateur communs de leurs coefficients. On a pu ainsi fournir une factorisation partielle des polynômes de Stirling qui nous a permis d'apporter une réponse positive à une question posée par D.S. Mitrinović et R.S. Mitrinović [49], relative à une propriété vérifiée par les polynômes de Stirling, restée sans réponse depuis près d'un demi-siècle.

Dans le chapitre 3, après avoir donné des algorithmes de résolution de certaines équations diophantiennes et rappelé quelques résultats de Ljunggren sur le nombre de solutions de certaines équations diophantiennes quartiques , nous avons démontré, en utilisant des propriétés du symbole de Legendre, que l'équation de Cassels $y^2 = px\left(Ax^2+2\right)$, possède au plus six solutions en entiers strictement positifs. Nous avons ainsi pu améliorer la majoration du nombre de solutions obtenue par Alain Togbé [69] et avons prouvé que sa conjecture (voir Conjecture 3.1) a une réponse positive si $(A,p) \equiv (1,5)$, $(1,7)$, $(3,3)$, $(3,5)$, $(5,3)$, $(7,3)$ ou $(7,5)$ $(\mathrm{mod}\ 8)$.

Enfin, dans le chapitre 4, on a démontré que si $P \in \mathbb{Z}[x]$ est un polynôme séparable, alors le polynôme $R(s,t) - a = \mathrm{Res}_x(P, x^2+sx+t) - a$ est un polynôme absolument irréductible. Ce résultat, sans doute le plus important de ce chapitre 4, nous a permis d'appliquer la méthode de Runge, en l'occurrence le théorème 4.21, et ce, pour démontrer, en premier lieu que si P est un polynôme séparable, alors l'équation $R(s,t) = a$ possède un nombre fini de solutions. Puis de généraliser ce résultat pour tout polynôme $f \in \mathbb{Z}[x]$ possédant au moins trois racines distinctes ; autrement dit, f possède un facteur séparable dans $\mathbb{Z}[x]$ de degré supérieur ou égal à 3.

Les résultats obtenus dans cette thèse pourraient constituer une base d'un travail qui gagnerait à être poursuivi. Plus précisément, les perspectives futures sont l'utilisation systématique du calcul ombral afin d'élaborer, non seulement de nouvelles identités combinatoires vérifiées par des suites de nombres, mais aussi d'inédites identités satisfaites par des suites de polynômes comme la suite

des polynômes d'Apostol-Bernoulli et la suite des polynômes d'Apostol-Euler. On rappelle que la suite des polynômes d'Apostol-Bernoulli $\left(\mathfrak{B}_n(x;\lambda)\right)_n$ et d'Apostol-Euler $\left(\mathfrak{E}_n(x;\lambda)\right)_n$ sont définies pour $\lambda \in \mathbb{C}$, par les séries génératrices exponentielles :

$$\frac{z}{\lambda e^z - 1} e^{xz} = \sum_{n=0}^{\infty} \mathfrak{B}_n(x;\lambda) \frac{z^n}{n!} \quad \text{et} \quad \frac{2}{\lambda e^z + 1} e^{xz} = \sum_{n=0}^{\infty} \mathfrak{E}_n(x;\lambda) \frac{z^n}{n!} \quad \text{pour } \lambda \neq -1.$$

Une perspective des plus intéressantes serait de démontrer la conjecture d'Alain Togbé ou, dans le cas contraire, exhiber un exemple pour lequel la conjecture n'est pas vérifiée. Nous souhaitons par la suite étendre notre travail à l'étude d'autres équations de Cassels. Plus généralement, nous nous intéresserons à l'étude des équations $y^2 = px(Ax^2 - 2)$, $y^2 = px(Ax^2 \pm 1)$ et $y^2 = px(Ax^2 \pm 4)$, Nous espérons ainsi améliorer les majorations sur le nombre de solutions en entiers strictement positifs obtenues par Li et Yuan [79] et Wu et al. [76]. Une perspective, peut-être un peu lointaine, serait d'améliorer le résultat obtenu en 2001 par Luca et Walsh [45]. En effet, ces derniers auteurs ont démontré que l'équation diophantienne $y^2 = nx(x^2 + 2)$, possède au plus $3 \cdot 2^{\omega(n)} - 1$ solutions en entiers strictement positifs, où $\omega(n)$ désigne la fonction de Hardy-Ramanujan qui compte le nombre de facteurs premiers tous distincts de n.

> *Hardy déclara, à propos de certaines formules (de Ramanujan) qu'il ne pouvait comprendre, qu'« un seul coup d'œil sur ces formules était suffisant pour se rendre compte qu'elles ne pouvaient être pensées que par un mathématicien de tout premier rang. Elles devaient être vraies, parce que personne n'eût pu avoir l'idée de les concevoir fausses. » Hardy aimait classer les mathématiciens sur une échelle de* 1 *à* 100*. Il s'attribuait* 25*, donnait* 30 *à Littlewood,* 80 *à David Hilbert et* 100 *à Ramanujan.*

Bibliographie

[1] A. Adelberg, *A finite difference approach to degenerate Bernoulli and Stirling polynomials.*, Discrete Math., 140 (1995), pp. 1–21.

[2] ——, *Congruences of p-adic integer order Bernoulli numbers.*, J. Number Theory, 59 (1997), pp. 374–388.

[3] ——, *Arithmetic properties of the Nörlund polynomial $B_n^{(x)}$.*, Discrete Math., 204 (1999), pp. 5–13.

[4] S. Akhtari, *The Diophantine equation $ax^4 - by^2 = 1$.*, J. Reine Angew. Math., 630 (2009), pp. 33–57.

[5] S. A. Alkabouss, T. Garici, and J. Larone, *On the equation* $\mathrm{Res}_x(P(x), x^2+sx+t) = a$, Int. J. Number Theory, 14 (https ://doi.org/10.1142/S1793042118500653, 2018), pp. xx–xx.

[6] F. Bencherif and T. Garici, *Suites de Cesàro et nombres de Bernoulli*, Publ. Math. Besançon Algèbre Théorie Nr., 2012/1 (2012), pp. 19–26.

[7] ——, *On a property of Stirling polynomials.*, Publ. Inst. Math., Nouv. Sér., 102 (2017), pp. 149–153.

[8] M. Bhargava, *The factorial function and generalizations.*, Am. Math. Mon., 107 (2000), pp. 783–799.

[9] V. Bouniakowsky, *Note sur l'emploi des procédés élémentaires du Calcul Intégral dans des questions relatives a l'Analyse de Diophante.*, Bull. de St. Pétersb., 11 (1853), pp. 65–74.

[10] L. Carlitz, *Bernoulli numbers*, Fib. Quart, 6 (1968), pp. 71–85.

[11] J. Cassels, *A Diophantine equation.*, Glasg. Math. J., 27 (1985), pp. 11–18.

[12] J.-L. Chabert, *Une caractérisation des polynômes prenant des valeurs entières sur tous les nombres premiers.*, Can. Math. Bull., 39 (1996), pp. 402–407.

[13] ——, *Integer-valued polynomials on prime numbers and logarithm power expansion.*, Eur. J. Comb., 28 (2007), pp. 754–761.

[14] C. Chang and C. Ha, *On identities involving Bernoulli and Euler polynomials.*, Fibonacci Q., 44 (2006), pp. 39–45.

[15] C. A. Charalambides, *Enumerative combinatorics.*, Boca Raton, FL : Chapman & Hall/CRC, 2002.

[16] J. Chen and P. Voutier, *Complete solution of the diophantine equation $X^2 + 1 = dY^4$ and a related family of quartic Thue equations.*, J. Number Theory, 62 (1997), pp. 71–99.

[17] K.-W. Chen, *A summation on Bernoulli numbers.*, J. Number Theory, 111 (2005), pp. 372–391.

[18] L. Chen, *On the Diophantine equation $y^2 = px(x^2 + 2)$.*, Acta Math. Sin., Chin. Ser., 53 (2010), pp. 83–86.

[19] W. Y. Chen and L. H. Sun, *Extended Zeilberger's algorithm for identities on Bernoulli and Euler polynomials.*, J. Number Theory, 129 (2009), pp. 2111–2132.

[20] J. Cigler, *q-Fibonacci polynomials and q-Genocchi numbers*, arXiv preprint arXiv :0908.1219, (2009).

[21] L. Comtet, *Analyse combinatoire. Tome 2. (Combinatorial analysis. Vol. 2).* Le mathématicien. 5. Paris : Presses Universitaires de France. 190 p. 20 F. (1970)., 1970.

[22] ——, *Analyse combinatoire approfondie*, Ed. Techniques de l'Ingénieur, 2003.

[23] L. E. Dickson, *History of the theory of numbers. Vol. II : Diophantine analysis. Reprint of the 1920 original published by Carnegie Institution, Washington, DC.*, Mineola, NY : Dover Publications, reprint of the 1920 original published by carnegie institution, washington, dc ed., 2005.

[24] J.-H. Evertse, *Lower bounds for resultants. II.*, in Number theory. Diophantine, computational and algebraic aspects. Proceedings of the international conference, Eger, Hungary, July 29–August 2, 1996, Berlin : de Gruyter, 1998, pp. 181–198.

[25] J.-H. Evertse and K. Győry, *Lower bounds for resultants. I.*, Compos. Math., 88 (1993), pp. 1–23.

[26] M. Fujiwara, *Some applications of a theorem of W. M. Schmidt.*, Mich. Math. J., 19 (1972), pp. 315–319.

[27] I. Gaál, *On the resolution of resultant type equations.*, J. Symb. Comput., 34 (2002), pp. 137–144.

[28] I. Gaál and M. Pohst, *Solving resultant form equations over number fields.*, Math. Comput., 77 (2008), pp. 2447–2453.

[29] T. Garici, O. Kihel, and J. Larone, *The number of solutions to $y^2 = px(Ax^2 + 2)$*, Publ. Inst. Math., Nouv. Sér., (to appear).

[30] M. B. Gelfand, *A note on a certain relation among Bernoulli numbers*, Baškir. Gos. Univ. Ucen. Zap. Vyp, 31 (1968), pp. 215–216.

[31] A. Gérardin, *Solution de l'équation $x^3 + y^3 + z^3 = u^2$ (question 3129, de E. N. Barisien).* Interméd. des math. 23, 7–8, 1916.

[32] I. M. Gessel, *Applications of the classical umbral calculus.*, Algebra Univers., 49 (2003), pp. 397–434.

[33] ——, *On Miki's identity for Bernoulli numbers.*, J. Number Theory, 110 (2005), pp. 75–82.

[34] I. M. Gessel and R. P. Stanley, *Stirling polynomials.*, J. Comb. Theory, Ser. A, 24 (1978), pp. 24–33.

[35] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete mathematics : a foundation for computer science. 2nd ed.*, Amsterdam : Addison-Wesley Publishing Group, 2nd ed. ed., 1994.

[36] R. M. Guralnick and M. Lorenz, *Orders of finite groups of matrices.*, in Groups, rings and algebras. A conference in honor of Donald S. Passman, Madison, WI, USA, June 10–12, 2005, Providence, RI : American Mathematical Society (AMS), 2006, pp. 141–161.

[37] K. Győry, *Some applications of decomposable form equations to resultant equations.*, Colloq. Math., 65 (1993), pp. 267–275.

[38] C. Jordan, *Calculus of finite differences.* Budapest : Hungarian Agent Eggenberger Book-Shop. XXI, 654 p. (1939)., 1939.

[39] M. Kaneko, *A recurrence formula for the Bernoulli numbers.*, Proc. Japan Acad., Ser. A, 71 (1995), pp. 192–193.

[40] A. Khinchin, *Continued fractions.* Chicago and London : The University of Chicago Press. xi, 95 pp. (1964)., 1964.

[41] S. Lang, *Algebra*, New York, NY : Springer, 3rd revised ed., 2002.

[42] A. M. Legendre, *Essai sur la théorie des nombres.*, Duprat,Paris, 1797.

[43] G. Liu and H. M.Srivastava, *Explicit formulas for the Nörlund polynomials $B_n^{(x)}$ and $b_n^{(x)}$.*, Comput. Math. Appl., 51 (2006), pp. 1377–1384.

[44] W. Ljunggren, *Ein Satz über die diophantische Gleichung $Ax^2 - By^4 = C$ ($C = 1, 2, 4$).* 12. Skand. Mat.-Kongr., Lund 1953, 188-194 (1954)., 1954.

[45] F. Luca and P. Walsh, *Squares in Lehmer sequences and some Diophantine applications.*, Acta Arith., 100 (2001), pp. 47–62.

[46] E. Lucas, *Théorie des nombres. Tome I : Le calcul des nombres entiers. Le calcul des nombres rationnels. La divisibilite arithmétique.*, Gauthier-Villars, Paris, 1891.

[47] H. Minkowski, *Zur theorie der positiven quadratischen formen.*, J. Reine Angew. Math., 101 (1887), pp. 196–202.

[48] D. S. Mitrinović and R. S. Mitrinović, *Sur les polynômes de Stirling.*, Bull. Soc. Math. Phys. Serbie, 10 (1958), pp. 43–49.

[49] ——, *Tableaux qui fournissent des polynômes de Stirling.*, Publ. Fac. Electrotech. Univ. Belgrade, Ser. Math. Phys., 34 (1960), pp. 1–23.

[50] ——, *Sur une classe de nombres se rattachant aux nombres de Stirling. Appendice : Table des nombres de Stirling.*, Publ. Fac. Electrotech. Univ. Belgrade, Ser. Math. Phys., 60 (1961), p. 62.

[51] H. Momiyama, *A new recurrence formula for Bernoulli numbers.*, Fibonacci Q., 39 (2001), pp. 285–288.

[52] L. J. Mordell, *Diophantine Equations*, Pure and Applied Mathematics, Elsevier Science, 1969.

[53] S. Narumi, *On a power series having only a finite number of algebraico-logarithmic singularities on its circle of convergence.*, Tohoku Math. J., 30 (1929), pp. 185–201.

[54] N. Nielsen, *Recherches sur les polynômes et les nombres de Stirling.*, Annali di Mat. (3), 10 (1904), pp. 287–318.

[55] ——, *Recherches sur les polynômes de Stirling, Hovedkommissionaer : Andr* , Hovedkommissionaer : Andr. Fred. Høst & Søn, Kgl. Hof-Boghandel, Bianco Lunos Bogtrykkeri, København, Denmark, (1920).

[56] ——, *Traité élémentaire des nombres de Bernoulli.* Paris : Gauthier-Villars, x, 398 p. 8° (1923)., 1923.

[57] N. E. Nörlund, *Vorlesungen über Differenzenrechnung. (Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, Bd. 13.).* Berlin : J. Springer, IX u. 551 S. 8° (1924) ; Reprinted by Chelsea Publishing Company, New York., 1954.

[58] A. Pethö, *Application of Gröbner bases to the resolution of systems of norm equations.*, in ISSAC '91. Proceedings of the 1991 international symposium on Symbolic and algebraic computation. Bonn, Germany, July 15–17, 1991, New York, NY : ACM Press, 1991, pp. 144–150.

[59] ——, *Systems of norm equations over cubic number fields.*, Grazer Math. Ber., 318 (1993), pp. 111–120.

[60] G.-C. Rota, *The number of partitions of a set.*, Am. Math. Mon., 71 (1964), pp. 498–504.

[61] C. Runge, *Ueber ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen.*, J. Reine Angew. Math., 100 (1887), pp. 425–435.

[62] A. Schinzel, *An improvement of Runge's theorem on diophantine equations.* Commentarii Pontif. Acad. Sci. 2, No.20, 9 p. (1969)., 1969.

[63] H. P. Schlickewei, *Inequalities for decomposable forms.*, Astérisque, 41-42 (1977), pp. 267–271.

[64] W. M. Schmidt, *Inequalities for resultants and for decomposable forms.* Diophantine Approx. Appl., Proc. Conf. Washington 1972, 235-253 (1973)., 1973.

[65] I. Schur, *Über eine Klasse von endlichen Gruppen linearer Substitutionen.*, Berl. Ber., 1905 (1905), pp. 77–91.

[66] N. J. Sloane et al., *The on-line encyclopedia of integer sequences.* URL https ://oeis.org/,[Online], 2017.

[67] J. Stirling, *Methodus differentialis, sive Tractatus de summatione et interpolatione serierum infinitarum. Auctore Jacobo Stirling, RSS*, prostat apud J. Whiston & B. White, in Fleet-street, 1764.

[68] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres.*, Paris : Société Mathématique de France, 2ème éd. ed., 1995.

[69] A. Togbé, *A note on the Diophantine equation* $y^2 = px(Ax^2 + 2)$., Afr. Mat., 25 (2014), pp. 739–744.

[70] A. Togbé, P. Voutier, and P. Walsh, *Solving a family of Thue equations with an application to the equation* $x^2 - Dy^4 = 1$., Acta Arith., 120 (2005), pp. 39–58.

[71] C. Tweedie, *The Stirling numbers and polynomials*, Proc. Edinb. Math. Soc., II. Ser., 37 (1918), pp. 2–25.

[72] A. von Ettingshausen, *Vorlesungen über die höhere Mathematik, vol. 1, C*, Gerold, Vienna, 1827.

[73] P. L. von Seidel, *Uber eine einfache Entstehungsweise der Bernoullischen Zahlen und einiger verwandten Reihen, Sitzungsberichte der Münch*, Akad. Math. Phys. Classe, 7 (1877), pp. 157–187.

[74] E. A. Wirsing, *On approximations of algebraic numbers by algebraic numbers of bounded degree.* 1969 Number Theory Institute, Proc. Sympos. Pure Math. 20, 213-247 (1971)., 1971.

[75] K.-J. Wu, Z.-W. Sun, and H. Pan, *Some identities for Bernoulli and Euler polynomials.*, Fibonacci Q., 42 (2004), pp. 295–299.

[76] W. Wu, A. Togbé, B. He, and S. Yang, *On the number of solutions of the Diophantine equation* $y^2 = nx(Ax^2 \pm C)$, S. Pac. J. Pure Appl. Math., 2 (2013), pp. 1–16.

[77] S. Y. Yan, *Number theory for computing.*, Berlin : Springer, 2000.

[78] P. Yuan, *Rational and algebraic approximations of algebraic numbers and their application.*, Sci. China, Ser. A, 40 (1997), pp. 1045–1051.

[79] P. Yuan and Y. Li, *On the Diophantine equation* $y^2 = px(Ax^2 - 2)$., JP J. Algebra Number Theory Appl., 14 (2009), pp. 185–190.

[80] ——, *Squares in Lehmer sequences and the Diophantine equation* $Ax^4 - By^2 = 2$., Acta Arith., 139 (2009), pp. 275–302.

Index

S

U

V

Z

.

USTHB
Faculté de Mathématiques
le 9 mars 2018